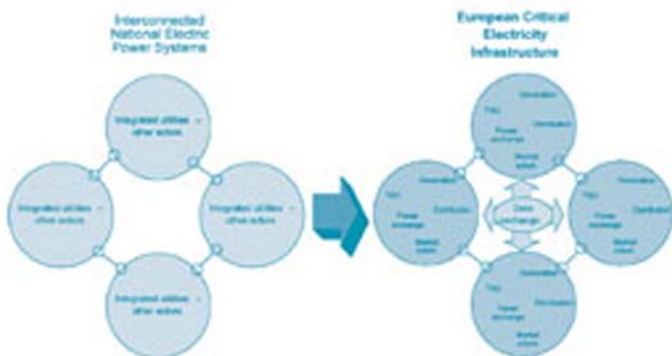


# Critical Infrastructures at Risk

## Securing the European Electric Power System

A.V. Gheorghe, M. Masera,  
M. Weijnen and L. De Vries



**ETH**

École Polytechnique Fédérale de Zurich  
Swiss Federal Institute of Technology Zurich

future

EUROPEAN COMMISSION  
European Union  
Joint Research Centre

WELT  
Wissenschaftszentrum  
für Energieerzeugung  
und Umwelttechnik  
Karlsruhe Institute of Technology

# CRITICAL INFRASTRUCTURES AT RISK

# TOPICS IN SAFETY, RISK, RELIABILITY AND QUALITY

---

VOLUME 9

---

## *Editor*

Adrian.V. Gheorghe

*Swiss Federal Institute of Technology, Zürich, Switzerland*

## *Editorial Advisory Board*

P. Sander, *Technical University of Eindhoven, The Netherlands*

D.C. Barrie, *Lakehead University, Ontario, Canada*

R. Leitch, *Royal Military College of Science (Cranfield), Shrivenham, U.K.*

*Aims and Scope.* Fundamental questions which are being asked these days of all products, processes and services with ever increasing frequency are:

- What is the risk?
- How safe is it?
- How reliable is it?
- How good is the quality?
- How much does it cost?

This is particularly true as the government, industry, public, customers and society become increasingly informed and articulate.

In practice none of the three topics can be considered in isolation as they all interact and interrelate in very complex and subtle ways and require a range of disciplines for their description and application; they encompass the social, engineering and physical sciences and quantitative disciplines including mathematics, probability theory and statistics.

The major objective of the series is to provide a series of authoritative texts suitable for academic taught courses, reference purposes, post graduate and other research and practitioners generally working or strongly associated with areas such as:

- Safety Assessment and Management
- Emergency Planning
- Risk Management
- Reliability Analysis and Assessment
- Vulnerability Assessment and Management
- Quality Assurance and Management

Special emphasis is placed on texts with regard to readability, relevance, clarity, applicability, rigour and generally sound quantitative content.

*The titles published in this series are listed at the end of this volume.*

# Critical Infrastructures at Risk

Securing the European Electric Power System

A.V. Gheorghe

*Swiss Federal Institute of Technology, Zurich, Switzerland*

M. Masera

*European Commission - Joint Research Centre, Ispra, Italy*

M.P.C Weijnen

*Technical University Delft, The Netherlands*

L. J. De Vries

*Technical University Delft, The Netherlands*



Springer

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN-10 1-4020-4306-6 (HB)

ISBN-13 978-1-4020-4306-2 (HB)

---

Published by Springer,  
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

*www.springer.com*

*Printed on acid-free paper*

All Rights Reserved

© 2006 Springer

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording or otherwise, without written permission from the Publisher, with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

Printed in the Netherlands.

# Contents

<b>Executive Summary .....</b>	<b>VII</b>
<b>Contributing Authors .....</b>	<b>XXVII</b>
<b>Acknowledgements .....</b>	<b>XXIX</b>

## **Chapter 1: Introduction**

1.1	Scope .....	1
1.2	Infrastructures, Risks and Society.....	2
1.3	Definitions .....	4
1.4	The European Electricity Infrastructure Today and Tomorrow .....	6
1.5	Background and Structure of this Book.....	16

## **Chapter 2: Infrastructures at Risk**

2.1	Introduction .....	19
2.2	A Generic Approach to Critical Infrastructures.....	20
2.3	Trends in Systems of Critical Infrastructures .....	26
2.4	Risk and Vulnerability in Critical Infrastructures.....	33
2.5	Conclusion.....	36

## **Chapter 3: Liberalisation and Internationalisation of the European Electricity Supply System**

3.1	Introduction .....	37
3.2	Liberalisation.....	38
3.3	Internationalisation.....	61
3.4	System Security.....	78
3.5	Conclusions .....	83

## **Chapter 4: The Security of Information and Communication Systems and the E+I Paradigm**

4.1	Introduction .....	85
4.2	The Evolution towards the E+I Paradigm.....	86
4.3	The Impact of Digitalization on Security.....	94
4.4	ICS Security Risks .....	104
4.5	Conclusions .....	116

## **Chapter 5: Governing Risks in the European Critical Electricity Infrastructure**

5.1	Introduction .....	117
5.2	Risks in the European Critical Electricity Infrastructure .....	118
5.3	Risk Governance of ECEI .....	134
5.4	Conclusions .....	151

## **Chapter 6: Concluding Remarks and Recommendations**

6.1	Introduction .....	153
6.2	A European Council for the Security of Electric Power .....	155
6.3	Policies Supporting the Development of a Secure ECEI .....	158
6.4	A Multidisciplinary R&D Programme and a Public-private Knowledge Platform Addressing the “Security of Critical Infrastructures” .....	160

## **Appendices**

<i>A.1 Learning from the Past – Electric Power Blackouts and Near Misses in Europe</i> .....	163
<i>A.2 Critical Electricity Infrastructure: Current Experience in Europe...</i>	195
<i>A.3 Security Conceptual Frameworks</i> .....	255
<i>A.4 ICS Security Standards</i> .....	261
<i>A.5 Critical Information Infrastructures (CII) and Risk Analysis Framework</i> .....	271
<i>A.6 Critical Information Infrastructure Protection – Organizational and Legal Aspects</i> .....	295
<i>A.7 Profiling the Risk Governance Gap</i> .....	303
<i>A.8 The Institutional and Regulatory Context for Risk Governance of the European Critical Electricity Infrastructure</i> .....	323
<i>A.9 Costs of Power Infrastructure Malfunctioning</i> .....	331

<b>References</b> .....	<b>343</b>
-------------------------	------------

<b>Glossary</b> .....	<b>367</b>
-----------------------	------------

<b>Subject Index</b> .....	<b>369</b>
----------------------------	------------

# Executive Summary

## What this book is about

This book investigates the potential risks and vulnerabilities of the European electricity infrastructure, with the objective of contributing to its adequate protection. The work started from the understanding that the market and technical transformations recently experienced by that infrastructure demand a new appraisal of its exposure to risks. Factors such as deregulation, the unbundling of vertically integrated utilities and the increase of cross-border power flows, challenge the applicability of the traditional approaches to risk assessment and management. In this light, the final aim of the book is to set the basis for an appropriate industrial and political European-wide response to these challenges.

A number of significant power contingencies witnessed by Europe during recent years, has raised serious questions about the reliability of the electricity infrastructure. Some of those contingencies revealed the potentiality of a significant impact on the welfare of society. Society has incorporated electricity as an inherent component, indispensable for achieving an expected quality of life. Therefore, impingements on the continuity of the electricity service can distress society as a whole by affecting individuals, social and economic activities, other infrastructures<sup>1</sup> and essential government functions. It is even plausible to hypothesise that in extreme situations a grave power failure might have significant effects on national security. From such considerations emerges the necessity of properly identifying and evaluating the threats, and of an adequate decision making framework for dealing with those risks in a multi-national setting.

<sup>1</sup> See W.A.H. Thissen, P. M. Herder (Editors) – “*Critical Infrastructures. State of the Art in Research and Application*”, Kluwer Academic, 2003



The series of blackouts and near misses in the last few years present several notable lessons that policy makers, industry and society as a whole have to take into consideration:

- There are hints of some inadequacy in the European electricity infrastructure. Heavy workloads and traded off reserve capacities make systems vulnerable to widespread disruptions. The first line of defence protection systems has played a key role in the majority of catastrophic failures. Power systems are not designed to cope with the concurrent outage of two or more critical components.
- Incidents have been aggravated by other factors, including the lack of timely comprehension by control room operators of potentially far-reaching failures and short-term emergency requirements.
- The recent liberalization of the European electricity market has led to increased cross-border trades for which the international interconnectors among the national transmission systems were not originally designed.
- European transmission system operators, which have only limited system monitoring capabilities and limited influence on international power trading, confront more and more unanticipated congestions on the tie-lines.

During the last decade Europe has developed a comprehensive energy supply policy, unbundling the previous monopolies and opening the generation and distribution markets<sup>2</sup>. This policy towards an integrated European market has deeply changed the business and regulatory landscape of the electric power infrastructure. From the consumer point of view, the effects have been positive: there are more potential suppliers and prices follow market rules.

The immediate economic effects of the new policy have not been accompanied by changes in the underpinning physical systems, whose evolution demands at least medium term investment and planning. To date the power infrastructure has shown an appropriate reliability level, but new threats can be foreseen. Some of the threats are internal to the infrastructure, mainly due to the increasing complexity of many technical and market components, such as the institutional fragmentation among the different states, and some are external, for example the menace of terrorism and of cyber attacks.

<sup>2</sup> European Commission, DG for Energy and Transport, Memo, *Energy infrastructures: increasing security of supply in the Union*, December 2003

Therefore, the security, adequacy, stability and reliability of the evolving European electric power infrastructure deserve a cautious and thorough consideration<sup>3</sup>. Electricity is a “common good” for all the interconnected European countries. It is central to their future economic development and to the security and welfare of almost half billion people. For this reason, although local contingencies can be tolerated up to a given degree, if the power system would appear unreliable at the continental level, it will become a matter of major political and social concern. Europe cannot afford systematic failures and major disruptions of its power infrastructure.

## The European Critical Electricity Infrastructure

This report acknowledges that the various national electricity systems after the transformation experienced in recent years, now form part of a unique and integrated so called **European Critical Electricity Infrastructure (ECEI)**. The situation results from an evolution that is taking place, and is determined by two main driving forces: market liberalization<sup>4</sup> at the continental scale, and high interconnection among regional systems. This has been made possible by the pervasive incorporation of information and communication technologies.

The infrastructure, a socio-technical artefact, tends to function as a unity, although it embeds several jurisdictions, operators and markets. It derives from the interconnection of national and regional systems, but at the same time it behaves as a single, compound system-of-systems. It is decentralized, but disturbances can propagate through it and risks have to be coped with in a coordinated way. The passage from a set of electricity systems to the ECEI is not just a quantitative question of more elements or actors - it represents a qualitative leap. ECEI, an infrastructural system-of-systems, is intrinsically different from a set of weakly interconnected power systems, where energy flows among different systems are marginal and local operation and control are sufficient. The fact that the shortcomings within ECEI exceed the providence of individual parties means that there is

<sup>3</sup> A comparative analysis of policy and regulation in Western Europe has been earlier provided in the book “*European Electricity Systems in Transition*”, Atle Midttun (Editor), Elsevier Science Ltd., Amsterdam, 1997

<sup>4</sup> European Commission, DG for Energy and transport, Memo, *Towards a competitive and regulated European electricity and gas market*, 2004

a need for new, effective instruments for managing risks and vulnerabilities.

The following picture outlines the evolution from national electric power systems (EPS) to their embedding ECEI (see Figure 1). The book analyses the implications of this development, and studies the positive and negative effects of its extensive interconnectedness and digitalisation i.e. the ubiquitous application of information and communication (IC) technologies.

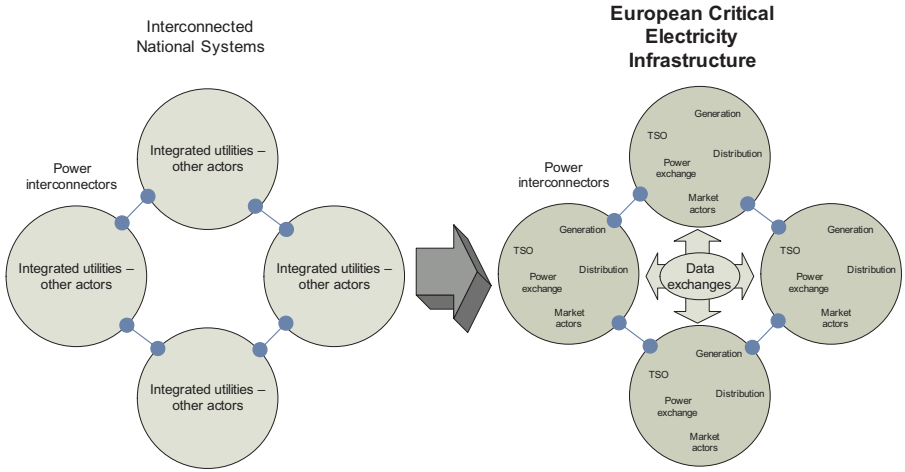


Figure 1. Advent of the European Critical Electricity Infrastructure

## Trends and driving forces

The *liberalization* of the European electricity sector has replaced centralized control by national and sub-regional monopolies with a complex decentralized market structure, in which many different agents control each one a part of a technically highly integrated ECEI. The distribution of the many functions in the electricity infrastructure among numerous different actors has greatly increased the complexity of the sector.

This *de facto* decentralized control can only work appropriately in the long term if all the different agents in the system experience the correct incentives and comply with compatible rules through the European infrastructure. Technical reliability, which used to be the gauge for the

electric power systems performance, is not enough for the ECEI reality. Many other factors, including environmental compatibility, market practicality and national security, have to be included in the decision making process. **Security** can be used as the overarching concept, incorporating all the other objectives.

With respect to this notion of security, all stakeholders should have a common understanding of the overall system goals and be willing to work towards them, both during normal operation and in the case of contingencies. If not, the pursuit of their own private ends, although legitimate, may enter into conflict with public objectives such as availability and affordability. Whereas the regional monopolies of the past required only a relatively simple regulation of their performance and tariffs, the complex decentralized system that is the result of liberalization requires careful crafting of its institutional structure to ensure that multiple, and sometimes conflicting, public goals are met.

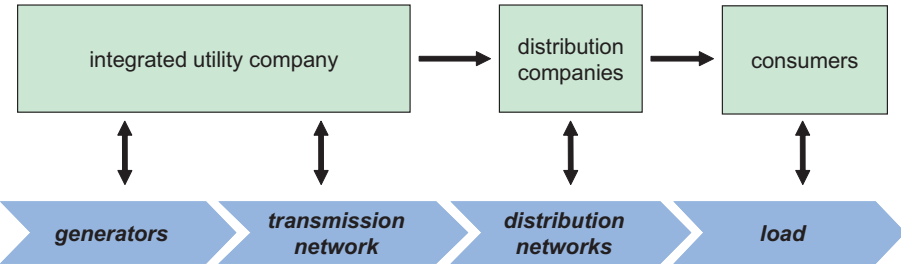


Figure 2. The organizational structure of the electricity system before liberalization

Figures 2 and 3 illustrate the organizational changes that liberalization brought about. In the past, in a situation of regional monopolies, nearly all functions were performed by the same agent: the electricity utility company. A simple model of a current liberalized electricity system shows the different groups of actors who together control the physical system and operates the economic system (see Figure 3). In Europe many of these electricity systems are interconnected with each other and the operation is coordinated in several regional blocks (UCTE, NORDEL, UKTSOA, ATSOI).

A second trend, which already existed prior to liberalization but was further stimulated by it, is the *internationalisation* of the electricity system i.e. interconnection among national grids. The operation of the vast

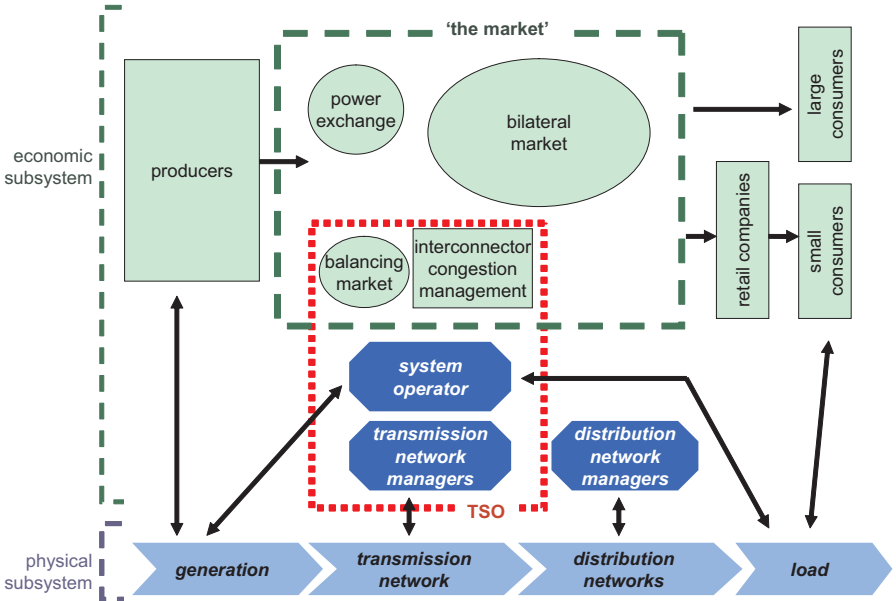


Figure 3. The organizational structure of a liberalized electricity system (decentralized model)

European power network is complicated by the many different jurisdictions and standards that exist. At a technical level, the transmission system operators (TSOs) cooperate with each other, coordinating their operations. At the economic level, large differences continue to exist between the markets in the different countries. In order to create an international level playing field, economic and technical conditions in the different countries, such as transmission tariffs and network access rules, should be put into synergy. In practice, however, different countries liberalize with different speeds and implement different models including taxes and subsidies, not always considering the global consequences of local measures.

The complexity that results from the combination of the liberalization and the internationalisation of the ECEI poses a threat to the reliability of electricity services. A clear case is given by the difficulties that the resulting fragmentation puts to the coordination of responses to wide-area contingencies. The multitude of industrial actors and the many countries involved also complicate the achievement of a balanced development of the system in the long-term, which in turn may give rise to more contingencies.

A third trend, which we will call *evolutionary unsuitability*, is caused by the fact that electricity transmission networks are being used increasingly in ways for which they were not initially designed. Electricity systems are not just operated under high stress conditions, but also beyond the limits of their original design.

Some technical developments complicate this situation. For instance, the increasing development of wind power with rapid operational changes is already leading to stability problems in certain areas. The proposed increases in distributed generation, which means the generation of electricity in small units closer to consumers, can diminish investments in transmission and distribution of electricity, but may also change the way power networks are used. It is impossible to foresee the many changes and uses that the infrastructure will be subjected to. It will require a new approach to the engineering, deployment and operation of the infrastructure, which will include several non-engineering aspects. A continuous collective learning in the production and management of complex systems is required.

A fourth significant trend is the wide scale application of *information and communication (IC) technologies* in electricity systems, from the level of individual devices up to the operational control of entire electricity networks, and from customer databases to automated spot markets. While the use of IC technologies provides augmented functional capabilities for the monitoring and control of installations, the large increase in interconnected equipment and information flows also expands the vulnerability of the ECEI to failures of the information infrastructure and to deliberate cyber attacks. On the other hand, the communication among the infrastructure's stakeholders is fundamental for coping with growing flows and congestions

The amalgamation of electric power systems and IC has given place to a new construct: "Electricity plus Information" (or *E+I*). The ECEI is a clear example of the E+I paradigm, composed of closely interlinked electricity functions (i.e. production, trading, transmission, distribution, billing, customer interaction, etc.) and information-based processes.

When assessing the security of the infrastructure, this E+I reality cannot be ignored. The nature of E+I affects which vulnerabilities and threats have to be taken into consideration, which measures can be taken for solving the problems, but also how actors might interact in the prevention, detection and reaction to risk events<sup>5</sup>.

<sup>5</sup> COM/2004/702 final-Communication from the Commission to the Council and the European Parliament, "Critical Infrastructure Protection in the Fight Against Terrorism", Brussels, 20.10.2004

## Weaknesses of the European Critical Electricity Infrastructure

The analysis of the trends mentioned above, lead the book to the identification of the main *internal* weaknesses and threats (see Figure 4) that affect the ECEI. These can be classified into:

- Market related, e.g.:
  - Uncertainties whether investment in competitive markets leads to a *socially optimal fuel mix* (i.e. one that meets all the concerns of society), or whether the market design can be adjusted to this end. While in theory it may be possible to include all environmental externalities, it appears more difficult to incorporate geopolitical considerations such as fuel security<sup>6</sup>. Markets entail the danger that all new power plants make use of the same cheapest available fuel.
  - The additional regulatory uncertainty that exists during the transition phase to a liberalized market may *discourage investment* in generation capacity. It is also the question whether competitive markets, even in a stable phase after liberalization, provide adequate and timely investment incentives.
- Regulation related, e.g.:
  - With liberalization, new forms of network regulation with a *stronger focus on costs* have been introduced. It is still the question whether the new forms of regulation can balance the incentive to reduce costs with incentives to maintain network quality and expand in a timely and economically efficient manner.
  - The complexity of the institutional design, combined with the fact that the different European countries liberalize their power markets with different speeds and implement different models, creates a significant *risk of market distortions*, the effects of which are not fully understood.

<sup>6</sup> COM/2003/743 Communication from the Commission to the European Parliament and the Council on Energy *Infrastructure and Security of Supply*

- Technology related, e.g.:

- The development of power based on renewables and possibly the development of distributed generation, all lead to *changes in the way the networks are used*. This stresses the operational control and protection of the networks, including the primary energy supply<sup>7</sup>.
- The lack of proper security-related standards and of specific security technologies for *information and communication systems* in the control and protection of the electricity infrastructure jeopardises the achievement of the required risk-related goals.
- The increased use of information and communication technology creates a *risk of power system malfunctioning when the information and communication infrastructure fails*. It also introduces the risk of malicious activities through the information and communication infrastructure with the goal of disrupting the power supply.

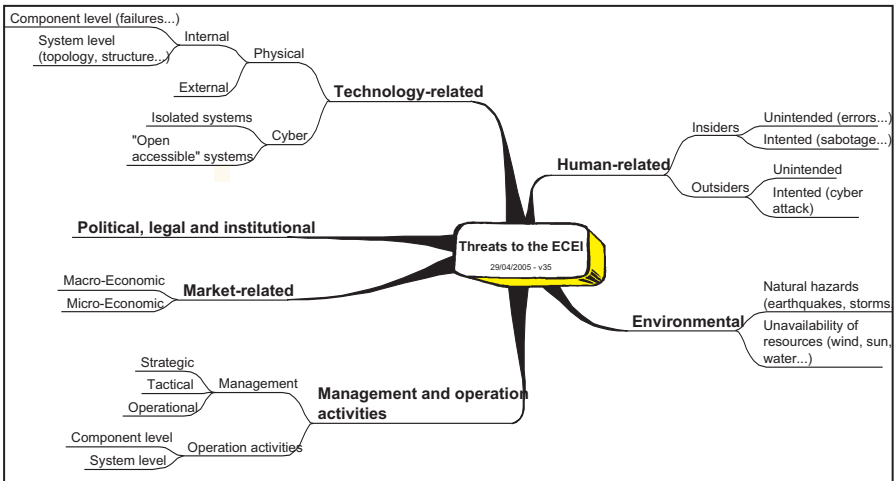


Figure 4. Threat landscape for ECEI

<sup>7</sup> COM/2003/0741 Proposal for a regulation of the European Parliament and the Council on conditions for access to the network for cross-border exchanges in gas



- Topology related, e.g.:
  - The complexity of the network topology creates the possibility of failures that propagate throughout the system, potentially leading to *cascading blackouts*. There is also a potential that failures escalate from local problems to broad disturbances, as happened in the most recent blackouts.
  - The array of multiple connections among systems within the ECEI will require a well orchestrated coordination for restoring services in case of widespread contingencies. Restoration is also dependent on proper computing and communication capabilities and on human factors (such as training). This danger is increased by the organizational complexity that is the result of liberalization.
  - Many of the existing *control and protection strategies and contingency defence plans* are outdated. They were developed in a time when international flows were smaller, generation was dispatched by the system operator and the use of information and communication technology was much more limited.

In addition to the risks that are a consequence of the structure of the system, there are also **external** threats, old and new, that originate from the context where ECEI operates:

- Malicious threats:
  - Much attention is currently given to the *risk of terrorist attacks*<sup>8</sup>. The likelihood is difficult to estimate, but it would require a sophisticated, well-coordinated attack to bring a large part of the European power system down. Failure of individual power plants or power lines is a contingency that the system is designed to withstand, but a complete assessment, considering the interdependencies with other infrastructures has not yet been performed.
  - Power lines are vulnerable to *acts of vandalism and sabotage* from irresponsible or criminal persons, who provoke damage for some ideological or illicit intent.

<sup>8</sup> For a comprehension assessment of threats related to terrorism see “*Making the Nation Safer. The Role of Science and Technology in Countering Terrorism*”, National Academy Press, Washington D.C., 2002

- Accidental threats:
  - The infrastructure is deployed in regions with intensive human activities. There is a non negligible chance of accidental events affecting the physical integrity of the installations, for instance the *inadvertent breaking of power lines*. Underground distribution cables are especially susceptible to damage by, for instance, construction activities.
  - *Natural hazards*, although well known, cannot be ignored. From earthquakes to flooding, from slides to big storms, and including extreme weather conditions, several negative conditions have to be taken into account, considering that they might affect other infrastructural services on which the ECEI is dependent.
- Risk aversion by society:
  - A more mundane but at least as relevant danger is that *the growth of transmission capacity falls* too far behind the growth in consumption. The main restriction on new power lines is the difficulty to obtain the necessary permits. There is a risk that the NIMBY syndrome (Not In My Back Yard) is expanded to the BANANA syndrome (Build Absolutely Nothing Anywhere Near Anyone). This also affects the siting of new generation plants.
- Insufficient R&D:
  - The current increase in the scale of the ECEI, and of the new trends and vulnerabilities by which it is characterized, is not reflected by an equal increase in *research and thinking at system-level*. Much research focuses on the performance of individual components or on the control of individual networks, while crucial questions such as international network stability and market performance remain underexposed.

## The need for risk governance

The European electric power sector has been evolving rapidly in the last decade. The EC Directive 96/92/EC, adopted in 1996, established common rules for the European Union electricity internal market. It established the basis for the opening up of the national markets, for the unbundling of the

vertically integrated electricity companies, and in general for the new organisation of the power generation, transmission and distribution businesses.

As a means for establishing a communication between the stakeholders of the electric power system and the policy decision makers, a forum was convoked to discuss the regulatory process and the formation of the European internal electricity market. It was set up and organised by the European Commission, the first meeting was held in 1988, and it is normally known as the ‘Florence Forum’. Its objective is to provide a neutral and informal framework for discussions concerning the implementation of the Electricity Directives and to foster the integration of national markets.

The normative context was complete in 2003 with the new Electricity Directive n. 54<sup>9</sup>, complemented by the Regulation 1228 on cross-border trade<sup>10</sup>. This Directive aims to establish by July 2007 at the latest, an open European market for electricity, where consumers will be free to shop around across borders.

At the same time, a set of regulators have been instituted in all countries for ensuring the correct operation of the national markets and the fulfilment of the public service character of electricity supply.

The fundamental issue of this policy initiative has been the institution of the European internal market for electricity<sup>11</sup>, and hitherto it has been successful and beneficial for the European citizen. Nevertheless, risk (and security in the broad sense employed in this book) has not been considered a main concern. Security of supply is mentioned as one of the public service attributes to be guaranteed<sup>12</sup>. Specifically, it is said that the goal is to achieve a “competitive, secure and environmentally sustainable market in electricity” (Art. 3). Some issues mentioned in the Directive are: market

<sup>9</sup> Directive 2003/54/EC of the European Parliament and the Council of June 26, 2003 concerning common rules for the internal electricity market; Official Journal L 176, 15/07/2003

<sup>10</sup> EC Regulation 1228/2003 of the European Parliament and the Council of June 26, 2003 concerning conditions for access to the network for cross-border exchange in electricity; Official Journal L 176, 15/07/2003

<sup>11</sup> COM/2005/576 Green Paper on a European Programme for Critical Infrastructure Protection, Commission of the European Communities 17.11.2005

<sup>12</sup> COM/2003/740 Proposal for a Directive of the European Parliament and the Council concerning measures to safeguard security of electricity supply and infrastructure investment

mechanisms for ensuring sufficient electricity generation; long-term planning; and the need to monitor the balance between supply and demand — topics left to the responsibility of each country. However, no provision has been made for coping with the systemic risks that affect the European Infrastructure as a whole.

Therefore it is possible to ascertain a mismatch between the policy goal of developing a secure European electric power sector, and the lack of dedicated mechanisms for dealing with risks that might rise above the control of the single power company, the single country or the coordination among TSOs in a synchronous zone. These ECEI risks will not be satisfied by the mere accumulation of these restricted measures.

Would current instruments be effective for jointly dealing with systemic risks affecting the infrastructure? Past methods of managing risk are no longer adequate in the current ECEI scenario. This is partly due to the emergence of new risks, but also to the restructuring of the electricity industry. In the past, utility companies with a regional monopoly could be held responsible for virtually every aspect of the delivery of electricity. Electric utilities managed technical risks as well as environmental and health risks. It was common practice to apply cost-benefit analysis in order to fulfil primarily the shareholders' concerns.

However, in the current decentralized nature of liberalized electricity systems, individual actors cannot be held responsible for the way the system as a whole functions. This means that, more than in the past, issues such as reliability and resilience should be addressed at the level of the whole system.

The scale and geographical scope of the new potential security risks requires the coordination of decision making at many different levels. This would be by international bodies such as the EU and by associations of transmission system operators (UCTE, ETSO), at the national level, by governments and regulators, and at the company level by generation companies, network companies and system operators. In the near future, the situation will become more intricate as the European electricity infrastructure will be interconnected with North Africa, the Middle East, the whole Balkans, and ample regions of Eastern Europe and Central Asia (from Lisbon to Vladivostok, and from the Arctic Circle to the Maghreb).

The Florence Forum is the only institution that convenes all European stakeholders - industry, regulators, policy decision makers and consumers. Nevertheless, considering its current structure, mission and working style (periodic deliberations focused on market-related issues), it does not appear to match the requirements for dealing with ECEI risks.

Therefore, an innovative approach is needed. This book analyses the changes and proposes a new way for society<sup>13</sup> to handle them: **risk governance**. Risk governance refers to a decision-oriented process where joint solutions are defined by the involvement of all relevant stakeholders. The process should synthesise the multiple dimensions of the problem: the individual interests and concerns of each industrial company, the market and technical criteria for reliable operation, plus the objectives of the different countries and European society as a whole.

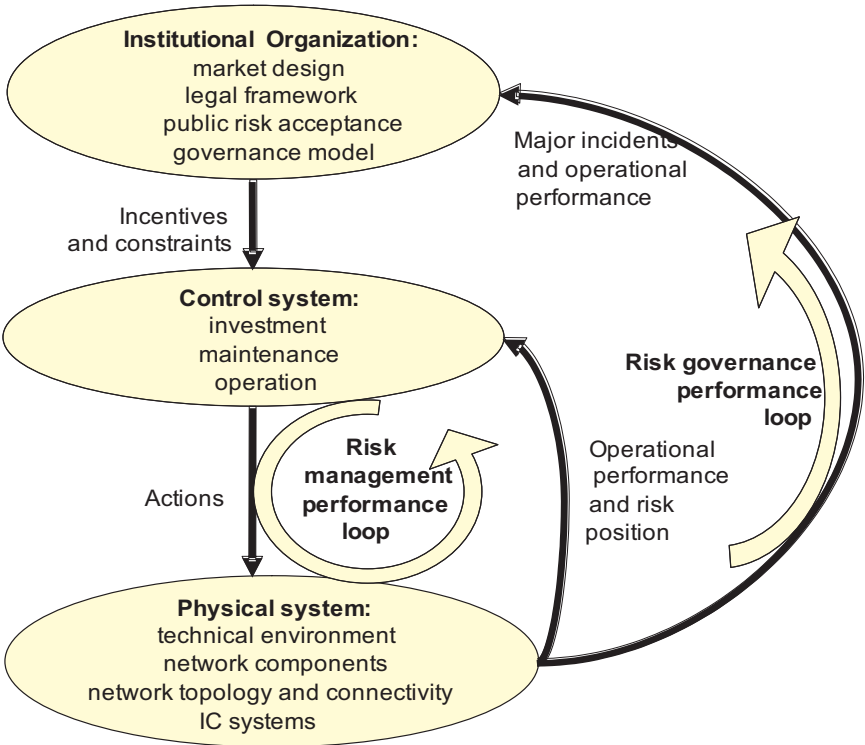


Figure 5. Risk management and risk governance performance loops

<sup>13</sup> On a parallel line of work, in relation to CII (Critical Information Infrastructures), one can consult “Policymaking for Critical Infrastructure. A Case Study on Strategic Interventions in Public Safety Telecommunications”, by Gordon A. Gow, Ashgate Publishing Company, Hampshire, U.K., 2005

Figure 5 illustrates the complementarity and differences between risk management and risk governance by depicting the three levels of decision making in the national systems of the ECEI. The base is the physical system, consisting of the power stations, the networks, the consumer equipment and the IC systems. The middle level contains the agents who directly control the physical system: the generation companies who control the power plants, the distribution network managers, the transmission system operator who controls the transmission network and balances the system, and last, but not least, consumers. The way these actors deal with risks in their own organization is represented by the risk management performance loop.

In a liberalized system, all the parties should work together, as well as with other parties who do not directly influence the physical system such as traders, brokers, power exchanges and retail companies. The highest level in Figure 5 represents the institutional environment embracing all the actors at national level: the design of the market, the regulatory framework, the rules and regulations, the distribution of functions, and the roles and responsibilities of the actors. Through the risk governance process, the different actors (should) cooperate to handle risks that exceed the boundaries of their own risk management processes.

Risks that are (or should be) the subject of the risk governance process are either risks that involve multiple actors or risks that originate outside the control of the involved actors. If the solution is within the risk management loop, there is no need for governance of the issue. However, if the solution is beyond the powers of the actor that is affected, there is a need for risk governance.

## **Lessons learned and policy recommendations**

Four main lessons were learned from the investigations leading to this book:

- European society is witnessing the advent of **ECEI**, a new kind of human construct of great technical complexity and institutional fragmentation, which cannot be managed by a single entity. It is increasingly subject to risks that are critical for society. Those risks are of a very varied nature, and have to be counteracted with an appropriate approach.

- The ECEI is evolving into an “Electricity plus Information” (E+I) infrastructure. The stable operation of the power systems, the management of security issues, the functioning of the markets, the links between industry, regulators and users: all are information-based. The efficient and secured electric service is now an E+I compound product.
- The **new risk landscape** faced by ECEI can be broken down into three layers:
  - Technical layer: risks are caused by technical deficiencies (including failure of components, design of control devices, human errors, engineering flaws). Solutions are mainly technical in nature (e.g. strict application of IC security measures, proper training of operators and improved communications, review of protection mechanisms). Some problems can be addressed by single actors, or by the joint effort of a limited group of them.
  - System layer: risks are caused by the interaction of several technical, organisational and market factors, with effects that are not always predictable (e.g. congestions, deviations of energy flows from schedule). Solutions have to unavoidably combine different matters (e.g. technical, financial) and actors, at times crossing national boundaries.
  - Socio-political layer: risks have a society-wide resonance, potentially affecting the proper performance of a whole community: its security and survivability. Due to the interconnectedness of ECEI, such situations are transboundary by nature and increasingly risky. Solutions have to address the infrastructure as a unity and address the unsuitability of design and operation criteria with current use and of policy objectives with security of supply. This complexity calls for a European approach to risk governance.
- The need for **Risk governance**:
  - ECEI’s emerging risks of European-wide relevance have to be governed by means of a decision-making process tailored to its specific needs and requirements. Key features to be considered are: the multiplicity of stakeholders, the emergent security attributes of the infrastructure, and the dynamic nature of the system and the environment.

- In order to be successful, risk governance should take into account all risk factors and all threats that cannot be dealt with adequately by individual actors' risk management processes, and in a comprehensive and systematic way: e.g. bearing in mind among others power system dynamics, market incentives, IC technologies, and potential malicious attacks.
- Risk governance implies the involvement of all stakeholders and clear rules for the deliberation and development of decisions. In Europe, due to the international nature of the problem, this situation will require the participation of national authorities and the EU, all businesses associated with the electric power infrastructure, international organisations, and not least the end users, including operators of other infrastructures depending on electricity.
- The risk governance process needs to be supported by proper tools embracing a variety of standpoints (political, jurisdictional, technical, environmental, economic, etc.), and requiring the utilization of advanced instruments.

Based on the previous points, the authors of this book recommend three policy priorities:

1. The institution of a new body dedicated to risk governance of the ECEI is urgently needed. The creation of a **European Council for the Security of Electric Power (ECSEP)** is suggested as an option, to ensure that:
  - clear security of supply performance standards for the ECEI are formulated and adhered to;
  - roles and responsibilities for risk management are unambiguously allocated, ensuring that high professional standards and a strong sense of responsibility are maintained in all risk-related decisions;
  - stakeholders can exchange risk-relevant information in a secure way, for supporting more knowledgeable risk assessment and risk management practice, and adequate disturbance alert systems and crisis and emergency management capabilities.
2. The adoption of policies supporting the development of a secure ECEI and relevant to other critical infrastructures, and in particular:



- A system of **economic and regulatory incentives** promoting the implementation and adoption of state-of-the-art security capabilities, in accordance with ECSEP strategies and in the respect of market rules;
  - An “**Infrastructure security business**” policy encouraging the deployment of innovative technologies and services for the assurance of the security of ECEI and other infrastructures.
3. A multidisciplinary R&D programme and a **public-private knowledge platform** addressing the “**Security of Critical Infrastructures**”<sup>14</sup>, including:
- Promotion of centres of excellence dealing with multidisciplinary themes on Risk Governance and Critical Infrastructures.
  - Development of dedicated knowledge networks between: the centres of excellence, infrastructure network managers and system operators, infrastructure service providers, technology providers, governmental bodies and other main stakeholders, for the definition of research programmes and dissemination of research results.
  - Promotion of cross-sectoral knowledge platforms and Communities of Practice, involving practitioners from the infrastructure sectors, governmental bodies (e.g. regulators) and academic experts, in a public-private partnership setting, in order to stimulate processes of cross-sectoral learning (e.g. through exchange of best practices).
  - Promotion of university curricula in relevant fields pertaining to the design and management of Critical Infrastructures, for the preparation of designers, managers and policymakers dealing with the future generation of ECEI and other Critical Infrastructures.
  - Promotion of intensive education and training efforts geared towards the needs of practitioners in the Critical Infrastructure sectors.

<sup>14</sup> See also P.M. Herder, Z. Verwater-Lukszo (Editors), “Towards Next Generation Infrastructures”, Special Issue, Int. J. Critical Infrastructures, Vol. 2, nos 2/3, 2005

- Development of a European R&D programme for the “Security of Critical Infrastructures”, taking advantage of existing projects and initiatives under the Information Society Technologies, Environment and Energy Sustainability programmes of the European Commission, and similar national programmes. The programme should include a co-ordinated and multidisciplinary R&D approach to develop proper answers to the complex problems presented by infrastructures.

# Contributing Authors

V. Ajodhia	Technical University Delft, The Netherlands
I. Bouwmans	Technical University Delft, The Netherlands
M. De Bruijne	Technical University Delft, The Netherlands
H. De Jong	Technical University Delft, The Netherlands
L.J. De Vries	Technical University Delft, The Netherlands
G. Dondossola	Centro Elettrotecnico Sperimentale Italiano, Milan, Italy
M. Dunn	Swiss Federal Institute of Technology Zurich, Switzerland
A.V. Gheorghe	Swiss Federal Institute of Technology Zurich, Switzerland
H. Glavitsch	Swiss Federal Institute of Technology Zurich, Switzerland
R.A. Hakvoort	Technical University Delft, The Netherlands
H. Knops	Technical University Delft, The Netherlands
C. Kuenzi	International Risk Governance Council, Geneva, Switzerland
M. Masera	Joint Research Centre, European Commission, Ispra, Italy
M. Sajeva	Joint Research Centre, European Commission, Ispra, Italy
M. Schläpfer	Swiss Federal Institute of Technology Zurich, Switzerland
A. Stefanini	Joint Research Centre, European Commission, Ispra, Italy
D. Vamanu	Horia Hulubei National Institute of Physics and Nuclear Engineering, Bucharest, Romania
M.P.C. Weijnen	Technical University Delft, The Netherlands
I. Wigert	Swiss Federal Institute of Technology Zurich, Switzerland
Y. Wijnia	Technical University Delft, The Netherlands

## ACKNOWLEDGEMENTS

This document has had a complicated history, due not only to the diversity of authors collaborating on a common effort but also to the essentially emergent nature of the subject of risk governance and to the shifting emphasis of the variety and breadth of the many issues that comprise the field of critical infrastructures.

The authors wish to express sincere gratitude to Professor *Wolfgang Kröger*, Director of the Laboratory for Safety Analysis at the Swiss Federal Institute of Technology in Zurich, for his continuous and substantive support throughout the development of this project. Professor Kröger has provided continuous advice, encouragement and criticism to us, and is also responsible for encouraging the active interest of the International Risk Governance Council (IRGC), of which he is Founding Rector and Vice-President.

The editors and authors also wish to thank Professor *Granger Morgan*, Lord Chair Professor of Engineering and Head of the Department of Engineering and Public Policy at Carnegie Mellon University, for his constant interest and support in guiding the study and for his contribution to the detailed review process which provided the authors with considerable guidance in the completion of their work. Professor Morgan chairs the IRGC's Scientific and Technical Council, and we are extremely appreciative of the constructive advice and comments received from all the members of that body.

We also wish to express our thanks to the IRGC's Board and its President, *José Mariano Gago*, for their support and assistance to the authors.

The authors are deeply indebted to all those who, in the various stages of the development of the manuscript, have provided valuable suggestions for improvements to the text and have enhanced the practical relevance of the work and helped to propel the project towards its conclusion. We wish, in particular, to acknowledge the very considerable contributions of *Jean-Marie Cadiou*, Director of the Institute for the Protection and Security of the Citizen at the European Commission's Joint Research Centre in Ispra, Italy, and *Martin Fuchs*, President of the Union for the Co-ordination of Transmission of Electricity.

We thank all those who have helped and supported our work in writing this book, in which the opinions expressed and the conclusions drawn are entirely those of the authors.

# Chapter 1

## Introduction

*Adrian Gheorghe, Margot Weijnen, Marcelo Masera, Ivo Bouwmans*

### 1.1 Scope

This book examines the European electric power system as a specific critical infrastructure, which has experienced profound transformations during the last years and is subject to new risks. The nature of the transformations and the character of the risks demand a proper answer due to the central role of electric power in our societies. Traditional approaches, from risk management to emergency preparedness, fall short of providing adequate solutions.

This book, addressing policy and business decision makers, attempts to trigger a discussion on the suitability of risk governance. By risk governance is understood a risk decision making process where there is no privileged actor (not even governments) able to define and deal with the situation.

Governance “describes structures and processes for collective decision making involving governmental and non-governmental actors (Nye and Donahue 2000). As the operation of the electricity infrastructure is in the hands of private actors, and governments have the responsibility of overseeing the security of society, risks with a wide impact have to be handled by their joint effort. In Europe this situation is further complicated by the need to harmonize a great number of countries. Some of them are members of the European Union and share common rules; others (e.g. Switzerland, Norway) are part of the infrastructure, with specific legal arrangements.

The book concludes with the proposal to set up an apposite institution to facilitate the needed risk governance process, the European Council for the Security of Electric Power (ECSEP) and suggests supporting it with three other initiatives: the fostering of a European-wide public-private

partnership focused on security and risks issues, the adoption of active policies for the promotion of innovative security services and technologies, and the organisation of a multidisciplinary R&D programme dedicated to the security of infrastructures. These recommendations are discussed in detail in Chapter 5.

The following chapters endeavour to identify the driving factors shaping the evolution of the European electric power system: the *liberalization* of the power markets, the *internationalisation* of the electricity interconnections and flows, the *evolutionary unsuitability* determined by the intensive use of the infrastructure in ways for which it was not initially designed for, and the emergence of a new paradigm (called *E+I* here) originated by the ubiquitous application of information and communication technologies.

The key questions addressed in this book are:

- Which are the driving trends shaping the European electric power infrastructure, and what are the related risks?
- What appropriate approach to deal with this situation can be conceived?

## 1.2 Infrastructures, Risks and Society

The welfare of our societies has come to rely upon many infrastructures. It is hard to think of an economic or societal activity that does not depend on infrastructure-related services, such as electricity and water supply, transportation, information and communication technology, health emergency response and others. A long record of effective operation has caused Western societies to take the availability of such services for granted. Moreover, while infrastructural systems have shown to be considerably trustworthy, they have failed in the past and may still fail in the future. The complexity of infrastructures has grown to overwhelming levels, making it more difficult to understand the potential causes and consequences of failures. Furthermore, as infrastructure-related services pervade economy and society, the severity of potential failures increases.

The ever-accelerated geographical expansion of the energy, transportation, and telecommunications infrastructures has resulted in the emergence of enormous networks that transcend national borders and even

continental shores. The multitude and variety of nodes and links in these networks, and of the operations and services deployed, as well as the hosts of owners, operators, suppliers and users involved, have created enormously convoluted constructs. The intricacy of infrastructures limits the understanding of their behaviour and, consequently, the options to effectively control and steer the processes involved. There is an urgent need to generate more systematic knowledge on these complex systems, if one is to succeed in adequately handling the many threats and vulnerabilities.

Current trends, such as the *liberalization* of the markets, the *internationalization* processes that stimulate the cross-national interconnection of infrastructures, and the widespread access to telecommunication networks (e.g. the Internet), are enhancing the security requirements on the infrastructures. A further compounding difficulty comes with the fact that, owing to historical and cultural reasons, different countries have different, if not conflicting, perceptions on the relative value of profit versus risks and vulnerability.

Recent events, most notably a number of malicious acts and large-scale blackouts, have contributed to a renewed awareness on the critical role of infrastructures in Western economies. A growing request for security has prompted decision makers and analysts to review the mechanisms to ensure the normal behaviour and performance of infrastructures. In particular, an intensified interdependency of the energy, transportation, and telecommunication infrastructures prompts the need for an intersectoral approach.

The consequences of service interruptions, even of short duration, have become potentially huge, in both financial and societal terms. Substantial losses may occur, along with severe environmental, health, and life impairment. In the long run even more serious problems may arise. In a liberalized market, the economic incentives for owners and operators of electricity facilities are difficult to assess. Investing in capital-intensive installations and networks is an increasingly troublesome issue. While over-investment under volatile financial and primary fuel markets may prove a deadly option for business actors, a prolonged under-investment may result in an unreliable energy supply for society. Similar problems may arise in other sectors, which, due to the increasing interdependence of the infrastructures, may have repercussions on the energy supply system.

A thorough understanding of how infrastructures are evolving is crucial for making sound intra-, and inter-sectoral policies, which should ensure the ultimate goal: their efficient *and* secure *and* safe functioning. By

exercising a risk-oriented thinking, this book aims at outlining the need for a proper governance process.

### 1.3 Definitions

In our view, an **infrastructure** is a socio-technical system-of-systems that delivers a vital service, and in which something (e.g., goods, information, etc.) is transferred between the nodes of the system. The nodes, together with the links among them, form a network. An infrastructure includes all the elements required for its functioning: subsystems, as well as the governance, management and control processes.

System-of-systems have been described as meta-systems that “are themselves comprised of multiple autonomous embedded complex systems that can be diverse in technology, context, operation, geography and conceptual frame.”<sup>1</sup> In a system-of-systems infrastructure (i) the overall structure escapes the control of any single actor, and (ii) the different sub-systems evolve autonomously.

As regards the focus of this book, the electricity infrastructure includes the physical components such as wires, transformers and capacitors, as well as energy companies, regulators, traders and consumers, the energy market, and the grid codes.

#### Defining Infrastructure

In the tongue of its realm of origin – the Western industrialized world, ‘infrastructure’ refers to basic services that include, *inter alia*, transportation (roads, railways, airports, water navigation canals etc.), utilities (power plants, transmission and distribution grids, oil, gas and derivatives pipelines, water supply systems, sewers, telephone etc.), municipal services (e.g. police, fire departments, garbage collection), some key civil installations (e.g. important bridges, dams), health related services; and the list stays essentially open.

<sup>1</sup> Keating, C., Rogers, R. Unal, R., Dryer, D., Sousa-Poza, A., Safford, R., Peterson, W. and Rabadi, G., “System of Systems Engineering,” *Engineering Management Journal*, Vol. 15, No. 3, Sep. 2003, pp. 36-45.



American Heritage Dictionary:

*“The basic facilities, devices, and installations needed for the functioning of a community or society, such as transportation and communication systems, water and power lines, and public institutions including schools, post offices, and prisons.”*<sup>2</sup>

Executive Order 13010<sup>3</sup> presidentially- signed July 15, 1996 defines “infrastructure” as:

*“The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security ..., the smooth functioning of government at all levels, and society as a whole”.*

What makes an infrastructure *critical*? The notion of criticality relates to the potential risks and depends on several factors, as for instance the standpoints of the different stakeholders.

Infrastructures are critical because they provide services that are *vital to one or more broad governmental or societal functions or attributes*. This can be related to the survivability of the citizens as far as the safety of their life is concerned, or to their quality of life.

### **Defining Critical Infrastructure**

An early version of a U.S. National Plan for Critical Infrastructures<sup>4</sup> (PDD-63) states that :

*“critical infrastructures as those systems and assets – both physical and cyber – so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security, and/or national public health and safety”.*

In the last decade the criteria for rating a service or a facility as a critical infrastructure have evolved<sup>5</sup>. The *concept* of critical

<sup>2</sup> The American Heritage Dictionary of the English Language, Fourth Edition, Houghton Mifflin Company. Boston, MA. 2000

<sup>3</sup> Executive Order 13010 – Critical Infrastructures, Federal Register, July 17, 1996, Vol. 61, no. 138, pp. 37347 - 37350

<sup>4</sup> PDD-63 – “Defining America’s Cyberspace: National Plan for Information Systems Protection”, Version 1.0, An Invitation to a Dialogue, White House, 2000

<sup>5</sup> The US National Strategy for Homeland Security adopted in July 2002 listed the following critical infrastructure sectors: agriculture, food, water, public health,

infrastructures went from: “those structures whose prolonged disruption could cause significant military and economic dislocation”,

to – for instance:

“organizations or facilities of key importance to public interest whose failure or impairment could result in detrimental supply shortages, substantial disturbance to public order or similar dramatic impact” (see SSI, 2004), adopted in Europe by the German authorities.

It should be clear that there is no universally accepted definition of critical infrastructures. The only general rule seems to be that:

*The higher the developmental level of a society,  
the longer the list of its critical infrastructures,  
and the more severe the society’s dependence on them.*

Moreover, according to Moteff et al. (2003), “while the definition of critical infrastructures is broad and the number of infrastructures that are being considered critical has grown, limiting the number of infrastructures under study *a priori* might miss a dangerous vulnerability... [however a] priority of effort will be required.”

## **1.4 The European Electricity Infrastructure Today and Tomorrow**

### **1.4.1 Perceiving the risks today – problem statement**

During the 20<sup>th</sup> century, Europe developed diverse national electric power systems. The current electricity infrastructure has to serve about 400 million people, and a large variety of industrial customers, spread over many countries with different legal regimes and regulatory authorities. The last decades witnessed the increasing interconnection among systems, in a rather opportunistic fashion, with no central control mechanism and no

emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping.

shared, reliable data resource on which the many operators should base their decisions.

The last decade, following the European Directive 96/92/EC concerning common rules for the internal market in electricity, saw the emergence of continental space for the trading of power, which wasn't accompanied by a parallel increment in transmission capabilities. While the obstacles to cross-border trade were addressed by means of the definition and implementation of a set of common rules, the physical constraints to power transmission and the coordination among TSOs require conspicuous investments and rather long engineering processes. This situation opened opportunities for mismatches between market transactions and the underpinning technical systems.

The series of blackouts in the last 3 years (2003 in Northern America, Sweden/Denmark, London and Italy, 2004 in Greece, 2005 in Moscow) attracted considerable news coverage, though they were not without precedence<sup>6</sup>. The inquiries into the causes and consequences of blackouts and other near misses, have heightened concerns at all levels of society regarding the stability of the electric power system and the potential crippling effects onto other vital systems.

Such concerns follow from the evidence that the assumption of a continuous supply of electricity cannot be taken for granted. That assumption stemmed from many years in which the nationally designed, built and operated electricity grids were sufficiently fit for their purpose and robust to satisfy the ever-increasing demanded electricity. Many factors, both technical and socio-economic in nature, have caused the system to become increasingly fragile: for instance, ageing installations, market pressures on operators, intensive use of open communication networks. These points are developed in more detail in the following chapters.

<sup>6</sup> There are an estimated 300 smaller-scale incidents annually in Europe alone.

### **Is the current power infrastructure suitable?**

There is a general impression that European power systems might fall short of the performance requirements expected for the next years. This needs to be matched by adequate technical measures.

Technical weaknesses have more to do with the ageing of the generation and transmission equipment, than with the systems being used for purposes beyond their design basis, such as the large-scale cross-border transmission of electricity, characterised by congested electricity flows.

In Europe, the use of inter-connectors to enable power flow from exporting countries to importers has allowed some countries to refrain from investing in generation capacity, or even give up some existing national generation capacities.

There are also doubts regarding the ability of current and planned generation plants to meet demand. As an example, the growing reliance on gas-fired plants will face the need to find alternative sources when gas supplies would become scarce. In addition the availability of renewable sources is already known to be erratic, for instance the randomness of sunshine and wind.

Figure 1.1 shows the complexity and interdependencies of the current electricity infrastructure. The industrial and market actors that compose the infrastructure are shown. They provide an energy service to the end users, complemented more and more by information. The electricity infrastructure interacts with the information and communication infrastructure for various purposes: remote control of installations, emergencies, maintenance of equipment, logistics, market operations, etc. Moreover, there are continuous interconnections with other infrastructures – such as transport systems for the supply of fuels and raw materials. The figure also illustrates that both the infrastructure and the interactions are subject to vulnerabilities and threats, of both physical and cyber nature.

The exposure to this variety of hazards brings about risks that are difficult to comprehend because of the large number of potentially combined factors that could concur in each scenario. The control of all those risks is getting beyond the capabilities of any single actor – and as a matter of fact of any single country. This pattern is common to all types of infrastructures.

This awareness about potential risks emphasises the need to be reassured that the electric power system can meet the growing requirement for uninterrupted electricity supply. Several significant questions have to be answered:

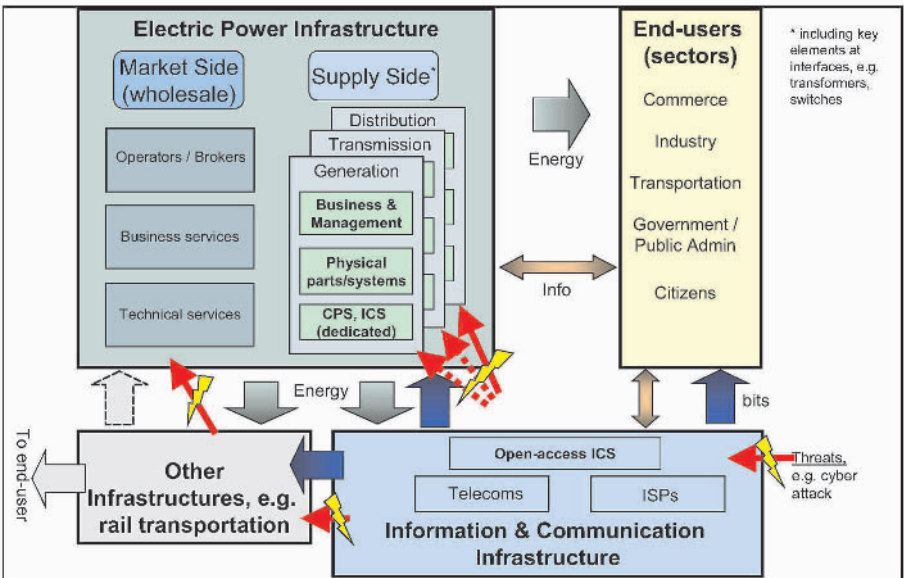


Figure 1.1. Critical Infrastructures: complexity and interdependencies (attributed to W. Kröger)

- which is the security level, against all possible hazards, that is at the same time tolerable for society, aimed by governments and affordable for industry;
- which level of capital investment and technological development is adequate for contrasting those risks;
- how to take into consideration the interests of the multiple industrial actors (generation, transmission and distribution companies), market actors, and other stakeholders, in the context

of environmental and safety norms and the obligations of a public service;

- which are the means and ways by which the risk-related decisions will be made.

### **Emerging weaknesses**

The increased use of open access information and communication systems over the past decade, particularly in enabling automated sensors and remote control of some key facilities, has offered new functional capabilities, but has introduced an additional potential vulnerability by increasing the risk of malicious attacks.

A series of socio-economic weaknesses has emerged from the liberalisation and privatisation process:

- \* conflicts of interests among industrial actors as a consequence of the fracturing of the original ownership and control structure;
- \* the reduction of profitability within the generation and transmission segments of the system; and
- \* conflicts between national regulators and the generators and grid operators on tariffs and public service norms.

### **1.4.2 The European Union policy context**

European policies on electricity began to consider the infrastructural dimension in the late 1980s, in parallel with the ongoing debate around the European Single Market. The legislative basis for this was established between 1985 and 1993. The notion of Trans-European Networks (TEN) was established as a needed complement to the measures paving the way to free trade and free movement within the European Union. At that time, the infrastructural issues were mainly posed in terms of economic growth and employment generation. Current TEN policies promote the interconnection and interoperability between national systems, as well as their universal access.

As far as electricity is concerned, the regulatory framework for the internal market was set in the Directive 96/92/EC, adopted in December 1996. The Directive established common rules for the generation, transmission and distribution of electricity. For instance, the procedures for the construction of new generation capacities were specified. Nevertheless, it also recognized that the operators of the electricity infrastructure had public service obligations, which had to be appropriately defined by the Member States in accordance to Community legislation. These obligations were considered as instruments for balancing fair competition with the nature of a public service and the general interests of society. Examples of such obligations were the requirement to supply all customers in a given area at an equal price.

In the said directive, the safety and security of the electricity system were mentioned (along with the protection of the environment, land use and siting, use of public ground, energy efficiency, the nature of primary sources) as variables to be considered in the authorization of new installations. In addition, the role of the national or regional transmission system operators (TSO) was confirmed, as responsible for dispatching the generating installations in their area of reference, and for determining the use of interconnections with other systems.

More recently, the Electricity Directive 2003/54/EC was issued, establishing common rules for the generation, transmission, distribution and supply of electricity. In this document, security is accepted as having two meanings: security of supply and provision of electricity, and technical safety. With the second meaning, a reference is made to potential incidents that would require safeguard measures (“...where the physical safety or security of persons, apparatus or installations or system integrity is threatened”). However, there is no reference to the critical aspects of the electricity infrastructure, apart from the conventional recognition of the need for security of supply.

The main political thrust still seems to focus on the openness of the market (so that in the near future, allegedly, consumers be free to choose their electricity supplier), on the efficiency of the transmission network, and on possible improvements in the market operations. The norms for the implementation of the directive emphasise the need to ensure the security of supply, for instance when treating the role of national regulators and the public service obligations.

A specific note on “Measures to Secure Electricity Supply” accompanies the Directive. There the security of supply is defended as a “public good”, and therefore one that deserves universal access. An implicit objective seems to be to increase the standards of service for customers. In the following discussion, almost all points are related to market issues such as: the tendering for new capacity, reliability contracts, and capacity subscriptions, etc. It is mentioned that the security of supply should include harmonized network security standards.

The Directive has been accompanied by the Regulation 1228/2003/EEC on cross-border trade in electricity, which sets rules for transmission of electricity between the EU Member States. It became effective July the 1<sup>st</sup> 2004, and stands for a directly applicable Community law. It regulates tariffs and congestion management.

The Regulation also states the need to provide information on interconnection capacities, by means of coordination and information exchange mechanisms that ensure the security of the networks in the context of congestion management, but no direct mentioning of contingencies is made.

In addition to these legislative measures the Florence Forum has been established, where all stakeholders (national regulatory authorities, Member States, European Commission, transmission system operators, electricity traders, consumers, network users, and power exchanges ) meet regularly to discuss the situation and potential improvements in the electricity market. After the inception meeting in 1998, ten other meetings have dealt with cross-border issues in the electricity trade, in particular the exchange tariffs and the management of scarce interconnection capacity.

During the meeting of September 2004, UCTE presented their *Operation Handbook* (partially issued beginning 2005). Important points there were the defence of the binding nature and legal enforceability that the Operation Handbook, as a set of security and reliability standards, should have. UCTE stated that the “Operation Handbook is the cornerstone for the legal framework ensuring the security of the interconnected systems”.

Apart from the factual information, the above is an indication as to the complexity of the problem, partly relating to the large number of actors engaged in securing the supply of electricity: national governments and other public authorities, regulators, transmission and distribution system operators, generators and suppliers of fuels. This requires an unambiguous determination of responsibilities, and a clarification of the relationship between the binding nature of some rules on the one hand, and the



competitive aspects of the market, on the other hand. The situation will also benefit from some meaningful harmonization of practices and normative rules between different countries.

At the same time, any assessment of the European situation with respect to the security of supply will have to develop a truly comprehensive view, including EU and non-EU members, neighbouring countries, and all kinds of threats that might jeopardize supply security. It seems that the concepts related to security have still to be unequivocally defined, and accepted by all stakeholders. In the end, the technical perspective on the problem cannot be dissociated from the framework defined by the market and the law, and from the nature of the prevailing risks, including cyber risks, and man-induced and natural hazards.

This comprehensive approach to security is noticeable in the proposal for a directive *“Concerning measures to safeguard security of electricity supply and infrastructure investment”* (European Commission, 2003). There it is recognised that investment is fundamental for electricity supply security and sustainability, that *“In a number of cases, the security of supply issue goes beyond national borders and requires careful co-ordination between the Member States concerned”*, and that *“A second consideration is that Member States need to adopt policies relating to security of supply which are reasonably consistent with each other”*. It is also acknowledged that there could be the temptation for some Member States or operators to adopt a “free ride” attitude towards the security of supply, relying on measures taken by the others.

The security of the power network is left to the Member States, who should set minimum standards, and it is accepted that *“Control of these critical energy infrastructures is, in turn, highly dependent on the security and reliability of the monitoring and controlling ICT infrastructures”*.

### 1.4.3 The advent of ECEI

The situation of electric power systems in Europe was radically altered by the succession of policy initiatives discussed above. These policies triggered a transformation process, still not fully developed, characterised by:

- Conversion from vertically integrated monopolies, towards a market-oriented solution to power generation and distribution, the definition of more independent transmission operators, and

the constitution of power exchanges and national regulatory bodies;

- Harmonization of the legal and normative regimes among countries;
- Recognition of the internal and external dimensions of the security of energy supply: internally, referring to the balance of environmental, consumer, safety, political and economic aspects; externally, acknowledging the dependence on adequate and suitable fuel supplies.

The evolution of the European power systems is going in the direction of progress in the multiplication of industrial and market actors, more installed distribution and generation capacity for satisfying the demand, and further interconnections within the current infrastructure and with neighbouring zones (e.g. North Africa, Middle East, CIS countries). For instance, with the Directive on Electricity Infrastructure and Security of Supply of 13 December 2003 the European Union and its Member States have decided to provide incentives to the market forces for increasing the investment in electric power installations.

Some policy decisions might also change the technical characteristics of the power grid: the Directive on electricity production from renewable sources, adopted in 2001, calls for increasing the production from renewable energy sources by 2010 to 22% of the electricity consumed in the European Union; the situation of nuclear power stations might change in light of concerns about global warming and commitments about greenhouse emissions; increments in trade (only 8% of production in 2002) will need the construction of many more interconnection lines.

This passage from the original situation to the future scenario foreseen by the European Directives, entails three main transitions levels:

- Countries: which have to implement changes in the legal regimes, the regulatory and market institutions, the rules for connection to the grid, etc.
- Companies: which have to adjust to the new situation by modifying their organisation, business processes, investment, pricing and marketing strategies, safety and security policies, etc.

- The infrastructure itself as a whole, with its overall service capabilities, operational rules, security principles, interconnection tariffs, congestion management.

This transition process is bringing forward a new construct, with its specific features and behaviour: the *European Critical Electricity Infrastructure (ECEI)*.

This infrastructure, a new and advanced socio-technical artefact, is making itself visible in a progressive way. It tends to function as a unity, although it embeds several jurisdictions, operators and markets. It derives from the interconnection of national and regional systems, but at the same time it behaves as a single, compound system-of-systems. It is decentralized; still disturbances can propagate all through it, and risks have to be coped with in a coordinated way.

The passage from a set of electricity systems to the ECEI is not just a question of more interconnections or more industrial actors - it represents a qualitative leap. ECEI, an infrastructural system-of-systems, is intrinsically different from a set of weakly connected power systems, where energy flows among different systems are marginal, and local operation and control are sufficient for managing the generation and supply objectives.

The following picture outlines the evolution from national electric power systems (EPS) to their embedding ECEI (see Figure 1.2).

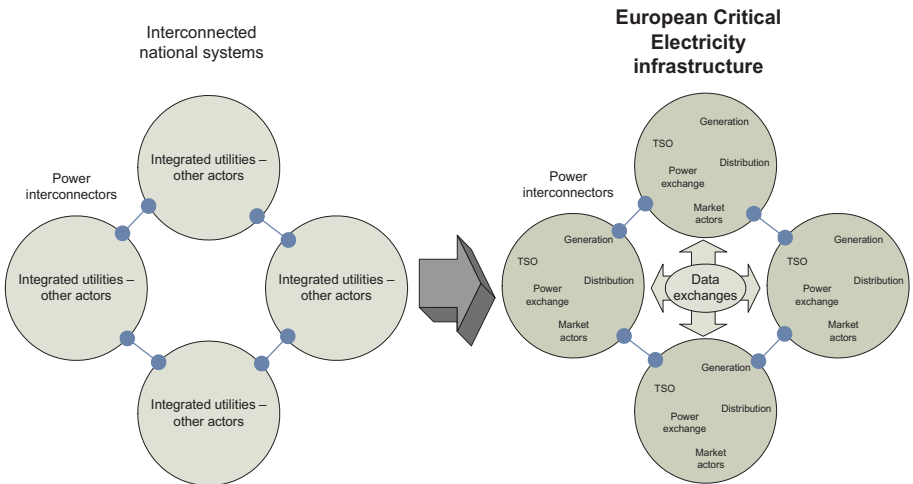


Figure 1.2. Evolution from national power systems to ECEI structure

The Union for the Co-ordination of Transmission of Electricity (UCTE) estimates that after 2008 a significant decrease in generation margins may lead to a more unreliable system. Some important questions are still open to be answered.

Can we expect the future "network of networks" to be totally self-regulating, with no rules by government? On the one hand, the more complex and advanced any network system becomes, the less one can guide it centrally. On the other hand, diversity does not assure optimality when different participants pursue different strategies and private and public objectives diverge. Some traditional subjects of regulation, such as price and entry controls will become unnecessary. But issues involving free flow of information, interconnectivity, universality of service, and international asymmetry will not vanish with competition. Thus, rules and regulations will change, but not disappear entirely.

Of a speculative concern, yet difficult to dismiss, is the fact that, in the absence of a concerted effort to alleviate weaknesses within the system, the assumed paradigm of assured operability might be replaced by one in which the supply is rationed. This would be the ultimate test of political will on behalf of the governance factors, and would also require the participation in decision making of the users themselves to an unprecedented level. The conundrum would then consist in either agreeing to rations, or open purses as investors in alternative supplies (discrete, distributed generation capacity to assure survivability and reduce recovery times), so that some resilience be eventually built back into the system.

The EU and Russia have recently agreed to connect their electricity grids by 2007; while Russia has recently announced plans to liberalize its electricity market. Although the potential benefits of such a historical decision can only be saluted, special care should also be exercised to properly meet the technical challenges entailed by the dramatically enhanced expanses to be covered, the compatibility issues and additional, including unforeseen stresses on the overall mega-system.

## **1.5 Background and Structure of this Book**

### **1.5.1 Intended audience**

The intended audience of this book is composed of those policy and business decision makers concerned with the risks jeopardising the

European Critical Electricity Infrastructure. In addition, we hope that the reflections expounded in the present text will serve as background material also to those in charge of designing and developing other critical infrastructures.

Our chief ambitions are to raise awareness on the nature and urgency of the problem, and to offer a framework enabling those responsible for the regulation and operation of the European electric power systems to ensure the adequate and safe supply of electricity.

There are many individuals and organisations sharing this responsibility. None of them can be ignored when making risk-related decisions. The long list of stakeholders includes:

- governments (as the bodies holding the ultimate responsibility for the overall energy policy, but also as owners and operators of power systems in some countries),
- generation, transmission and distribution companies (as owners and operators and as the primary source of investment),
- independent regulators (whose influence can encourage or hinder certain key behaviours, including investment),
- power exchange operators and actors;
- suppliers of electric power equipment and services;
- sector and professional associations; and, not the least,
- end users.

Moreover, the authors would be keen on attracting the attention of researchers and educators. The future of the critical infrastructures field is highly dependent on the solutions and knowledge eventually produced by them.

### 1.5.2 Structure of chapters

*Chapter Two* presents several generic models of critical infrastructures (technical-physical systems in interaction with socio-economic systems, taking into account physical transactions vs. business transactions), characterized by different levels of complexity. Critical infrastructures are seen as *systems of systems*.

*Chapter Three* describes two of the main trends in the European power system: liberalisation and internationalisation. To understand these trends and their consequences, a significant part of the chapter is devoted to developing a structural analysis of, first, the structure of an individual electric power system and, second, how the European system of connected

electric power systems is organised and functions. Special attention is paid to the challenges to system security in the new environment.

*Chapter Four* considers the interaction and interdependencies between information and communication systems and the electric power systems, their vulnerabilities and needs for new governance solutions.

*Chapter Five* discusses several potential solutions aiming at a better management of the risks and vulnerabilities of the European electricity infrastructure, from a risk governance perspective, and propounds the institution of a dedicated body, the European Council for the Security of Electric Power.

*Chapter Six* reports recommendations on policy measures that will foster the governance of risks and the increase the security of the European Critical Electricity Infrastructure.

The *Glossary* includes a list of specific terms used in the context.

The *References*, listed for the whole book, are supportive to the arguments exposed throughout.

## Chapter 2

# Infrastructures at Risk

*Ivo Bouwmans, Margot P.C. Weijnen, Adrian Gheorghe*

### 2.1 Introduction

Rapid developments in recent years have led to drastic changes in the way we think about and deal with infrastructures. EU directives called for deregulation of the networked utility infrastructures so that EU common markets could be formed in order to strengthen the EU economy and to achieve a more efficient and high quality service provision. The ensuing liberalisation and internationalisation of the utility sectors affect not only the market structure, but also the physical networks themselves in unprecedented ways.

At the same time, the trend of increasing interconnectedness between infrastructures causes new vulnerabilities, as changes or failures in one infrastructure may affect other infrastructures as well. Targeted attacks by groups or individuals on vital points in some infrastructures could cripple the entire system of interconnected infrastructures. It is questionable whether the new complexities that arise as the consequence of infrastructure interconnectedness across both national borders and sectoral borders can be adequately handled by the regimes of national and sectoral regulation. In this chapter we will therefore attempt to unravel the complexity of infrastructure systems from a generic perspective in order to identify the strategies and tactics available for handling infrastructure complexity with a view to vulnerability and risk governance. We will discuss the consequences of these developments for the networked utility infrastructure systems and the way they could or should be designed and managed.

The crucial role of networked utility infrastructures as the backbone of the economy is reflected in the fact that the damages incurred to society in case of infrastructure failure may amount to higher orders of magnitude

than the direct value of “lost load” or service not provided. In other words, the networked utility infrastructures are critical for modern society. As the networked infrastructures enable virtually all economic activity, the security and affordability of infrastructure bound services are conditions for economic productivity and growth. On the longer term, smooth functioning infrastructures are an important asset for the investment climate.

In analysing these critical infrastructures, one has to understand and assess the relevance of the various categories of potential failures, namely those related to hardware, software and human organisation. The weaknesses in the system’s design and operations can be evaluated, identifying the potential initiating events – such as malicious attacks on individual or combined critical infrastructures, or accidents deriving from natural causes or internal faults, identifying and describing specific threats e.g. cyber threats. This leads to insight in how to categorize them individually, as well as collectively, addressing issues of vulnerability of such systems, their degree of resilience and survivability at the confluence with failure or system’s dependence, and identifying ways of harmonising procedures that should address interests of worldwide significance in a format that allows co-operation at international and trans-sectoral levels.

## **2.2 A Generic Approach to Critical Infrastructures**

Recent developments in the thinking about complex systems give insight in how infrastructures cohere and behave as systems. In this section a systematic approach is presented for the analysis of infrastructures and the way complexity manifests itself in them. The constituting parts of the networks – the physical network and the actor network – are shown in their mutual relation. The increasing interrelation between infrastructures adds to the complexity.

### **2.2.1 Physical network complexity**

The physical networks of the infrastructures are huge systems composed of a multitude of nodes and links. The effect of the number of nodes seems quite obvious: the more nodes, the more complex the system will appear. These nodes are generally not ‘passive’, but they interact with and adapt themselves to their surroundings. Their reaction to external changes is often non-linear, which can result in unpredictable behaviour of the system as a whole. Chaos is one possible form of such unpredictable



behaviour. Chaos theory tells us that even if we knew the differential equations that accurately describe the changes in the nodes, our prediction of the state of the system would gradually diverge from its actual state, due to the exponential growth of tiny errors in our measurement of the present state. Chaos theory can, however, give us insight into the general behaviour of the system and the system states that can be expected.

Emergent behaviour, which is the behaviour of the system seen as a whole, follows from the behaviour of the agents at the lowest level as they interact with each other. This emergent behaviour can be much more difficult to describe than the actions of the individual agents at the lowest level. In other cases, however, emergent behaviour may be simpler to describe than the combined behaviour of the individual agents, as in the case of ants that have rules to follow pheromone trails set by other ants. The system behaviour is that all ants eventually follow the shortest route from the ant nest to the food supply.

This illustrates that we can model emergent behaviour without modelling the behaviour at lower levels of the system or at the level of its components. For the users of infrastructure bound services, it is only the performance at the top level, the level of the overall system, that counts.

### **2.2.2 Social network complexity**

The social network, or actor network, consists of all entities – people, institutions, companies – that have a relation with the infrastructure under consideration (see Figure 2.1). As in the case of a node in the physical network, each actor in the social infrastructure network can be described as an agent that acts according to a set of rules. In the social network, the rules are determined by legislation and regulation, business economics, economic regulation, moral and cultural codes, etc.

In addition to the externally imposed implicit and explicit rules, each agent will have its own strategy. In the case of, e.g., a driver on the motorway, behavioural psychology may shed light on the determinants of individual driver behaviour. If the agent is a company, business economics and strategy will influence its behaviour. An incumbent company may drop prices in order to keep new entrants from the market, whereas a new entrant may lobby for tighter restrictions on incumbent behaviour.

Agents also show learning behaviour: when faced with a similar situation for a second time, their behaviour will be influenced by the lessons drawn from the first time.

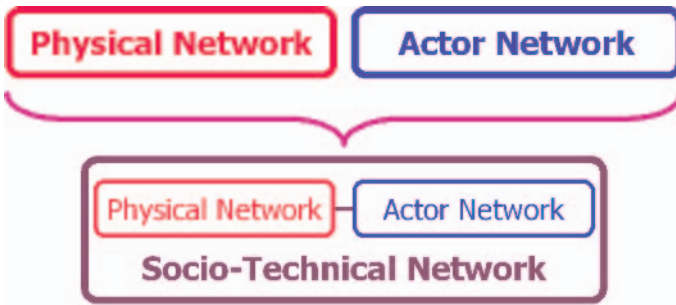


Figure 2.1. Infrastructures as socio-technical networks

So, in infrastructures, not only the physical network but also the social network poses a serious challenge to those who try to understand the behaviour of the system. This challenge may even be more difficult, given the often irrational behaviour of the actors. As in physical infrastructure networks, much of our insight in the functioning of social infrastructure networks is gained from studying and modelling emergent behaviour. In many cases, in both physical and social networks, emergent behaviour can be described by new rules at higher levels of aggregation, disregarding the actions at the lowest level of the agents. Usually, the end users of the services generated by infrastructure systems are only interested in the system performance at the top level, such as the security and quality of service, and its affordability.

Together, the physical network and the actor network combine to form the socio-technical network: one system, where the individual parts are mutually dependent. Changes in either of the subsystems inhibit or enable developments in the other.

### 2.2.3 Network growth

Part of the problem with understanding the behaviour of infrastructures is that most of these systems were not designed as integrated systems, but gradually evolved over time. Most infrastructures originate from local networks. Over time, municipal networks evolved. In the Netherlands, for instance, city networks for electric lighting were established in the first decades of the 20th century. Interconnection of city networks and network expansion to rural areas were forged through intervention of the provincial authorities (Hesselmans, 1995). Provincial networks thus emerged in the first half of the 20th century. The national grid was not fully established until the second half. Over time, the density of end-user connections

increased. Transport functions in the infrastructure were intensified (increasing throughput) to serve a steadily increasing number of users and a steadily increasing demand per user. To improve the security of service, the national grid was interconnected across national borders. At the moment, most national grids in Europe are interconnected. In the course of about one century the system's dimensions have grown several orders of magnitude.

As illustrated by the case of electricity infrastructure evolution in the Netherlands, infrastructure networks generally do not grow randomly. New nodes added to the existing network are linked to specifically selected nodes. In the natural gas infrastructure, for instance, new urban areas will be connected to existing main pipes. In the world wide web, new pages usually link to pages that already have a large number of links to them. The advantage of such a "preferenced" or "associative" network is that the network becomes very robust against multiple failures of random nodes (Barabási, 2002). The disadvantage is that such a network is extremely vulnerable to targeted attacks. Eliminating just a few of the main hubs in the network may cause the network to become disconnected or stop functioning at all.

#### **2.2.4 Infrastructure interdependencies**

Last, but certainly not least, infrastructures are marked by growing interdependencies (schematically shown in Figure 2.2). In all critical infrastructures, advanced information systems are a necessity for the exchange of vital information on the status of subsystems between their operators, both within and across national borders, to maintain overall system stability. The critical information needs for adequate management of infrastructure capacity in the energy and transport infrastructure sectors and for the provision of added value entail an unprecedented dependency on the information and telecommunication infrastructure.

In general, two infrastructures are considered to be interdependent when each is critically dependent on the other – i.e. each one might fail due to failures in the other infrastructure. Interdependency is thus defined

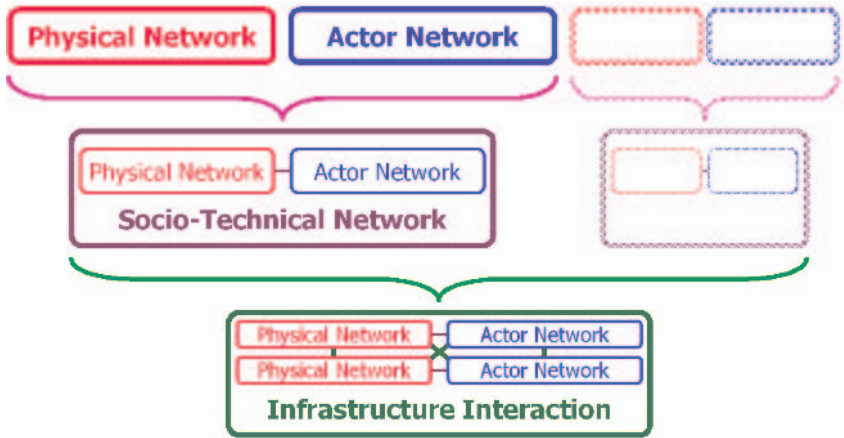


Figure 2.2. Interdependency between infrastructures

as a bi-directional relationship between two infrastructures, through which an unwanted hazardous state of one infrastructure is correlated with a hazardous state in the other. Interdependency among critical infrastructures should be the subject of specific assessments, such as an assessment of the degree of digitalization nested into the operation of an infrastructure. Analysis is also needed to assess the criticality of the flows of information crossing the interfaces between interdependent critical infrastructures. Interdependencies vary widely, and each has its own characteristics and effects on infrastructure agents. Among the various dimensions which characterise the interdependencies among critical infrastructures are: type of failure, state of operation, environment, coupling and response behaviour.

Infrastructures are interconnected not only across national borders and continents, but also across infrastructure sectors. The energy sector is increasingly vulnerable to disruptions in telecom and information services, and vice versa. Recent studies on Critical Infrastructure Protection have shown that many of these interconnections are poorly understood, even in the sectors themselves. Interconnection between infrastructures adds one more challenge to dealing with the complexity and vulnerability of infrastructures.

Other interconnections between infrastructure sectors are created by so-called convergence phenomena (Bauer et al., 2003):

- *Physical convergence* refers to the emergence of multi-functional infrastructures, which provide functions that used to be provided through different physical networks. Example: Internet services via power lines or via cable television infrastructure.

- *Organizational convergence* refers to the emergence of multi-utility firms, usually operating on the consumer market, selling combinations of utility services. Example: an integrated package of electricity, gas and drinking water services.

- *Market convergence* refers to the convergence of the markets for an infrastructure-related service that can be provided through different infrastructures. Example: Internet via telephone cable vs. Internet via cable tv or power lines.

- *Spatial convergence* refers to the physical clustering of different infrastructures in corridors or nodes. Example: glass fibre drawn through gas pipes or sewage lines.

The interconnections and the ensuing interdependencies between infrastructures have only recently been recognized as a priority area of technology and policy research. How do we allocate the risk management responsibilities in interconnected infrastructure systems? How do we prevent failures to cascade from one infrastructure to another? Within the EU institutions, security has captured attention in different forums, though mostly separately for each sector. A recent inter-sectoral initiative, originating from the European Council, asked for the preparation of an overall strategy to enhance the protection of critical infrastructures (Presidency conclusions of European Council, Brussels, 17-18 June 2004). So far, this initiative was geared towards the fight against terrorism. Therefore, it has resulted in measures in the areas of security and justice. It seems obvious, however, that any successful strategy to improve the security of critical infrastructures requires the key involvement of the transport, telecommunication and energy sectors.

### 2.2.5 Complexity and criticality

It is evident that simple systems are not complex. When, then, do systems that are getting ‘more complex’ become ‘complex’? There is no simple answer to this question. First of all, there is no universally accepted definition of ‘complexity’. But secondly, systems that have the potential to be ‘complex’ (by any formal definition we would adopt), do not necessarily show complex behaviour under all conditions.

For the analysis of infrastructure systems, however, the notion of ‘criticality’ as used in complexity theory is relevant: a system is ‘critical’

in this sense when a single local event can lead to effects that affect the system in its entirety (e.g. see Frigg, 2003). It should be borne in mind that this definition of a ‘critical system’ - as used in complex systems theories - is different from that used in the rest of this book, where it denotes a system that, when failing, would seriously disrupt society. The notion of ‘criticality’ is valuable, however, for it shows even more compellingly that the behaviour of systems can become unexpectedly difficult to understand as the systems expand and interact.

An example may be found in transport systems. Up to a certain number of cars per stretch of motorway no traffic jams are to be expected, apart from those caused by accidents. When the number exceeds the threshold for ‘criticality’, however, small disturbances in the traffic flow, even one as seemingly insignificant as a car driver lightly touching the brake, can trigger a traffic jam. Even in this simple example it would not be easy to predict the threshold. It is obvious that in the case of an entire infrastructure system it would be even more difficult, if not impossible, to do so.

## **2.3 Trends in Systems of Critical Infrastructures**

### **2.3.1 Trends in the socio-economic dimension of Critical Infrastructures**

As illustrated earlier, the evolution of infrastructures is not only a matter of technological innovation and physical network growth, but also entails a changing composition of the multi-actor network involved. During the evolution of the electricity infrastructure, the number of end-users has obviously increased dramatically. In the initial development stage, in the early 1900’s, the provision of the new service was only affordable for public authorities and a small number of wealthy consumers. After the technical feasibility and economic viability had been proven extensively, public authorities either took over from private firms, or established rules that enabled them to directly interfere with the planning, management and operation of the systems. Economies of scale by technological innovations and a growing sense of public utility value were the main drivers to implement interlocal connections and to expand the networks to rural areas. Universal access was generally made a requirement for utility companies, in addition to security and affordability of the public utility service.

Initially, local authorities used their mandate to grant permits and concessions to steer the development of new infrastructure. More often than not, authorities delayed the development of competing infrastructure if they had stakes in an established infrastructure. For example, in the Netherlands the development of the electricity infrastructure was initially postponed to protect the local city gas works, owned by the municipal authorities.

Until one or two decades ago, most critical infrastructures in Europe were still operated as public monopolies with direct or indirect government control of the implementation of infrastructure and the universal provision of the public utility service by some means of central planning and allocation of funds. This relatively transparent situation has changed considerably. Many infrastructures, in all EU Member States, have just completed or still are in the transition from a public monopoly structure to competitive markets. This transition does not affect the physical network directly, but mainly the social network. As a new playing field is defined, new actors enter, often in new roles. Foreign players, including players from outside Europe, have entered hitherto protected national markets. Traders and brokers have become active and power exchanges have been established. National regulators have been created to ensure non-discriminatory access to the transmission and distribution networks. Many of the physical assets have been privatised.

It will be evident that the social network has become much more complex with the larger number and diversity of actors, each of them with their own agenda. Options to steer the development of the infrastructure have changed dramatically. Whereas the old situation allowed the public authorities to directly intervene in the development of the system, investment signals for capacity expansion and innovation in generation—but not in networks—are established through market forces. The interaction between the physical and the social subsystem of a critical infrastructure is now, more than ever, shaped by legislation and regulation, especially by sector-specific regulation (*ex ante*) and by competition law (*ex post*).

It is clear that the development of Europe's Critical Infrastructures in the years ahead will occur in a context that is changing. As this change is touching all critical infrastructure sectors, we can speak of a paradigm shift (Ten Heuvelhof et al., 2004, on which the rest of this section is based; Figure 2.3 represents the two paradigms schematically).

- **The conventional paradigm**

The conventional paradigm is marked by the full vertical integration of activities in the infrastructure value chain. The fact that particular technological facilities (most notably the transport and distribution networks) have the character of a natural monopoly, combined with the assumption that decisions should lie with one actor, justifies this integration. In Europe, in contrast with the USA, the public monopoly model was generally preferred over the private monopoly model in view of the public interest goals at stake. Whether directly or indirectly, the Government controlled the realization of the infrastructure, as well as the public utility service provision functions by means of central planning and allocation of funds. Within this paradigm, infrastructures are a public monopoly by definition and a more efficient construction is unthinkable. The infrastructure and its technology dictate what happens in the production chain. The services provided on the infrastructure are seen as direct derivatives from the physical infrastructure. In this view, physical infrastructure operation and utility service provision are so strongly interwoven that they cannot be separated, even if only one segment of the production chain is a monopoly.

- **The new paradigm**

The new paradigm does not deny the existence of natural monopolies in infrastructures, but rejects the conclusion that infrastructure sectors should therefore be considered monopolies in their entirety. The new paradigm aims at improving service and reducing service costs by the introduction of competition wherever possible in the value chain. It does so by *unbundling* the value chain, so that non-monopoly segments (e.g. electrical power generation) can be opened up for competition. Even in infrastructures where a natural monopoly persists, as in the power transmission and distribution network, competition may be engineered either *on* the infrastructure (giving access to third parties who then compete for infrastructure capacity) or *for* the infrastructure (the regulator or network owner may periodically organize a competition in which parties try to win the exclusive right to operate the infrastructure for a certain period).

In the new paradigm, public interests can be ensured through adequate market design and network regulation (if the network retained its monopoly character), and additional legislation and regulation for safety, health, environment, etc. Unbundling, competition and private involvement should eventually lead to an improvement in efficiency, quality of service and transparency. On the other hand, it could be that by this decentralisation of decisions the outcome for the overall system is sub-



optimal, because it is merely an aggregation of partial solutions. The question is how to evaluate security in a system with reduced top-down control.

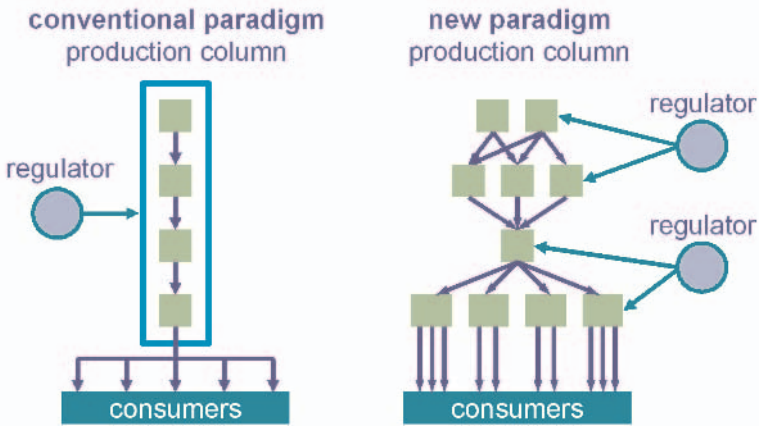


Figure 2.3. Conventional and new infrastructure paradigm

Through the liberalisation of the network utility sectors, the EU aims to establish effective competition in EU-wide internal markets, not only for gas and electricity (by 2007), but also for postal services (2006), rail transport (2008) and airspace. The High Level Group chaired by Wim Kok, which recently reported on how the EU should face the challenge of the Lisbon strategy for growth and employment (Kok, 2004), sees that “along with investment in R&D, completing the internal market is the key to boosting productivity and innovation”. The paradigm shift of liberalisation and unbundling is not a goal in itself, but a means to serve the goal of economic growth. If a competitive infrastructure-bound market behaves as a normal market according to economic theory, likely consequences of the new paradigm are a higher rate of innovation and a larger variety of technological innovations. While this may be desirable from the viewpoints of economic productivity and consumer choice, it also makes it more difficult to regulate and coordinate activities in the long production chains that now run across all infrastructures.

### 2.3.2 Technological innovation in Critical Infrastructures

The apparent stability of infrastructure sectors originated in the stability of their institutional context in terms of ownership structures and

legislative framework. Until recently, new business trends hardly touched the (public) utilities. Where private firms were forced to ensure their competitiveness in a globalizing economy, striving to become “leaner and meaner” through drastic business re-engineering, mergers, take-overs and strategic alliances, the utilities enjoyed a relatively protected status that allowed them to conduct business as usual. Of course, the capital intensity of the physical infrastructures and their embeddedness in the spatial and economic structure imply a certain degree of inertia. This is why many may not associate infrastructure with innovation. However, this observation is only correct from the end-user perspective. On the supply side of the infrastructure, capacity was enhanced and technological innovations were implemented to satisfy the increasing demand. The orientation towards innovation was almost purely technological, and the selection of innovations was largely determined by the established architecture of the infrastructures. Innovations leading to competition with the established infrastructure were not naturally stimulated.

Innovations leading to new infrastructures such as alternative communication systems were not unleashed until the markets for infrastructure-bound services were deregulated. A prominent result is the surge of new information and telecommunications systems. The new telecommunication and information systems enter the domain of the “old” infrastructures, where they enable more intelligent infrastructure operation and smarter capacity management. Equally remarkable is the ongoing change from universal provision of commodity services to the personalized provision of value added services tailored to the needs of end-users.

This makes clear that the technological innovations in infrastructures also involve institutional, organizational, legal and commercial change, and vice versa. It is also evident that innovation occurs in all segments of the production chain of infrastructural services. By way of example, Table 2.1 distinguishes three levels for three sectors. The levels identify the physical assets of the infrastructure, the management of the assets as networks, and the actual service provision to the end-user.

Innovations therefore not only concern the new technologies, but also new types of services – directly for end-users, but also for other parties at the network level and at the level of infrastructure elements. In contrast with the monopoly thinking of the conventional paradigm, the new

Table 2.1. Levels in infrastructure: examples

Sector \ Level	Electricity	Rail	Fixed telephony
<b>Service provision</b>	electricity supply	transport of people and goods	telephony
<b>Network management and operation</b>	balancing services, voltage support, repair services, system planning	station management, traffic control, emergency services, repair services	network configuration, repair services, system monitoring, security services
<b>Physical assets: nodes, links and their elements</b>	transmission lines, substations, power generators, circuit breakers	railway lines, carriages, stations, signalling equipment	wires and cables, exchanges, telephones, interconnections with other networks

paradigm stimulates innovations. In fact, many innovations are underway that may strengthen the functioning of our critical infrastructures. Relevant innovations in the way to combat threats are, for example, concerned with the introduction of new ‘holistic’ concepts considering the vulnerability of the system as a whole (Van Mieghem, 2005).

The change from technology push (in the monopoly culture) to service pull (in a competitive market environment) in infrastructure innovation, however, is most pronounced in the proliferation of service innovations. The tendency of the market towards service quality differentiation where possible, leads to a dependency of infrastructure service providers on information and consequently on information and telecommunication infrastructure.

Similarly, under the new paradigm the approach to infrastructure capacity planning has changed from a supply driven approach to a market driven approach. Whereas capacity planning under the old paradigm showed a tendency towards overinvestment in order to guarantee security of service, the natural tendency of the market may be towards slight underinvestment, as no private investor is willing to run the risk of investing in overcapacity for the public good (De Vries, 2004). Even public owners of networks and other infrastructure assets are, under the

new regulatory regimes, often subjected to tough economic efficiency performance criteria, which may cause them to refrain from investments in capacity expansion or innovation.

### 2.3.3 Public values of Critical Infrastructures

As mentioned before, the term critical infrastructures is mainly used to indicate the critical dependence of society on infrastructure-bound services. In other words, the services provided through our critical infrastructures are of high public value. In order to steer the processes of change and innovation towards social benefit, we need to understand the concept of public value, as it represents the objective function of infrastructure design, operation, management and development. The concept of public value adds to the complexity of infrastructure organisation, as it contains multiple objectives, which may change over time. We should therefore be able to identify the public values at stake, to arrive at a trade-off between conflicting public values, and to signal emerging public values.

Implicitly, quite a few public values associated with infrastructures have already been mentioned: universal access, affordability, security and safety are generally recognised as public values. End-users are annoyed when a power failure disrupts their business and daily life, when they get sky-high cell-phone bills, or when they face traffic congestion. Under the “old” paradigm of infrastructure organisation, when the critical infrastructures were still run as vertically integrated public monopolies, they had a right to blame the public authorities. In the new situation, however, it is not so clear which actor(s) can be held responsible. Many critical infrastructures are now run in a multi-actor network containing both private and public actors in a complex web of competitive, co-operative and co-ordinative relationships. Private players in this web tend to be interested in public values only if they generate a reasonable profit.

As certain values appear to be considered public in one country and private in another, we argue that public values cannot be defined objectively and unambiguously. For instance, in industrialized countries, access to the Internet gradually has become a public value, while in many underdeveloped countries, even access to safe drinking water or a telephone is a rare commodity. Apparently, the concept of public value changes with economic development and with the structure of the economy. In the past decades, we have become used to a steadily increasing security and quality of e.g. electric power and telecommunication services, and as a consequence, our activities have

become increasingly dependent on these higher performance levels. At the same time a clean and healthy natural environment, the protection of landscapes and biodiversity and other elements of sustainable development have emerged as new public values. More recently, privacy and security have come to be generally recognised as important public values. The vulnerability of the economy and society to malicious attacks has necessitated a new interpretation of security and safety as public values. These examples illustrate that the set of public values is dynamic.

The issue of safeguarding public values therefore requires a transparent analysis and decision making process in which the set of public values is identified and agreed upon, in which issues of conflicting public values are reconciled, and in which public values are translated into performance criteria that infrastructure designers and operators have to operationalise and that regulators have to enforce. In the new situation of infrastructure market liberalisation and public utility privatisation it is as yet unclear how this decision making process should be staged.

Who is to decide what is in the public interest and what is not, and on what grounds? Who is responsible for taking appropriate measures to safeguard these public values? And what measures should that be? Which organisational models are effective and how can all parties be involved or stimulated to cooperate? Will the market provide its own solutions? Given the dependence of society on critical infrastructure services, it is of the utmost importance that the European Commission and Member State governments design and control the emerging common markets for critical infrastructure-related services in such a way that they steer the collective actions of all actors towards the adequate safeguarding of public values, including security.

## **2.4 Risk and Vulnerability in Critical Infrastructures**

As illustrated above, there are several reasons why the traditional way of looking at risks and vulnerabilities in infrastructures does not suffice anymore.

External attacks on the infrastructure may target specific nodes in the network. Combined with the intrinsic vulnerability that networks that have grown in a non-random way show for targeted attacks, this could result in infrastructure system collapse. Therefore, it has become impossible to calculate failures on the basis of internal evaluation only.

The liberalisation and the internationalisation of the energy market have resulted in a much larger number of actors in the field, without

centralised planning and control. This seriously restricts collective decisions about long-term development of the infrastructure, which in turn may lead to problems in the daily operation.

Finally, the interdependency of infrastructures, particularly between the energy and information infrastructures, leads to a larger and more complicated risk of failures. Errors in one system may easily cause failures in the other system, triggering new failures in the first and eventually leading to systemic failures in both infrastructures.

An evaluation process of risks of the critical infrastructures is currently taking place in various countries and by international organizations; a context for this, is set by the recent OECD study on Emerging Systemic Risks (OECD, 2003). Critical infrastructures have recently been given high priority by the international community; at the national and international levels, risk governance is one of the major issues in assessing vital systems' operability in interaction with society.

### **2.4.1 Framing the risk governance questions**

There is an undeniable sense of urgency to place the security of infrastructure-bound services high on the political agenda. From the complex system perspective, there is also abundant reason to place this issue high on the agenda for research and innovation.

A clear understanding of the structural and dynamic complexity of infrastructure systems is indispensable. Both the social and engineering sciences should be urged to arrive at a fundamental understanding of the large-scale and time-dependent behaviour of critical infrastructures, their dynamic evolution, the diversity of links and relations between nodes and actors, as well as the diversity of nodes and actors themselves.

It is evident that many of the challenges and problems that are to be confronted in infrastructure risk governance are relatively new. The inherent system characteristics of new information infrastructures, especially, differ radically from those of traditional infrastructures in terms of scale, connectivity, and dependencies. Moreover, the interlinked aspects of market forces, technological innovation, and newly emerging threats are likely to aggravate the problems in critical information infrastructures in the future. This situation forces analysts to look ahead constantly and to develop new analytical techniques, methodologies, and mindsets.

The need for knowledge to ensure a better understanding, the need for innovation, and the need for policy action to safeguard the security of infrastructure become evident when we see that the annual societal damage caused by critical infrastructure malfunctioning is enormous. Although

reliable aggregate cost figures are missing, even a conservative estimate of known damages incurred by routine failures already amounts to over 5% of the EU-25 GDP (Ten Heuvelhof et al., 2004).

Consequently the following urgent policy questions can be identified:

- Which public value issues will be solved by the market, and which require governance?
- Have the Member States given the security of vital infrastructures the priority it needs to have?
- How can Member States improve the security of such vital services as electricity, internet, telephony, air traffic, and road transport? Is this necessary in all cases?
- Are the current – European, national and sectoral – market designs and regulatory frameworks capable of dealing with the new complexities of infrastructures?
- What technological and institutional innovations are needed to make infrastructures more intelligent, more flexible, more robust and more resilient?
- How can Member States stimulate private investment in innovative infrastructure development?
- What initiatives are needed at the European level?

#### **2.4.2 Critical Infrastructure complexity and the management of vulnerability**

It has become more difficult to ensure a high level of security or various critical infrastructures. Rather than being a product of individual organizations, highly reliable services are more and more the outcome of networks of organizations, many with competing goals and interests. This creates new challenges for effective market and network regulation, and new needs for communication and information sharing. The California electricity crisis could have been much worse than it was if the operators of the various subsystems had communicated less intensively (EPRI/PIER, 2002).

The overall demand for infrastructure services is increasing. At the same time, society demands ever higher security of service as we grow more dependent on infrastructure-bound services. Given the market tendency towards capacity scarcity, this poses new demands on infrastructure capacity management. Innovations are needed to use the available capacity better. Where central coordination mechanisms are missing due to the decentralisation of decision power, the infrastructures should be equipped with self-organizing and self-healing properties so as

to deal intelligently with disturbances and recover more effectively from incidents.

By lack of options to interfere directly in the development of the system, we can only ensure that the collective actions of players are steered towards safeguarding the public interests through adequate innovative market design, adequate network regulation (if the network retains its monopoly character) and additional legislation and regulation for safety, health, environment, etc. A specific challenge is to ensure that the design of markets and regulatory frameworks generate sufficient investment signals to stimulate private actors to timely invest in infrastructure development and innovation.

In many cases, we have to make do with the existing infrastructures. Most of the established systems, capital intensive as they are, and embedded as they are in the economic and spatial structure, are slow in responding to changing economic conditions and changing user demands. In the design of new infrastructures, we still have not learned to properly deal with the many uncertainties that the system will have to face over its projected lifetime. Opportunities for greenfield infrastructure design are relatively scarce. However, if they arise, the challenge is to equip the design with the physical flexibility and the budget flexibility that ensure its adaptivity to changing requirements.

## **2.5 Conclusion**

Infrastructures have evolved from a collection of service-dedicated technologies and systems to critical infrastructures, characterized as system-of-systems. They have ended up as risky constructs that are vulnerable to new kinds of threats, and are prone to social, financial and technical interdependencies. New ways to properly assess and design future generation infrastructures have recently begun to emerge. Dealing with risks and vulnerabilities for such new constructs calls for a new type of governance.



## Chapter 3

# Liberalisation and Internationalisation of the European Electricity Supply System

*L.J. De Vries, H.M. De Jong, M.L.C. De Bruijne, H. Glavitsch, H.P.A. Knops*

### 3.1 Introduction

The electricity infrastructure is one of the most finely meshed infrastructures in existence. In Europe, nearly every home and building is connected to it because electricity is essential to the functioning of modern society. Without electricity, the standard of living would be set back by a century and it would become impossible to perform most economic activities.

The electricity infrastructure is undergoing rapid changes. This chapter describes two trends: liberalisation (in Section 3.2) and internationalisation (Section 3.3). Both trends have significantly altered the institutional structure of the European electricity supply system. Section 3.4 describes the challenges to system security in the new environment. Section 3.5 summarises the conclusions. A third important trend, the increasingly pervasive use of information and telecommunication technology, is discussed in Chapter 4.

In order to understand these trends and their repercussions for the electricity infrastructure, a significant part of Chapter 3 is devoted to a structural analysis of, first, individual electric power systems and, second, how the European system of connected electric power systems is organised and functions. For this purpose, there will be a brief discussion of the technical characteristics of electric power systems, but the main subject of this chapter is the changing roles and responsibilities of the actors in the electricity industry.

This book focuses on European electric power systems. Politically and geographically, the boundaries of Europe are not well-defined. For the purpose of this book we will consider the territory of the electricity networks that are part of the Union for the Co-ordination of Transmission

of Electricity (UCTE), plus the United Kingdom, Ireland and Scandinavia. While not all European countries are members of the European Union, each of the above areas contain EU member states. Due to the strong physical relations between electricity systems, therefore all European electric power systems are affected by the liberalisation policy of the EU.

## 3.2 Liberalisation

### 3.2.1 Background

In 1996, the European Union adopted Directive 96/92/EC, which gradually opened the European electricity market to competition, starting in 1998. In 2003 this directive was replaced by a new one (2003/54/EC) which imposed stricter conditions upon EU member states. The purpose of liberalisation is to increase the economic efficiency of formerly monopolistic markets by exposing as much of the value chain as possible to competition. To this end, the elements of the value chain that are natural monopolies (in electricity primarily the transmission and distribution networks) need to be ‘unbundled’ from competitive elements. This is necessary to prevent them from being used to create unfair competitive advantages for their owners, in other words to create a ‘level playing field’ in the market. A second requirement for a level playing field is that connected countries have similar regulations, market designs, tariffs, taxes *etcetera*.

The European Union’s policy of liberalising electricity markets affects virtually all electric power systems in Europe. Because most electric power systems are connected to each other, non-EU countries are also affected. This section is devoted to an analysis of the structural changes that are brought about by liberalisation. We will do this by analysing, at a generic level, the technical structure of an electric power system, the actors that control the ‘hardware’ of a liberalised electric power system, how the system as a whole is designed to function and how connected electricity systems interact. In this section we will limit ourselves to the analysis of an individual power system, which is defined as a system that is operated by a single TSO (also known as a control area). In Section 3.3, we will analyse the relations between interconnected power systems.

#### Analytic framework

We will use the term *electric power system* to indicate the combination of the systems that produce, transport and deliver power and that provide related services. The system includes parties that trade in electricity or provide trade-related services such as electricity exchanges and brokerage

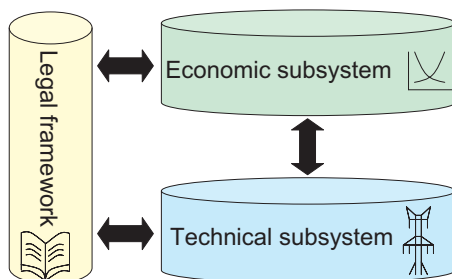


Figure 3.1. Basic structure of the analysis  
Source: De Jong (2004a)/De Vries (2004)

services. A single electric power system is defined as a system that is controlled by one TSO (transmission system operator; see below). Each country in Europe has at least one TSO; some countries have more than one. The term electric power system coincides with the more technical definition of *control area* that the UCTE uses (UCTE, 2005b).

The electric power system can be divided into two subsystems: a technical subsystem, centred on the production and transmission of electricity, and an economic subsystem, in which electric power and transmission and distribution services are traded. A legal framework regulates both subsystems and their interactions. Figure 3.1 presents a graphic representation of this basic conceptual framework. Below, this framework will be detailed step by step to arrive at a generic model of electric power systems. Because the legal framework is strongly influenced by EU policy, it will be discussed briefly in Section 3.2.6. The subject returns more in depth in Section 3.3, which discusses the European power system.

Most European markets are of the decentralised kind, in Hunt's (2002) typology.<sup>1</sup> This means that they do not have a mandatory power pool, but that market parties may trade their electricity bilaterally and only need to notify the system operator of their physical programs. In integrated markets, on the other hand, all physical trade takes place through a mandatory pool (such as the PJM pool), and bilateral contracts can only be financial.

The following sections will describe the impact of liberalisation upon a generic electricity system. For this purpose, we will start by describing the technical and the economic subsystems. At a conceptual level, these are similar in most European countries, as the same technical functions need to

<sup>1</sup> See also Section 3.2.4.

be performed by actors who operate within a market environment. Next, the way the system functions as a whole will be analysed.

### 3.2.2 Technical structure

The technical subsystem of an electric power system consists of the hardware that physically produces and transports electric energy to customers as well as the equipment in which the electric energy is consumed. It further consists of the people and organisations that build, maintain, operate and control the equipment. The structure of the technical subsystem is determined by the nature of the components of the power supply system: the power stations, the transmission network, the distribution networks and the consumer equipment. The system operator and the network operators are responsible for the safe and stable operation of the system. This section will briefly describe the components and operation of the technical subsystem. See also the text box below for the definitions.

#### Power stations

The most important characteristics of power stations are:

- size (capacity),
- controllability (speed with which they follow changes in load),
- availability (scheduled and unscheduled outages),
- reactive power generation capacity,
- energy source (coal, nuclear energy, wind, *et cetera*), and
- environmental impact (emissions, waste, noise).

The first four characteristics are essential for determining a power station's behaviour in the transmission network. All characteristics have value in the economic subsystem. The latter two characteristics may be important for the economic subsystem if customers demand electric energy from a source that is sustainable or at least less harmful to the environment than conventional power stations.

#### **Definitions**

**Ancillary services:** compensation for power losses, management of reactive power, and voltage and frequency support.

**Control area:** contiguous part of a network within which the energy balance and power quality are controlled.

**Dispatch:** operating instructions for power stations.

**Electric power system:** the combination of systems that produce, transport and deliver power and provide related services, including the actors and institutions that control the physical components of the system. The electric power system consists of a technical and an economic subsystem.

**Economic subsystem:** the actors that are involved in the production, trade or consumption of electricity, in supporting activities or their regulation, and their mutual relations. These relations may exist in the context of a competitive market, but this is not necessarily so: the operators of the networks also are part of the economic subsystem.

**Technical subsystem:** the physical part of the electric power system, consisting of the hardware that physically produces and transports electric energy to customers, as well as the apparatus that use the electricity.

**Power station:** an apparatus that produces electric energy from another form of energy. Primary energy sources can be hydrocarbons, nuclear energy, or sustainable energy sources such as wind, the sun, geothermal energy and biomass. Secondary energy sources such as diesel oil or hydrogen gas may also be used.

**Consumer equipment:** term used for all apparatus that use electricity from the public electricity infrastructure, varying from consumer appliances to industrial processes.

**Transmission and distribution:** both terms refer to the transport of electricity. Transmission typically indicates transport over longer distances, for which higher voltages are used, while distribution indicates local transport to end users. The transmission and distribution systems are networks. They often have multiple routes between two points to enhance system reliability. As a result, not line capacity but network capacity is the determining factor.

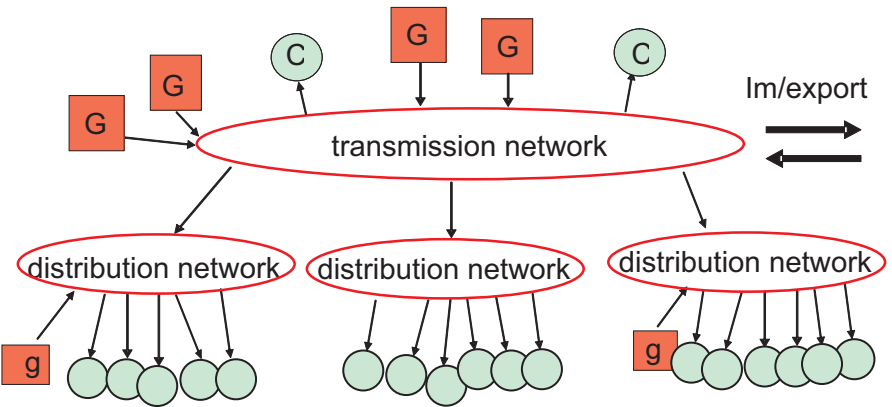
**Transmission line:** circuit in an electricity transmission network. The main technical characteristics of transmission lines are their capacity, which is the amount of energy they can transmit, and their impedance, which is the combination of their electric resistance and phase-shifting properties.

**Transformer:** apparatus that converts electricity from one voltage level to another voltage level. They are an essential part of any large-scale electricity network, as electricity is transported at high voltage levels and mostly used at much lower voltage levels.

## Networks

Electric energy is transmitted from power stations to consumers through a highly meshed network. This network actually exists of a number of networks of different voltages which are connected by transformers. The electrical power system is structured in layers of different operating voltages: for long-distance transmission of electricity, high voltages are used because energy losses are lower; for local distribution lower voltages are used because they are more practical. In Europe a typical series is 420, 220, 110, 50, 20 and 0.4 kV (1 kV = 1000 Volts). Presently the majority of the electrical energy is produced in centralised power stations connected to the 420-, 380-, 220- and 110-kV-networks.

Usually, electricity networks are divided into transmission and distribution networks, but the boundary between the two is somewhat arbitrary.



G/g: large/small generator  
C/c: large/small consumer

Figure 3.2. Schematic representation of electricity networks

For the purpose of this research, the electricity networks from power station to consumer can often be considered as a whole, which is why they often are referred to as 'the network'.

The geographical boundaries of a network are, in principle, arbitrary. Their shape is historically developed, so their boundaries often coincide with political boundaries. Neighbouring networks usually are connected. In this section, a single network will be considered to be that part of the interconnected network that is administered by one system operator. Figure

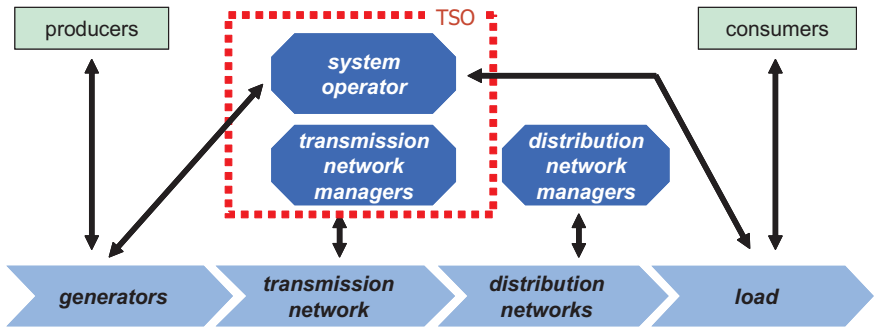


Figure 3.3. Schematic representation of the technical subsystem

3.2 shows the basic structure of electricity networks. The dominant characteristics of transmission and distribution networks are:

- the morphology of the network, including connections to networks of other voltages,
- the transmission capacity of each line,
- the impedance of each line, and
- possibilities to control voltage and reactive power.

Consumer equipment

The last large category of physical components is the consumer equipment that uses the electric energy for lighting, power *et cetera*. This equipment places a load upon the network. The most important characteristics are:

- maximum demand,
- reactive power demand,
- demand pattern, and
- interrupt ability (can they be switched off).

Operation and control

The combined characteristics of power stations, consumer equipment and network components determine where and how much electricity is generated and consumed. Different combinations of supply and demand result in different load patterns of the network. Two functions are needed to manage the technical subsystem, namely a system operator and a transmission system manager, see Figure 3.3. In Europe, these two usually are combined into the figure of a transmission system operator (TSO). Although the actors that perform these functions are not themselves part of the technical subsystem (according to the definition used here) they are included in the figures, as their role is central to the functioning of the system.

The system operator maintains system stability and manages the energy balance within a control area because the network itself cannot store electric energy. Because in decentralised markets actual demand and supply may differ from the amounts that were contracted by market parties, the system operator needs to maintain the power balance continuously. To this end, TSOs contract operating reserves (power plants that can generate electricity on short notice, sometimes augmented with interruptible contracts with large consumers). If the market projected supply and demand well, the need for balancing is small, but still it is a crucial activity for system stability. The costs of maintaining the balance are passed through to the parties who create the imbalances: power stations who produce more or less than scheduled and consumers (or retail companies who operate on their behalf) whose consumption deviates from their contracted volumes. This takes place in a so-called balancing market, in which the TSO pays for regulating power (for increases as well as decreases) and in which market parties pay for imbalances in their output.

The transmission network manager guards against congestion, maintains reliability of transmission service and provides ancillary services for transport, among others to maintain voltage levels. In principle, there can be multiple transmission operators per control area, but in Europe this is rare, if it occurs at all. In European power systems, the tasks of the transmission operator and the system operator are combined in one agency, the transmission system operator (TSO). The reason is that while the tasks of the system operator and the network manager are quite different conceptually, they require similar information and similar control measures. Moreover, historically these tasks often were executed by the same utility company.<sup>2</sup> Distribution network managers perform a task similar to that of the transmission network manager, but they are only network managers, not system operators. Network costs are recovered through tariffs, which influence the market through the constraints they impose and the financial incentives they create.

### Contingency response

The liberalisation of the European interconnected network, which is operated by a number of independent transmission system operators, poses new challenges to security control. Congestion may appear in one of the networks due to actions far away from the critical location, outside the control of the TSO in whose network it occurs.<sup>3</sup> Disturbances in one

<sup>2</sup> In the USA, however, the two are often not combined, for instance because a system operator controls a system that encompasses the networks of multiple network companies.

<sup>3</sup> The management of congestion will be discussed in Section 3.3.3



network may affect neighbouring networks; large disturbances often involve multiple TSOs who need to cooperate closely.

One of the curiosities of decentralised electricity markets is that in real time they are not decentralised. The speed with which disturbances need to be addressed does not allow for negotiating time between market parties. Therefore the system manager is solely responsible for operating the system in real time. The operational control over the system by market parties is limited to submitting schedules up to a certain period before real time. In real time, the TSO has the power not only to operate the network, but also to increase or decrease the output of power stations and, ultimately, to shed load, if this is in the interest of the overall stability and controllability of the system. The costs to market parties are either covered by contracts for regulating power and interruptible contracts with consumers or are reconciled afterwards in the balancing market. So in real time, control over the system is still hierarchical.

The centralised control structure of the electrical power systems varies. None of the large interconnected systems in the world are completely centrally controlled (PJM, UCTE, Nordel). Central control is augmented with regional control centres. Control centres are equipped with communication means that are connected to substations and power stations. This provides the operators with information about the current state of the system. They may respond by taking action by remote control or by manual intervention, for instance by instructing power plant operators over the telephone. Substations at the lower voltage levels (50 kV, 20 kV and below) are usually not remote-controlled. Quite often they are unmanned and therefore switching for purposes of restructuring can be performed only with a delay.

To protect network equipment from damage due to overloading, many parts of electricity networks have automatic protection devices that disconnect an element or device in case of excess stress. These circuit breakers act in a fraction of a second. The disconnection is performed in such away that the element is ready for re-connection after a short delay. The majority of protective relays and systems protect single components, not subsystems. This way of protecting components is mainly applied to transmission circuits, transformers, busbars and even generators. In case of overloading, these elements are disconnected automatically without consideration for the consequences to the behaviour of the overall system.

A consequence of disconnecting an overloaded component may be that another element is overloaded, which would lead to its disconnection as well. For instance, if one of two parallel transmission lines is disconnected because it is being overloaded, all the current will flow through the other line, which now also may be overloaded. This method of protection is a

first line of defence that does not take the security of the system into account.

Another example is the protection of a power station in response to a drop in the frequency. A frequency drop is an indication that not enough power is supplied to the system, that is, that more power is used by consumers than is being supplied to the system by the generators. When the system frequency drops below a predefined level, the power station is separated. This protects the power station, but less power is supplied to the system, as a result of which the power system experiences a further drop in frequency. This may cause other generators to disconnect, which may lead to a cascading outage of generating units and finally to a blackout.

At first sight this approach to security may appear an ill-conceived concept, but at a closer examination one will come to the conclusion that it is inevitable. It is absolutely necessary to avoid possible damage to equipment in case of disturbances. Automatic protection is necessary because of the short time spans (there may be a danger of explosions). System security is augmented by additional systems and schemes, partly automatic, semi-automatic or human, which have as a goal to prevent blackouts by providing reserve power, reducing demand through interruptible contracts or, as a last resort, switching off groups of consumers in a controlled fashion to reduce load and maintain system stability.

### 3.2.3 Technological developments

While electricity network components have a long life cycle and their geographical design cannot be changed easily, network development is characterised by a strong path dependency. Nevertheless, some changes are on the horizon or already occurring:

- Distributed generation, the generation of electricity from relatively small-scale power plants that are connected to distribution networks, is becoming a significant source of electricity in some areas. If this trend perseveres it could fundamentally change the way that distribution networks are operated. Distributed generation may also significantly impact market dynamics because it could practically eliminate the entry barrier to the generation market. If small generation units would be available 'off the shelf', this would also greatly reduce investment risk and therefore improve security of supply (De Vries, 2004). Distributed generation is limited, however, to areas where primary energy is available, such as in the Netherlands with its finely meshed natural gas infrastructure. Whether the share of distributed generation will grow depends upon its economic viability.

- Increasingly, electricity is being generated from uncontrollable sources such as wind and sun. While these sources have a low environmental impact, their fluctuating nature represents a challenge to network and system management. Currently, the large volume of wind power in the north of Germany and in Denmark already is stressing these systems (Berger, 2005). The effects are widely felt: for instance, the Dutch import capacity is limited so it can not accommodate unforeseen flows from northern German wind turbines (TenneT 2003; Sambeek *et al.* 2004). There are some trends that may mitigate these effects in the future, such as better wind forecasts and the possible development of storage devices.
- FACTS (Flexible AC Transmission Systems) are gradually being introduced. They may improve the efficiency with which transmission networks are being used. However, the more advanced types of FACTS, which make use of power electronics, create side effects. Because the systemic effects of their implementation on a large scale are uncertain, they have not yet been implemented in Europe. Currently, the application of FACTS is limited to phase-shifting transformers.
- The increased use of ICT at every level of the electricity infrastructure has a profound impact upon its design and operation. The use of ICT creates both opportunities, in terms of more efficient, more effective and faster response to disturbances, and risks such as the threat of cyber attacks. The increased complexity of the power system and the interdependence between the electricity and the ICT infrastructures also represents a vulnerability. The trend manifests itself differently at the different levels of the electric power system. For instance, a selection of offline application routines presently active in the control centres could be operated closed-loop. Examples are wide-area protection schemes, flow based load and generation shedding, corrective switching and start-up of reserve units. Power exchanges, on the other hand, are an example of a service that cannot function without the internet. In Chapter 4 the increased dependence of the electricity infrastructure upon the information and telecommunication infrastructure will be examined.

### **3.2.4 The electricity market**

Now we will turn to the economic subsystem, in which producers, consumers and other network parties, as well as actors with a monopoly such as the TSO and the distribution network managers together manage the electric power system. While the actors in the economic subsystem

control the technical subsystem, they are also constrained by the physical limitations of the technical subsystem. Thus the performance of an electric power system is the result of the characteristics of both the technical and the economic subsystems. In this section, we will describe the structure of the economic subsystem and the actors that are part of it. Having analyzed both the technical and economic subsystems, we will consequently turn to the performance of the socio-technical system as a whole.

#### Integrated versus decentralised markets

Hunt (2002) distinguishes two types of market: integrated and decentralised markets. An integrated market is characterised by a mandatory power pool through which all power is traded. In advance of real time, producers tell the pool operator the conditions under which they are willing to produce: the time, price, volume and location of generation. The pool operator then dispatches power stations in real time according to their cost (merit order dispatch) within the constraints of the network. (The latter is the reason why the pool often is operated by the TSO.) There are no imbalances, as the pool operator adjusts dispatch in real time. The marginal unit determines the electricity price. Examples of this model are the former England and Wales Pool and the Spanish market, as well as most markets in the USA.

More common in Europe is the decentralised market structure. In this type of market, individual contracts for power determine the dispatch. The TSO is obligated to accommodate these contracts to the extent that they are feasible within the physical constraints of the network, regardless of their economic merit.<sup>4</sup> In a decentralised market there is no mandatory power pool. Rather, organised power exchanges are the result of private initiatives. Consequently, they are not necessarily present in every market, but their significant added value has led to the development of one or more organised power exchanges in most European power systems (Boisseleau, 2004). A consequence of a decentralised system is that the scheduled power flows may differ from the actual flows, which is why decentralised systems need to have a balancing mechanism.

#### The supply of power

The supply side of the electricity market consists of generation companies, the owners of the power plants in which electricity is produced. These companies often are part of larger companies that are active in other parts of the electricity value chain and/or in the natural gas

<sup>4</sup> If the net effect of all contracts would lead to overloading of the network, the network is congested. Then the trades need to be rearranged so they fit within the constraints of the network. To this end, a number of congestion management methods have been developed (Knops *et al.*, 2001; De Vries and Hakvoort, 2002).

sector. Based upon the prices that the producers offer, the market decides the quantity of electricity that each generation company may sell at each moment in time, but the generating companies themselves decide which of their power plants they operate.

In theory, competitive power markets should provide an optimal volume of generation capacity. There are reasons to doubt whether real-life markets actually provide the right investment incentives at the right time. Therefore the implementation of a capacity mechanism may be considered to secure a sufficient volume of generation capacity (De Vries, 2004). See also Section 3.2.7.

### Demand

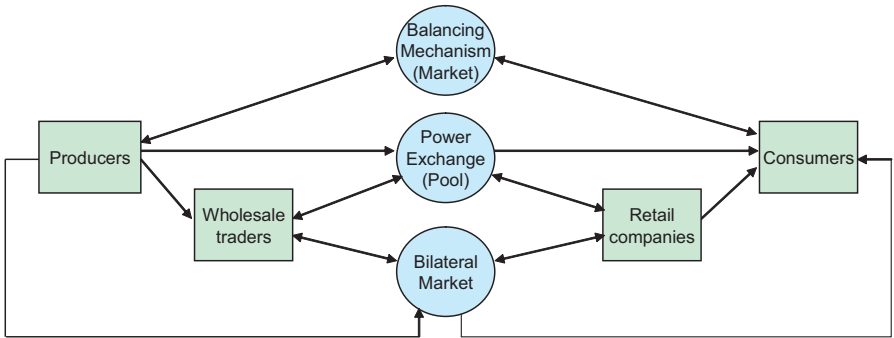
Ironically, those who are the object of the electricity supply industry – the consumers – are the least involved in the market. One reason is that the participation of many consumers is limited by the absence of real-time meters, as a result of which they have no incentive to respond to short-term price differences. Only large consumers usually have the necessary equipment to be active in the electricity market.

However, real-time meters are quickly becoming cheaper and in Italy, for instance, they are being installed with small consumers. It is unclear yet whether and to which extent consumers who have the necessary equipment will adjust their electricity consumption to real-time prices. Standard profiles consumption profiles typically are applied for consumers who do not have these meters.

### The market: mostly bilateral

Producers and consumers meet in ‘the’ market, which actually consists of multiple related markets. The largest volume of electricity is sold in the ‘bilateral’ market, which consists of private contracts between generating companies and their customers. These are either large consumers, traders or (often) retail companies who deliver it to small and medium size consumers (see Figure 3.4). Bilateral contracts are confidential, as a result of which there are no good data available regarding their price and duration. According to traders, contracts that are longer than two years are rare. Power exchanges greatly reduce transaction costs by providing a standardised trading platform, which facilitates market parties’ needs to adjust their trading positions on short notice. They also play an important role by providing a public reference price. There appears to be a trend towards more trading through organised power exchanges. The volume of the Nordic market Elspot already is equal to 44 % of total consumption (NordPool, 2004).

Another important component of the economic subsystem is the balancing mechanism, through which the TSO obtains regulating power



*Figure 3.4.* Schematic representation of the economic subsystem  
Source: De Jong (2004a)/De Vries (2004)

for maintaining the system balance and which transfers the costs of imbalances to the parties who caused them. Generation companies provide the system operator with bids for incremental or decremental electricity production and large consumers may offer to be interrupted.

#### Network and system operation

Although he is, or should be, a neutral party, the TSO plays an important role in electricity markets. In Section 3.2.2, the main roles of a TSO were described: system operation and transmission network management. Thus the most important central functions that are not suited for competition have been under the responsibility of the TSO. The only other monopoly function is the management of the distribution networks.

#### Unbundling

The Electricity Directive (2003/54/EC) of the European Union requires competitive activities such as generation and end-user supply to be unbundled from transmission and distribution network management and from system operation. Different levels of unbundling are possible; the directives require that the legal structures and organisational structures of the managing bodies of the networks are juridical separated from competitive parts of the electricity companies. The reason for unbundling is to avoid cross-subsidies and prevent the strategic use of bottleneck facilities by competitive parties. Most European countries have adopted the unbundling rules within their power companies and utilities and regulators have set up corresponding rules. Unbundling, however, complicates system security, because to manage disturbances, generation and transmission need to be operated in coordination. In such a state the system needs to be managed as if it were vertically integrated.

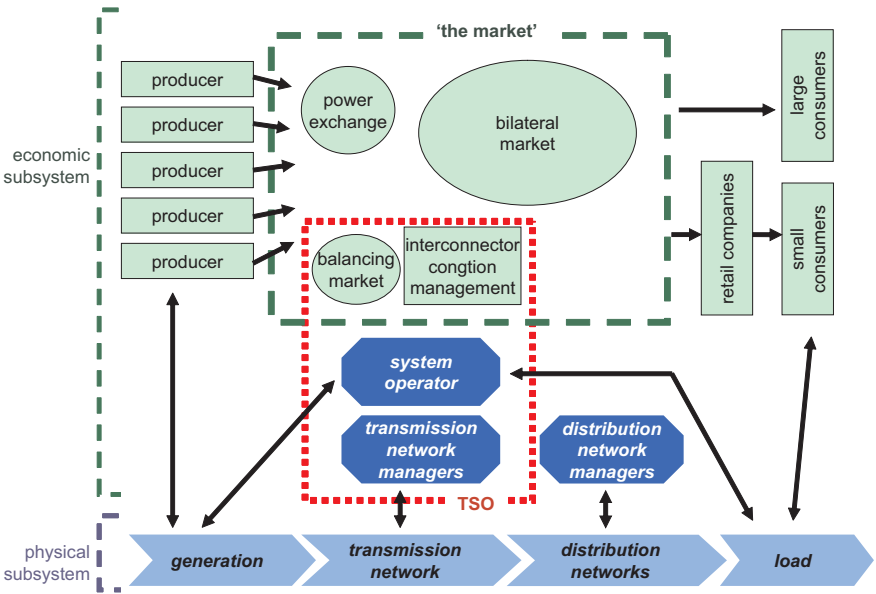


Figure 3.5. Conceptual model of a single electric power system  
Source: Knops *et al.* (2004)

### 3.2.5 An integrated socio-technical system

The technical and the economic subsystems that were described in the previous two sections are connected by information flowing between them in the form of supply curves, demand curves, network tariffs, access rules, capacity restrictions and dispatch instructions, among others. These relations are impacted by the legal framework. We will use Figure 3.5, which is a combination of Figure 3.3 and a simplified version of Figure 3.4, to make a brief inventory of these information flows. (It should be realised that, while the figure depicts a single system, in reality most systems are connected to neighboring systems. These relations will be discussed in Section 3.3.)

The most important information for the market consists of the supply and demand functions. The supply function is based upon the cost function of power stations but is not necessarily the same. The demand function is not well known because many consumers are not equipped with real-time meters and do not to respond to spot prices. As a result, the observed price-elasticity of demand is low.

### The electric power system before liberalisation

Before liberalisation, the electric power system consisted of little more than the technical system. The utility companies owned generation facilities as well as the networks. Sometimes they controlled the entire production chain from generation to retail; in other cases, different companies provide generation or distribution, for instance. Key is, however, that all services were provided by regulated monopolies.

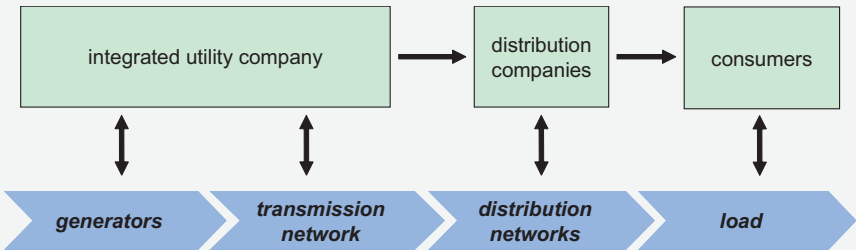


Figure 3.6. The organisational structure of the electric power system before liberalisation

Source: Knops *et al.* (2004)

The transmission system operator and distribution network companies charge market parties for their services in the form of tariffs, which are regulated to prevent the abuse of monopoly power. In addition to the price signals provided by transmission tariffs, the transmission operator may signal capacity restrictions to the market parties in the case of congestion. These charges contribute to the end user price for electricity.

The interaction between generation companies, and consumers which often takes place through intermediaries, results in the electricity prices. Consumers use these prices to establish their demand for electricity and decide from which generating company they purchase their electricity. How much electricity is demanded, when and where and at which price, is the basis for the producers' decisions which power stations to dispatch. Thus the market parties' choice of producers and the producers' choice of power stations determines to a large extent, the load pattern of the networks and the associated revenues to the transmission operators from the transmission tariffs.

Liberalisation has distributed the control over the electricity supply industry among many actors. The intention is to improve the economic



efficiency of the system by letting decisions be made by the actors who have the best knowledge. A side effect, however, is that the organisational complexity of the electricity supply industry has increased significantly, as can be seen by comparing Figure 3.5 with Figure 3.6 in the text box above.

The increased unpredictability and volatility of the behaviour of electric power systems that is the consequence of liberalisation would ideally require system operations to be able to respond more rapidly to reliability-threatening disturbances. However, the opposite may be true. Where in the old, vertically integrated structure, electric power system operations used to be an integral part of the electricity value chain, restructuring has unbundled the responsibility for different parts of the electric power system. The fragmented responsibility among different organisations involved in the operation of the electric power system creates new challenges for control, information management and reliability management. Even though formal authorities have sometimes changed little with regard to responsibilities, the introduction of competition, market incentives and fragmented ownership of key elements in the electricity infrastructure has created different relationships in electricity operations in real-time.

For example, although TSOs may still have the authority to control real-time system operations, system operators may find that, compared to the situation before liberalisation, market parties such as generating companies or distribution network operators react slowly to the TSO's directions and need to be more carefully monitored with respect to undesired strategic behaviour. Thus, dispatch orders under liberalised electricity operations may not be as reliable as in the centralised world. The introduction of formal market-based routines or rules may also reduce the flexibility and command-and-control capability of system operators. Finally, the old control options may be found to lead to severe market-disturbances.

In other words, although theoretically the introduction of competition would appear to have enhanced the speed and effectiveness of electricity operations in real-time, TSOs often find that this is only half the story. The introduction of markets has limited TSOs' control options and simultaneously increased their need for increased micro-management in order to check the behaviour of strategic actors.

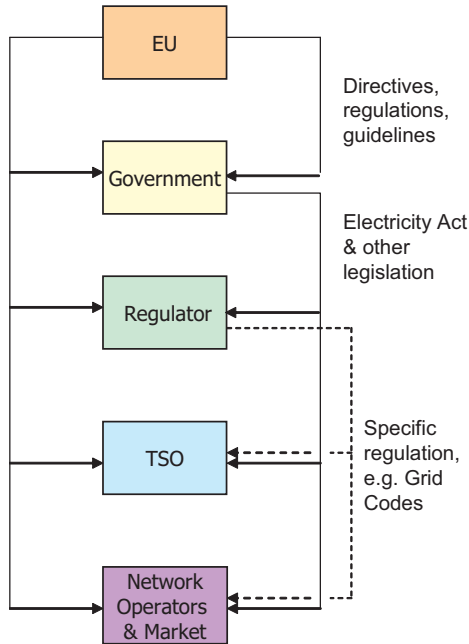


Figure 3.7. The legal framework  
Source: De Jong (2004a)

### 3.2.6 The legal framework

Both the technical and the economic system are regulated. The European Union imposes directives, regulations and guidelines on the EU member states. Directives do not directly affect actors in the electricity supply industry but need to be implemented in national regulation to have effect. Regulations, on the other hand, have a direct effect. Guidelines can both be directly binding or non-mandatory. Within a certain country, the government and the regulator can create rules for market participants and regulated parties such as TSOs and distribution network managers. TSOs also have the authority to develop rules, for instance with respect to network access and system balancing. Figure 3.7 shows the hierarchy of the legal framework.

Because the legal framework derives for an important part from the European Union, it will be discussed in more depth in the context of the internationalisation of the European electricity industry in Section 3.4.3. In addition, Box 3.2 describes the European regulatory process.

### 3.2.7 Generation adequacy

The most capital-intensive part of the value chain that is affected by the introduction of competition is the generation of electricity as competition between electricity networks is not deemed economically feasible. In the short term, the many changes in the electricity industry do not appear to have much effect upon the generation stock, simply because it takes power stations years to build and last decades. However, in the long term, the consequences for investment in power stations may be one of the main effects of liberalisation.

#### How the market should work

Electricity markets have a different dynamic from other markets due to three characteristics:

- Electricity is a strongly time-limited product. It currently cannot be stored, other than in pumped-hydro facilities, in a commercially viable way. However, the electricity supply system can only function in a stable manner if supply and demand are continuously balanced.
- The supply of electricity is only partly characterised by a gradually increasing marginal cost function. When all available generation units are producing electricity, no marginal increase is possible in the short term. As a result, the marginal cost curve ends with a perfectly price-inelastic section.
- The demand for electricity also is highly inelastic. This may be caused by the fact that there is no readily available alternative for most applications of electricity. At least as important is, however, that few consumers have an incentive to adjust their behaviour to real-time prices in the absence of the necessary metering equipment.

The combination of these three characteristics is the reason that most mechanisms which aid the clearing of other markets, such as delays in the delivery of the good, consumers switching to other goods or higher prices leading to a reduction in demand, are not available in current electricity markets. This has significant consequences: wholesale electricity prices are highly volatile, and secondly, there is a chance of service interruptions.

If the market does not clear, that is, if all available generating capacity is not sufficient to meet demand and some service needs to be curtailed, it may be necessary to institute a price cap to protect consumers against overcharging (cf. Ford, 1999; Hobbs *et al.*, 2001; Stoft, 2002). If consumers are not involved in real-time price setting, they otherwise may find themselves paying more for electricity than their value of lost load. This price cap needs to be determined carefully, as it impacts the attractiveness of investment in generation capacity. The price cap needs to equal the average value of lost load (VOLL), because at this price

consumers should, on average, be indifferent whether they receive electricity or not. Stoft (2002) shows that in a perfectly competitive market, this results in an optimal level of investment in generation capacity, with an optimal duration of power interruptions. Therefore the theory of spot pricing still is valid, even if demand is fully inelastic. Price caps can be problematic, however, because it is difficult to determine the optimal level, as the value of lost load is difficult to measure (Willis and Garrod, 1997; Ajodhia *et al.*, 2002).

Although theoretically sound, the reliance upon periodical price spikes to signal the need for peaking capacity has some significant weaknesses. To begin with, there is the risk that the price cap is set at the wrong level, resulting in over or under-investment. However, there are more fundamental issues. The first is that investment in peak generation units is quite risky, so that small distortions of the investment signal may have large consequences. The second is the argument that there is a positive externality associated with investment in peaking units, because security of supply is a public good (due to the network character of electricity supply). The third factor is the inevitable development of market power during periods of supply scarcity. These issues will be addressed in the next sections.

### Investment cycles

There are several reasons why energy-only electricity markets may not provide a sufficient incentive to invest in generating capacity in a timely manner.<sup>5</sup> Here we will provide a synopsis; a more extensive argument can be found in De Vries and Hakvoort (2003) and in De Vries (2004).

The high volatility of electricity prices (especially in markets without much hydropower), the capital-intensive nature of generation and the long lead time of new facilities together cause investment risk to be high. If investors are risk-neutral and have all the necessary information, this should not matter and the volume of generating capacity should still be socially optimal, at least in a perfectly competitive market (cf. Caramanis, 1982; Stoft, 2002). Generating companies would invest up to the point where their expected long-run average returns would equal the long-run marginal cost of generation. However, it is difficult to estimate future generator revenues, because they depend strongly upon the frequency, height and duration of price spikes.

<sup>5</sup> An 'energy-only market' is an electricity market in which there are no specific provisions to stimulate investment in generating capacity, like in most European markets. Consequently, generating companies base their investment decisions upon their expectation of future prices for electric energy.

Most liberalised electricity markets still are in a transition phase, so historical data are not a good basis for projecting such volatile future revenues. For instance, Europe started liberalisation with ample reserve capacity, as a result of which prices during the first years of liberalisation were quite low. In the summer of 2003, however, prices rose to unprecedented heights in many countries. A tightening supply of generating capacity is forecast for Europe (UCTE, 2005a). As a result, more price spikes may be expected and average prices may rise. When, or to what degree, remains uncertain, however, so that it is difficult to forecast future generator returns.

Several causes of regulatory uncertainty may further reduce the ability of generating companies to forecast their revenues. One example is the possibility of intervention by government in the electricity market, for instance by imposing a low price cap in response to an extended price spike. Changes in related markets, such as emissions trading schemes and restructuring of primary fuels markets also create uncertainty with respect to future generator returns.

Finally, investment in electricity generation is characterised by an asymmetric risk profile: investing beyond the socially optimal volume of generating capacity means that prices will be too low to recover the investment, while a volume of generating capacity that is below the social optimum leads to significantly higher average prices, which at least partly offset the lost turnover. Therefore it is to be expected that especially in markets that are less than perfectly competitive (as electricity markets generally are), generating companies would be somewhat risk-averse in their investment decisions (Neuhoff and De Vries, 2004). The significant entry barriers facilitate this.

High price volatility, long lead times, imperfect foresight, regulatory uncertainty and risk aversion are reasons for generating companies to delay investment until the need for new generating capacity becomes reasonably certain. Due to the low price elasticity of demand and the relative 'flatness' of supply curves, prices do not rise significantly in a competitive electricity market until the margin between available generating capacity and peak demand becomes small. Due to the long lead time before new generating capacity can be taken into operation, this margin is likely to decrease further and may even disappear before new capacity is available. Depending upon the growth rate of demand, investment in reaction to price rises may not arrive soon enough to avoid a prolonged period of shortages. The high prices that would develop in the mean time could trigger an over-reaction by investors, after which a period of excess generating capacity would lead to prices below the long-run marginal cost of generation. Therefore the electricity generation industry appears prone to investment

cycles. The theoretical arguments why insufficient investment may be expected are corroborated by the UCTE (2005a), who forecast declining capacity margins in mainland Europe towards the end of the current decade.

#### Asymmetric loss of welfare function

Stoft (2002) shows that in theory, the optimal volume of generating capacity can be determined from the average value of lost load and the long-run marginal cost of generation. However, estimating the average value of lost load is notoriously difficult (cf. Kariuki and Allen, 1996a, Kariuki and Allen, 1996b, Ajodhia *et al.*, 2002), which means that this calculation is likely to be inaccurate. Moreover, more important than the currently optimal volume of generating capacity is the optimal volume at the time that new capacity would come on stream, several years into the future. Considering the inherent difficulties in estimating the optimal volume of generating capacity, the question presents itself what the costs are of erring. This depends upon the perspective: investors have a different interest than consumers.

Like investors, consumers faces an asymmetric loss of welfare function with respect to the socially optimal volume of generating capacity, but one that is reversed. During the crisis in California in 2000 and 2001, at most 2 % of load was shed (Hawkins, 2001), but the costs to consumers were extremely high (Weare, 2003). The costs of excess investment, on the other hand, appear much more limited. Shuttleworth *et al.* (2002) calculate that if the economically optimal reserve margin were 8 % of installed capacity, and the reserve margin somehow was established at 20 %, the associated social cost would be about 1.1 % of the retail price of electricity. Therefore we may draw the conclusion that the provision of electricity is characterised by a strongly asymmetric loss of welfare function. This result is corroborated by Billinton (1994), who shows a strongly asymmetric loss of welfare function.

Given uncertainty about the precise optimal volume of generating capacity – especially as many years in advance as it takes to construct new generating capacity – the asymmetry is reason for consumers to err on the side of more generating capacity. However, we saw that cautious investors would tend to provide less generating capacity than the theoretical optimum, and that even without risk-averse investment there is a possible tendency towards investment cycles. Therefore it is in the interest of consumers to implement a mechanism to ensure a certain volume of generating capacity. This is not a new argument (cf. Cazalet *et al.*, 1978), but one that is often overlooked in the design of liberalised electricity markets.

### Market power during shortages

A third reason to change the market structure is that price spikes, which should provide the investment incentive in an energy-only market, can be manipulated if the price-elasticity of demand is limited (as it is in most existing markets). By offering less generating capacity to the market, generating companies may be able to increase the electricity price substantially (Stoft, 2002; Joskow and Kahn, 2002). This has several consequences. First, it leads to substantial income transfers from consumers to generators, as we saw in California. Second, the reduced availability of generating capacity during periods of tight supply may undermine reliability. Third, the fact that high prices may not (entirely) be the consequence of shortages undermines the effectiveness of the investment signal.

### Structural market power: a counter force?

The above analysis hinges on the assumption that liberalisation leads to effective price competition. If this is not the case, generating companies may be able to maintain prices above the competitive level much of the time, which would provide them with extra revenues which they could dedicate towards building more generating capacity. Large, incumbent generating companies could have an interest in expanding their generating capacity, because this would deter competitors and new market entrants from investing in generating capacity. A second motive could be that established generating companies would want to avoid the political turmoil that would result from a significant shortage. We may conclude that it is not certain whether underinvestment will occur in liberalised energy-only markets. Ironically, failure to create effective competition may prove beneficial to reliability.

### Capacity mechanisms

Several methods have been proposed to stabilise the market and provide better incentives to generation companies and consumers alike. The main effect of these capacity mechanisms is to make the demand for reserve capacity explicit, which reduces the investment risk for generation companies. For consumers, the benefits are better security of supply and lower price volatility. Capacity mechanisms may have additional benefits. The main benefit, in addition to minimising the risk of shortages, is probably the reduction of generator market power due to a reduced occurrence of episodes of scarcity. Reducing price volatility also is an important advantage to consumers, who generally cannot hedge themselves sufficiently against price spikes. The main capacity mechanisms are:

- capacity payments,

- strategic reserve (also known as ring-fenced reserve),
- operating reserves pricing,
- installed capacity requirements (also known as ICAP),
- reliability contracts,
- capacity subscriptions.

For an extensive analysis of capacity mechanisms, see De Vries (2004).

### **3.2.8 Conclusions with respect to liberalisation**

Liberalisation has replaced the paradigm of central, hierarchical control with the paradigm of decentralised control. The former has the advantage of being simple in structure and allowing coordination advantages, whereas markets have a more complex structure but should provide better incentives for economically efficient behaviour. A key consequence of liberalisation is that control over the system is distributed among multiple actors, as a consequence of which no single actor can be held responsible for the performance of the system. For instance, the provision of an adequate volume of generation capacity is the result of the investment and decommissioning decisions of all generation companies who are active within the system.

A consequence of the decentralised nature of liberalised electric power systems is that the institutional relations between the actors need to be structured carefully if they, together, are to meet the public goals for the electricity supply industry. This is true for the traditional goals of economic efficiency and reliability, but also for the contingency management. Given the need to respond extremely quickly to contingencies, the fragmented nature of liberalised electricity systems poses a new challenge. In recognition of this fact, TSOs have been allowed to retain control of their system in real time, having the authority to instruct power station managers. However, the fact that these power stations are no longer part of the same organisation may pose a barrier, as their relations now need to be formalised.

While the need for hierarchical control in real time has been recognised, the long-term development of the electricity supply system is completely left to the multi-lateral interaction between market players and network operators. Given the many market imperfections, there are reasons to doubt whether there will be sufficient investment in generating capacity. The implementation of a capacity mechanism is probably in the interest of consumers, given the importance that they attach to reliability and stable prices.



### **3.3 Internationalisation**

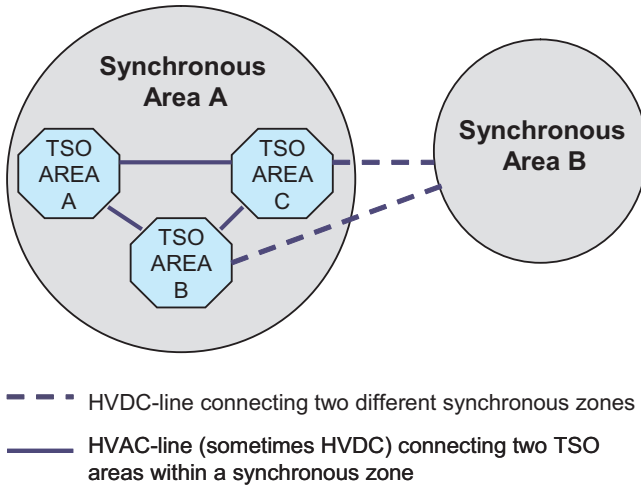
#### **3.3.1 Introduction**

The European electricity industry has outgrown national boundaries. Stimulated by liberalisation, the volume of international exchanges of electricity has increased rapidly and is now limited only by congestion of interconnectors. Together with liberalisation, the internationalisation of the industry has a significant impact upon the management of electric power systems, especially in real time. Whereas liberalisation has decentralised the decision making process, from the strategic level up to just before real time, internationalisation has increased the scale of the system. Both trends increase the average number of actors that are involved in contingencies. Whereas physically, the power system has reached the scale of the continent, the growth of the institutional structure has not kept pace. Because system operation typically takes place on a national or sub-national scale, there is an increasing need for cooperation between TSOs.

For instance, the management of congestion of interconnectors requires two or more TSOs to determine available transmission capacity, allocate available capacity to the market and agree how to distribute costs and revenues among themselves. Better cooperation is also required because the dispatch of generation changes much more rapidly than before liberalisation, which means that international network flows change more rapidly. Increased cooperation is also necessary in real time, as network disturbances tend to affect multiple control areas, so that multiple TSOs are involved in the management of contingencies.

#### **3.3.2 International network**

In Section 3.2, the general socio-technical structure of a decentralised electric power system was described. Now we will discuss the connections between electricity systems. Physically, electric power systems are linked by interconnectors (tie lines). Electric power systems can be connected synchronously (with alternating current (AC) lines) or asynchronously (with direct current (DC) lines) to neighbouring electric power systems. In a synchronously connected area, the frequency is the same in all the connected electric power systems. See Figure 3.8. The international power system can be divided into a number of synchronously connected areas with asynchronous connections between them.



*Figure 3.8. Synchronous and asynchronous connections*  
Source: De Jong (2004a)

In Europe, there are three large synchronous zones: the Nordel Synchronous area, the UPS/IPS synchronous area and the UCTE system. The United Kingdom and Ireland are isolated synchronous areas (UCTE, 2004b). Figure 3.9 shows the synchronous zones to which the different TSOs belong. Because there may be multiple TSOs within a country, the boundary between two different synchronous zones may run through a country. For instance, the east of Denmark belongs to Nordel, while the west is part of the UCTE. Generally, however, the boundaries of synchronous zones follow national borders. The different synchronous zones are operated independently from each other. The TSOs in each synchronous zone are jointly responsible for system operation in their zone. Each synchronous zone has an association of Transmission System Operators (UCTE, Nordel, and UPS/IPS) for the coordination of technical matters among the TSOs (UCTE 2004b).

ETSO is a continent-wide organisation of European TSOs. Whereas the organisations that are associated with the synchronous zones TSOI, UKTSOA, NORDEL and UCTE concentrate on technical issues, ETSO

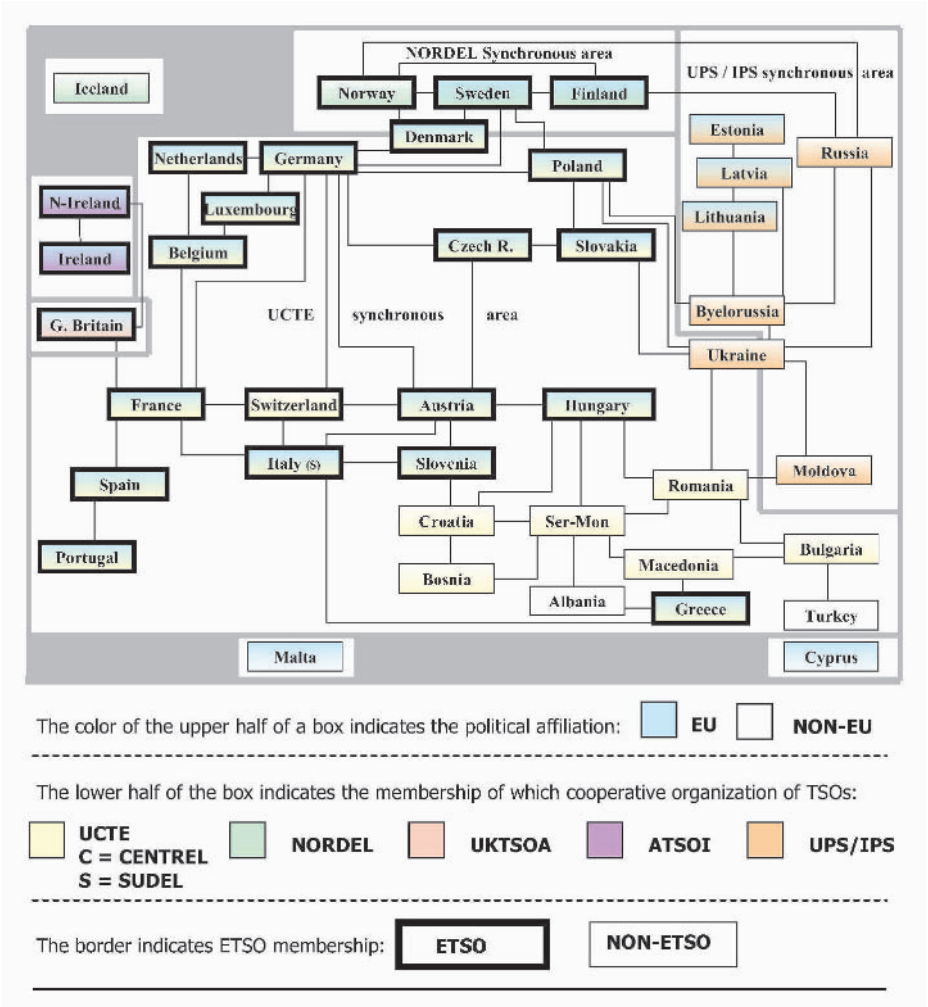


Figure 3.9. The physical structure of the European electric power infrastructure

Source: De Jong (2004b)

has a more regulatory focus. Its main goal is to contribute to the harmonisation of conditions for network access and usage in Europe (ETSO, 2004).

### 3.3.3 Congestion of interconnectors

The EU uses the following definition of congestion:

*“Congestion” means a situation in which an interconnection linking national transmission networks cannot accommodate all physical flows resulting from international trade requested by market participants, because of a lack of capacity of the interconnectors and/or the national transmission systems concerned.*’ (Regulation (EC) No 1228/2003).

We will use this definition here, including the limitation to interconnectors. This inclusion is somewhat odd because congestion may just as well occur within a single electric power system, as is the case in countries like Norway, Sweden, the U.K., Spain and Italy. However, in these cases the management of congestion is not within the jurisdiction of the EU.

#### Congestion management

Congestion management, the manner in which scarce interconnector capacity is allocated, has a profound impact upon the dispatch of generation resources and the economic relations between the electricity markets that are linked. In principle, the same methods can be used to handle congestion of an interconnector and congestion within an electric power system. In practice, the involvement of two or more TSOs and two or more regulators in the case of congested interconnectors creates organisational and juridical complications.

Different congestion management methods are used in Europe. For example, the cross-border capacity between the Netherlands, Belgium and Germany is allocated through explicit auctions, whereas the Nordic System uses market splitting and the France-Belgium cross-border capacity is assigned on the basis of first come, first served. The presence of an effective and efficient congestion management method is a necessary condition for the development of a successful regional market. Following is a brief overview of congestion management methods. One may roughly divide the existing approaches to congestion management in four categories:

1. Corrective methods,
2. Distributive methods,
3. Pricing methods,
4. Optimisation methods.

### 1. Corrective methods

Traditionally, congestion is handled by the TSO(s). Redispatching of generation resources (increasing the output of some power stations and decreasing the output of others) is the traditional means of congestion management within a vertically integrated utility company and is still the real-time remedy to congestion. Counter-trading is a somewhat more market-oriented method, where the TSO calls for bids to increase or decrease output (De Vries and Hakvoort, 2002).

#### Redispatching

The market trades as if network capacity is unlimited. As a result, a single electricity price develops. To avoid physical overloading of a congested link, the TSO intervenes in the generation pattern on both sides of the link by instructing generators on one side of the congested link to increase their output and generators on the other side to decrease their output. He requests reimbursement from decreased generators and needs to pay increased generators. The costs are socialised in the network tariffs.

#### Counter trading

Like redispatching, counter trading allows market parties to make their transactions without consideration for congestion. If the resulting power flow leads to congestion, the TSO creates a second market in which he requests generation companies to reduce generation on one side and increase generation on the other side of the congested line. Such changes of generation involve costs for which bids are to be submitted to the TSO. Like in the case of redispatching, the costs are socialised in the network tariffs. Both counter trading and redispatching have the advantage that they provide the TSOs with an efficient incentive for expanding the network. A disadvantage of both methods is that they may provide significant opportunities for manipulation to generation companies. In many European countries redispatching (or counter-trading) is the main congestion management method inside the control area; however, these methods are rarely used for interconnectors (DG TREN, 2002).

### 2. Distributive methods

Distributive methods of congestion management are methods by which the capacity is not assigned based on the willingness to pay but *on other criteria*. Two common distributive mechanisms are priority and pro-rata assignment.

### Priority

Parties receive capacity in a priority order until all available capacity is allocated. Examples of priority criteria are: chronological order (first come first served) and allocation based upon past use of capacity.

### Pro rata

Requests for capacity are partially accepted in the way that each participant is granted a fixed share of his requested capacity amount.

As will be discussed below, distributive methods will not be accepted under European legislation much longer.

## 3. Pricing methods

Pricing methods regulate access to the congested interconnector through some form of a price mechanism (De Vries, 2004). Essentially, pricing methods are forms of auctioning. Here, we will discuss implicit and explicit auctions.

### Explicit auctions

In explicit auctions the use of transmission capacity is offered to the highest bidders in regularly recurring auctions. The auction revenues can be used for network expansion. However, the congestion rents do not necessarily provide an incentive for the expansion of the network, nor an indication of an efficient level of network investment.

### Implicit auctions

In an implicit auction, the auction of transmission capacity is integrated with the spot market. The transmission capacity is implicitly auctioned: it is allocated to the highest bids in the spot market that make use of the congested link. Thus the energy and capacity bid are combined in a single package. Market splitting and market coupling are extensions of implicit auctions (EuroPex, 2005) in which the case-by-case method for managing structural congestion makes room for a more 'zonal' approach.

*Market splitting* requires that all bids that make use of the congested link are submitted to an organised power exchange. Without congestion, the power exchange is cleared normally, with a single clearing price. In case of congestion, the operator separates the generators into groups on either side of the congested link and creates separate clearing prices for each group. The two market prices are determined in such a way that just so much power is generated on the side that feeds the congested line that the line is used to its capacity. The concept can be applied to weakly meshed networks where congestion occurs in single power lines. A variant that is feasible in highly meshed networks has not been developed, except

if nodal pricing (locational marginal pricing) is considered to be this. Market splitting is used in Nordpool.

*Market Coupling* is a mechanism in which market parties may only trade in the exchanges of their own countries. The power exchanges then combine cross-border supply transactions up to the maximum capacity of the interconnectors (Giesbertz *et al.*, 2005). Energy will flow from the low price country to the high price country to the maximum extent possible. The mechanism of market coupling provides exactly the same results as the market splitting mechanism, only with a different starting point. The difference is that in the case of market coupling, different markets, each with their own power exchange, are coupled to the extent that the available interconnector capacity allows. In case of market splitting, only one power exchange is involved. Market coupling is expected to be used for the NorNed cable (DTe, 2004) and in the 'Benefran' project on the borders between the Netherlands, Belgium and France (EuroPex, 2005).

Compared to corrective methods, pricing methods create the opposite incentives for the long term. Pricing methods provide an efficient signal to generators regarding the cost of using the congested link but they do not provide the TSOs with an incentive for optimal capacity expansion (De Vries, 2004). Facing this choice, pricing methods appear preferable.

#### *4. Optimisation methods*

Locational marginal pricing (also known as nodal pricing) is a centralised congestion management method that can only be applied in an integrated market (in which the TSO also is the market operator). Using generators' and consumers' electricity bids, the TSO establishes a different price for each node in the network (for each time period) such that optimal dispatch is achieved while congestion is avoided. This method is conceptually more elegant, as it is the only congestion management method that fully takes network constraints into account. However, it is also complex and because it only works in an integrated electric power system, it is not suitable for Europe's decentralised electricity networks.

The Regulation (EC) 1228/2003 provides specific guidelines on congestion management being issued by the Commission (De Jong, 2005b). The regulation prescribes that congestion management methods must be market-based. The attached guidelines for congestion management also state that in case the scheduled commercial transactions are not compatible with secure network operation, the TSOs shall coordinate to alleviate the congestion in compliance with the requirements for operational security while keeping any associated costs at an economically efficient level, for example through redispatching or counter trading.

### The calculation of available transmission capacity

The volume of capacity that is auctioned is generally determined by the involved TSOs. There is a conflict between technical and economic interests, that is, the security of supply versus sufficient capacity for exploiting arbitrage possibilities (De Jong, 2005b). There is no unique relationship between the commercial transactions and the actual physical flows. In general, cross-border flows do not coincide with 'border commercial exchanges'. In fact, within the UCTE network there commonly is a significant physical flow in one direction, while net cross-border trade is in the other direction (ETSU/EuroPex, 2004). Once electricity is produced and fed into the network, it travels along the transmission grid according to the laws of physics, which means that all possible network paths are used inversely proportional to their resistance. Consequently, the actual physical load flow depends upon numerous factors within a large geographical area and is therefore difficult to predict. Transmission system operators carry out load flow-analyses in order to forecast possible congestion. These analyses ask for an intensive information exchange and cooperation between neighbouring TSOs.

Liberalisation has led to an increasingly intense use of electricity networks. This makes accurate prediction of the network load increasingly important. However, developments such as short-term trading and the expansion of fluctuating production units such as wind turbines makes actual flows even more difficult to predict.

New coordination systems which increase the exchange of information between neighbouring TSOs improve transparency and therefore have a positive effect on the security of supply and on competition. The TSOs of 21 European countries recently implemented a new load flow coordination system (Klaar, 2004). This system, the so-called 'Day Ahead Congestion Forecast' (DACF), provides for an extra check of system security on the day before operation. TSOs exchange a variety of forecast data, composed after market closure, on the basis of which accurate security calculations are made for the next day. More coordination and consequently more accurate predictions on future system status may lead to lower required reserve margins on cross-border transmission capacity, which would increase the amount of capacity that is available to the market (De Jong, 2005b).

### **3.3.4 Market integration**

Now that we have described the physical connections between electric power systems and the way that the capacity of these links is calculated and allocated, it is time to turn to the development of international



electricity markets: market integration. While a single ‘internal’ market is a long-standing goal of the EU, the idea that the development of regional markets is a necessary preceding stage to the creation of a single European electricity market is broadly accepted. An important reason is that many interconnectors are chronically congested, as a result of which trade between regional markets is limited. With respect to market integration it is useful to distinguish the supranational level (relations between European institutions and other actors) from the multinational level (relations between actors of neighbouring countries) because the relations between parties are quite different.

Supranational perspective

Figure 3.10 depicts the structure of the current supranational actor network in Europe. Box 3.1 describes the role of each of these actors. The main difference with the multinational actor network is the presence of the European Union as an international government, which has given rise to a number of international interest groups and international discussion platforms.

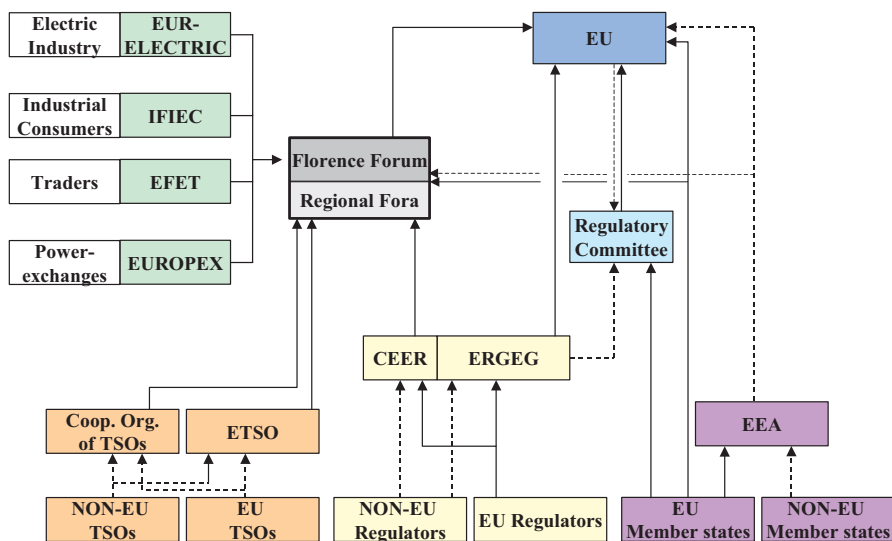


Figure 3.10. The supranational actor network  
 Source: De Jong (2004b)

Through supranational regulation the European Union lays down the ground rules for market integration. The regulatory processes which lead to new or adapted supranational regulation (Regulations, Directives and Guidelines) are quite complex. Box 3.2 describes the current European regulatory processes that affect electricity markets in detail. The fact that European supranational regulation is not specific and flexible enough to fully control the successful formation of regional markets means that there is a need for additional multinational coordination and harmonisation.

### **BOX 3.1: SUPRANATIONAL ACTORS**

#### Market Participants

At the supranational level, there are various interest groups of market participants, such as EFET for the electricity traders or EUROPEX for the interests of the various European power exchanges.

#### Regulatory Authorities

The Council of European Energy Regulators (CEER) is an association of energy regulators of the member states of the European Union (EU) and the European Economic Area (EEA). Alongside this council, a Commission Decision formally established the European Regulators Group for Electricity and Gas (ERGEG) on 11 November, 2003 (EC, 2003a). This group of member state regulators assists the European Commission with consolidating the internal energy market, in particular with respect to the preparation of European regulation. ERGEG has as a task to facilitate consultation, coordination and cooperation of national regulatory authorities in order to contribute to a consistent application of the European regulation. Experts from the European Economic Area (EEA) and from states that are candidates for accession to the European Union may attend the meeting of ERGEG as observers. At the moment it is

rather unclear what the exact relation is between the CEER and ERGEG, other than that ERGEG has an official advisory status and CEER does not. Currently, the same representatives take part both in CEER and ERGEG.

### Governments

Representatives of the various governments of the EU member states form the European Commission, which submits draft proposals for European Regulation. In addition, member states' government representatives take part in the Florence Forum, the relevant regional fora, and in the Regulatory Committee. The role of these fora and committee is explained in Box 3.2. The governments of non-EU member states that are part of the European Economic Area have the right to be consulted by the European Commission during the formulation of legislation but have no voice in the decision-making process (European Union, 2004a).

### Organisations of Transmission System Operators

In Europe there are various organisational associations of Transmission System Operators. Organisations (TSOs) like UCTE and NORDEL (UCTE, 2004a) focus on technical issues, while ETSO aims at EU-wide harmonisation of network access rules, especially with respect to cross-border electricity trade (ETSO, 2004). ETSO consists of the TSOs of Norway, Switzerland and the 25 EU member states, except for the Baltic States, Malta and Cyprus. There are three synchronous zones, in addition to several electricity systems which are not part synchronous with other systems. These zones are coordinated separately in order to maintain system balance (UCTE, 2004a). See also Figure 3.9 on page 63. In this organisational meshwork a number of special cases and anomalies can be identified:

- Germany is connected with nine different countries all of which are UCTE and EU members, except for Switzerland;
- Denmark and Ukraine are part of two different synchronous zones;
- Switzerland lies in the heart of Europe but is not a member of the EU;
- Northern Ireland is synchronously connected to Ireland and asynchronously to the United Kingdom to which it politically belongs;
- Albania is neither a EU member nor a UCTE member but nevertheless synchronously connected;
- Iceland, Malta and Cyprus are isolated electric power systems.

## **BOX 3.2: THE EUROPEAN REGULATORY PROCESS**

In order to fully understand the design of the current European regulatory process, the dynamics of the European regulatory process regarding electricity markets are discussed first.<sup>6</sup>

### First Electricity Directive

During the late 1980s and early 1990s, the European Commission started to challenge energy monopolies. Despite the clear economic ideas of the Commission, the process towards restructuring was mainly one of political debate and diplomacy. Without sufficient power to formally prescribe a certain industry structure, the Commission had to convince Member States that liberalisation really improved the efficiency of the power industry to the benefit of consumers. However, on July 25, 1996 Directive 96/92/EC was adopted. This first Electricity Directive focused mainly on legal and institutional issues, such as unbundling and network access. However, a vision for a European electricity market, a clear idea of what a common internal electricity market should look like and the major economic principles governing such an internal market, was still absent.

### Florence Forum

After the adoption of the first directive, Member States started its implementation in national legislation. Although the issue of unbundling was addressed in the first directive, major issues with respect to the industry structure and network unbundling remained. In addition, issues like adequacy of supply, system reliability, congestion management, network tariffication and the question of the ultimate market model still remained open. In 1998, the Commission tried to make progress by starting negotiations in what was later called the ‘Florence Forum. In the Florence Forum, representatives of the then 15 European Member States and their regulators, the electricity industry, and consumer organisations discussed these issues under the presidency of the Commission. However, the process basically failed, as Member States could not be enforced to implement the agreements.

### New Electricity Directive and Regulation

On June 26, 2003, Directive 2003/54/EC concerning common rules for the internal electricity market (replacing Directive 96/92/EC) and Regulation (EC) 1228/2003 on conditions for access to the network for cross-border exchanges were adopted with the aim of improving progress

in the formation of the single European electricity market. Although the second directive again prescribes legal and institutional issues, the directive also opens the door to more specific instructions. It is accompanied by a 'Regulation', that provides the possibility to establish specific legal binding guidelines on cross-border trade. For the first time, some attention was paid to the economic principles behind a single European electricity market (De Jong, 2005a).

#### Comitology procedure

To establish guidelines for cross-border electricity trade, the Commission is required to follow the comitology procedure as prescribed in article 5 and 7 of Decision 1999/468/EC. In the prescribed procedure, a Regulatory Committee must assist the Commission. In practice, the Commission drafts guidelines for the internal electricity market in close co-operation with the advisory committee, the European Regulators Group for Electricity and Gas (EREG). However, the Commission can only adopt measures if it obtains the approval of a qualified majority of the Regulatory Committee, which consists of representatives of the member states. If the Committee approves the Commission's proposal by majority, the defined measures become binding guidelines. The comitology procedure therefore provides the Commission with a relatively flexible instrument for establishing specific binding regulation.

#### Regional mini-fora

Despite this possibility for more specific and flexible European regulation, the integration process was still not developing smoothly. On March 1, 2004, the European Directorate-General for Energy and Transport (DG TREN) published a 'strategy paper' containing its medium-term vision for the internal electricity market. This vision was developed in response to request by participants in the Florence Forum. In the paper, the Commission recognises that most European electricity networks are not particularly well interconnected and that certain regions have already adopted common harmonised rules. Therefore, the Commission focuses on the development of cross-border trade and launches the concept of 'regional markets'. Issues such as the rules for bilateral trading, for standardised day ahead and intra-day markets as well as balancing, congestion and ancillary services could be developed first on such a regional basis. Nevertheless, there will remain a need for a minimum degree of harmonisation with which all Member States must comply. Moreover, regional markets should not differ too much in their basic design in order to facilitate eventual full integration into a single European electricity market.

In line with this idea of regional markets, in September 2004 the Florence Forum reached an agreement on the establishment of a series of regional mini-fora. Seven different regions were identified, each region consisting of a group of neighbouring countries. Some countries are part of more than one region. The fora were intended to provide an effective platform for the Commission, relevant regulators and for TSOs for meeting regularly in order to make progress with the integration process. The first task of the fora was to provide a plan and a detailed timetable for the introduction of at least a day-ahead co-ordinated market based congestion management mechanism.

The first series of mini-fora were held in the period of December 2004 to February 2005. The results of this first series are a number of general conclusions on congestion management methods, coordinated congestion management, legal issues with respect to congestion management and transparency. The conclusions will be taken into account by the advisory committee (ERGEG) and the European Commission while proposing an agreed set of Congestion Management Guidelines. The conclusions of the mini-fora are also reported to the Florence Forum. It is not yet clear whether a second series of mini-fora will take place in the future.

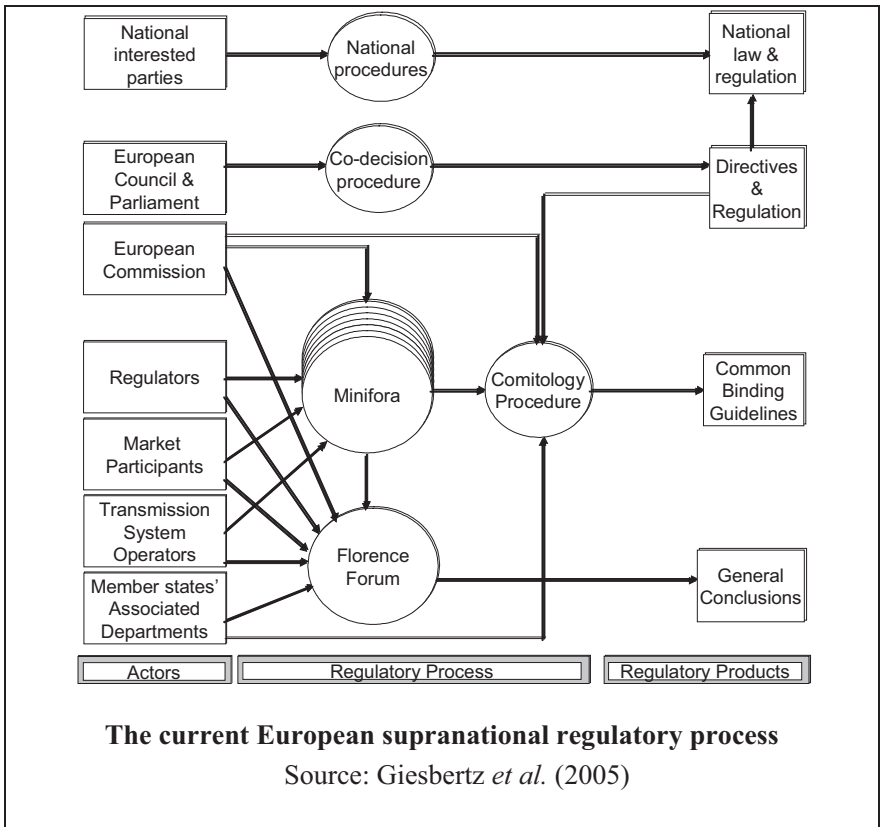
#### The European regulatory process

These developments have led to the current design of the European regulatory process, which is visualised below. It is quite complex, as several different discussion platforms and regulatory procedures exist.

#### Multinational perspective

So far, regional market integration is the result of the initiative of market players and close cooperation between TSOs or a regulatory process with political support. Typical for regional markets is that agreements are on a bilateral or multilateral basis; lacking an international hierarchy, regulatory processes are consensus-based. The multinational actor network describes the relations between the actors. Figure 3.11 shows the institutional relations between two connected electric power systems.

Figure 3.12 depicts the economic relations between two connected electricity markets. Market parties trade in the different national or international power exchanges and in bilateral markets. An example of an international power exchange is NordPool. As discussed above, an important aspect of the international economic subsystem is the treatment of congested interconnectors. In order to trade, parties need to secure access to the interconnector capacity between the countries. Finally, traders need to manage their imbalances. The involved TSOs solve the remaining imbalance through the balancing market(s).



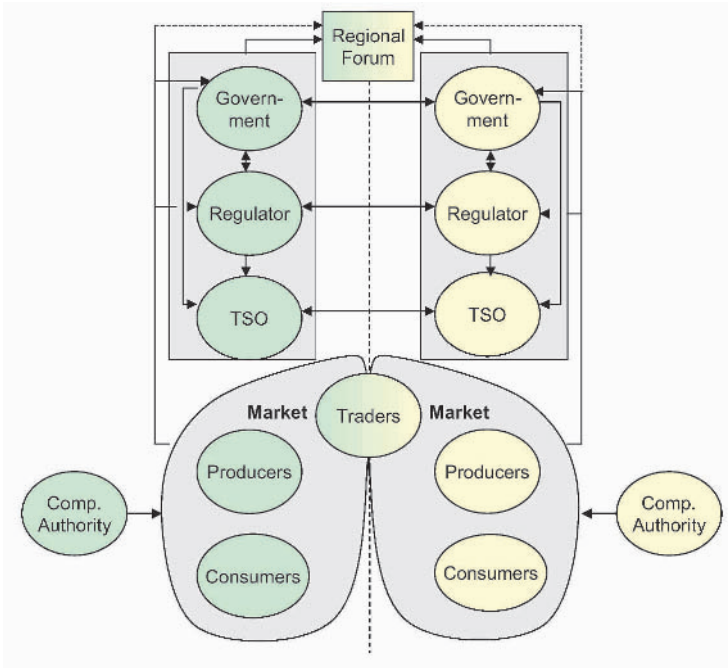


Figure 3.11. Multinational actor network  
Source: De Jong (2004a)

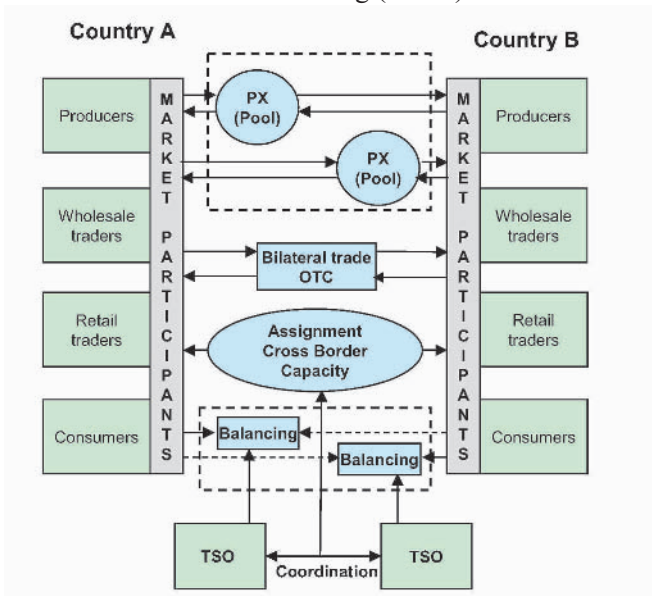


Figure 3.12. Economic subsystem, international  
Source: De Jong (2004a)



### Integration aspects

The management of the electricity network in continental Europe is characterised by a great heterogeneity (DTe/CREG/CRE, 2005). Further integration can be achieved in many different aspects, such as:

- *capacity calculation methods*: intensive cooperation and coordination between TSOs (real-time information exchange, introduction of more coordinated calculation methods);
- *congestion management methods*: implementation of integrating mechanisms such as market coupling/splitting;
- *regulatory monitoring*: international exchange of confidential information between regulatory authorities (e.g. regarding market power);
- *transparency and possibility of access to the respective market*: implementation of an international harmonised minimum of market transparency;
- *balancing mechanisms*: access for foreign market participants to the national balancing market/the integration of different balancing markets;
- *environmental regulation*: harmonisation of environmental regulation.

Although a number of integration initiatives have been taken, the European integration process is highly complex and therefore developing slowly.

## **3.4 System Security**

### **3.4.1 Introduction**

In this chapter we have seen that the liberalisation and internationalisation of the European electricity markets have led to:

- fragmentation of system control,
- increased international electricity exchanges,
- increased complexity of the system (both in technical and institutional sense),
- increased tension between economic and technical interests,
- increased unpredictability and violability, and
- increased dependence upon ICT.

As a result of these developments, the safe operation of the electricity system has become a challenging task. In this paragraph the specific

factors that threaten system security are discussed, as well as the current institutional framework for system operation.

### 3.4.2 Factors that threaten system security

Prior to the introduction of competition in electricity markets, most European national grids were – and to a large extent they still are – self-sufficient. However, current electricity markets rely increasingly upon international exchanges of electricity increase, as a consequence of which international security management is becoming more and more important. Especially during reliability-threatening events, current procedures and routines in cross-national electric power system operations are unsatisfactory. Recent large-scale power disturbances in both the U.S. and European electricity grids were able to cascade from one electric power system to another because system operations could not react fast enough to mitigate disturbances that occurred in parts of the interconnected network that were controlled and monitored by other system operators (cf. U.S.-Canada Power System Outage Task Force, 2003; Eurelectric, 2004a).

According to the overview of recent electric power blackouts and near misses in Appendix 1, the following factors may pose risks to system security:

- *Technical failure of critical grid components.* The unanticipated outage of critical infrastructure components such as generators, transmission lines or transformers (due to causes such as e.g. ageing, overheating, extreme duty) may put the system into emergency conditions.
- *Inadequate inspection / maintenance practices.* Inadequate maintenance may lead to an increase in equipment failure.
- *Adverse operation of line protection devices.* The automatic disconnection of one or more critical transmission network components due to an apparent fault may accelerate the geographic spread of a failure and reduce the available time for intervention by an operator.
- *Too sensitive settings of generator protection devices.* The “early” disconnection of generators because of protection devices settings, which are more sensitive than required by the grid connection rules regarding frequency and voltage disturbances, adversely affects voltage and frequency control.
- *Inefficient Load Shedding.* Inadequate automatic or manual load shedding can actually contribute to the development of a blackout.
- *Insufficient cooperation and communication between operators.* Inadequate joint emergency procedures and data exchange among the involved TSOs, and between the TSOs and the distribution and

generation operators respectively, can be a critical factor in case of a contingency.

- *Insufficient system overview by operators.* Insufficient real-time information about the power system may lead to inadequate assessments of the situation followed by inadequate countermeasures after a contingency.
- *Adverse behaviour of the operator.* Unanticipated human failure by operators (generation, transmission or distribution) can influence the extent of a power failure.

The following factors were identified to complicate and delay the restoration after a widespread blackout:

- *inability of generators to switch on the house-load operation,*
- *insufficient generators with black-start capabilities, and*
- *failure of electricity-dependent telecommunication.*

While most European national authorities have formulated binding regulations with respect to many of these factors, centralised control and management does not exist at the international level. Given the changing system requirements and the results of recent blackout investigations, international security management has proven to be a significant issue.

### 3.4.3 The institutional framework

#### European legislation

The European Directive 2003/54/EC lays down the obligation for Member States to define safety criteria (Article 5). These technical rules should ensure the interoperability of systems and should be objective and non-discriminatory. In addition, the Directive determines that each TSO is responsible for managing energy flows in its system, taking into account exchanges with other interconnected systems. A TSO is responsible for ensuring a secure, reliable and efficient electricity system and, in that context, for ensuring the availability of all necessary ancillary services insofar as this availability is independent from any other transmission system with which its system is interconnected. The TSO is also obliged to provide to the operator of any other system with which its system is interconnected sufficient information to ensure the secure and efficient operation, coordinated development and interoperability of the interconnected system (Article 9). However, the Directive's rules regarding system reliability and security of supply are quite general. Moreover, apart from few general remarks, scant attention is paid to international issues regarding system reliability.

Regulation (EC) no 1228/2003 on conditions for access to the network for cross-border exchanges in electricity, which came into force on June 26, 2003, adds some general rules concerning and congestion management and the exchange of information about interconnection capacities between TSOs. Article 8 of the Regulation provides the possibility to adopt and amend binding guidelines on the following cross-border issues:

- inter-TSO Compensations,
- harmonisation of the underlying principles for the methodology to charge producers and consumers for their network usage,
- congestion management, and
- common rules on minimum safety and operational standards for the use and operation of the transmission network.

To establish guidelines for cross-border electricity trade, the European Commission is obliged to follow the comitology procedure (see Box 3.2). The main idea is that the comitology procedure provides the Commission with a relatively flexible instrument to establish specific binding regulation. At the time of writing, ERGEG has drafted guidelines for inter-TSO compensation and congestion management which are ready to enter the comitology procedure.

International system security and reliability currently is handled through voluntary guidelines between the members of TSO organisations like UCTE and Nordel. However, as discussed above, The Regulation 1228/2003 provides the European Commission with the possibility to incorporate more specific binding guidelines.

#### UCTE operational handbook

At the 11<sup>th</sup> Florence Forum (see Box 3.2), the UCTE presented its plan to adapt the ‘old’ operational rules to the needs of the current electricity markets by developing an Operational Handbook (OH). This would need to be accompanied by a new Multilateral Agreement (MLA) to make the new set of rules contractually binding on all UCTE members. According to the UCTE (2004b), the Operational Handbook has several goals:

- to provided clearer and more precise technical rules,
- to provide a comprehensive and structured summary of all existing documents,
- to allow for the rapid establishment and review of rules,
- to adapt the old rules to the new regulatory and market environment,
- to provide additional measures and monitoring criteria, and
- to create binding security and reliability standards which can be enforced legally.

The UCTE Operation Handbook is a collection of relevant technical standards and recommendations in support of the technical operation of the UCTE interconnected grid, including operational policies for generation control, performance monitoring and reporting, reserves, security criteria and special operational measures. The basic subject of the Operation Handbook is the interoperability among synchronously connected control areas (UCTE, 2004d).

Figure 3.13 provides an overview of the different regulation schemes for network security. It is important to emphasise that the UCTE’s Multilateral Agreement, as a private agreement, does not replace existing or future national or European law or regulation.

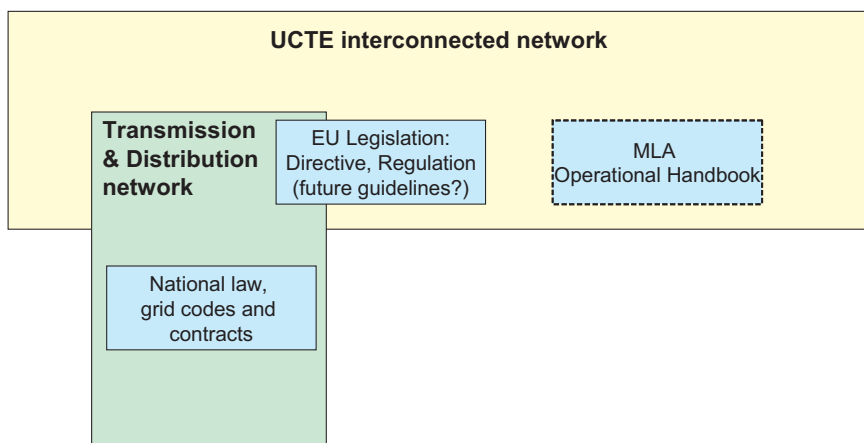


Figure 3.13. Regulatory overview  
(Based on UCTE, 2004c)

On July 1, 2005 the MLA came into force, including the first three policies: *load-frequency control and performance (p1)*, *scheduling and accounting (p2)* and *operational security (p3)*. Seven policies are foreseen all together; *coordinated operational planning (p4)*, *emergency procedures (p5)*, *communication infrastructure (p6)*, *data exchanges (p7)* and *operational training (p8)*.

An important advantage of UCTE’s OH and the underlying MLA is that the technical rules and standards which are incorporated in the OH also apply to TSOs which are situated in non-EU counties (for example the Swiss TSOs). Another advantage is that the rules are quite flexible and made by experts. However, the latter also is an important drawback, as the

rules are made from a single (TSO) viewpoint and do not necessarily represent the interests of other parties.

#### **3.4.4 Compliance and enforceability**

Considering UCTE's initiative of constructing an Operational Handbook with 'new' operational rules, the implementation of effective compliance monitoring and enforcement procedures forms a vital requirement. Ensuring the binding character of the 'new' operational rules is needed to truly take a step towards a higher level of international system security and reliability. Besides some naming and shaming options there is no compliance and enforceability process present.

Here, a parallel can be drawn between the North American Electric Reliability Council and the UCTE. Also the NERC has a weak position regarding enforcing their reliability standards. Up till now the NERC only relies on compliance reviews and simulated enforcement actions (NERC, 2005).

A major difference between the NERC and UCTE is that NERC contains members from all segments of the electric industry. In this way a variety of interests is taken into account. However, both the UCTE and NERC (and consequently their rules) have no structural independence from the industry/TSOs they represent.

Both in North America and Europe there is a need to make security and reliability rules mandatory and enforceable. At least some regulatory involvement seems to be necessary to ensure transparency, accountability and credibility. Here, Europe could learn from the American experience.

### **3.5 Conclusions**

After introducing a conceptual model of the electricity supply industry, this chapter has described two of the main trends that affect the European power system. By distributing the control over the physical system among many actors, liberalisation has led to a significant increase in the complexity of the power sector and fragmented responsibilities among many different actors. For instance, individual generation companies in a competitive market can no longer be held responsible for the total volume of generation capacity. Whereas the regional monopolies of the past could be held accountable for virtually every aspect of the performance of the electricity supply system, now a number of functions are provided collectively by 'the system'. As a result, the institutional design of the system has become crucial to its performance.

At the same time, the electricity supply system is becoming more international. This trend pre-dates liberalisation, but liberalisation has

given a strong impetus to international market integration. In principle, international trade should allow for a more efficient use of the generation resources in different countries. In practice, however, much trade is due to differences in tariffs, taxes and subsidies and therefore not necessarily economically efficient. The trend of internationalisation also poses risks: it further increases the complexity of the system, both at the technical and the institutional level, and it creates a risk of cascading failures, where failures in one system bring down connected systems. Although the European TSOs have taken the initiative to develop their own operational rules with respect to international system security, there is no solid monitoring and enforcement system in place. Furthermore, the rules are made from a single viewpoint – that of the TSOs – and do not necessarily represent the interests of other parties. At least some regulatory (independent) involvement appears necessary for ensuring transparency, accountability and credibility.

A third significant trend, the increasing penetration of information and communications technology into all levels of the electric power system, will be discussed in the next chapter.

## Chapter 4

# The Security of Information and Communication Systems and the E+I Paradigm

*Marcelo Masera, Alberto Stefanini, Giovanna Dondossola*

### 4.1 Introduction

This chapter will discuss the Information and Communication Systems (ICS) used in the electric power infrastructure, in light of their relevance for the occurrence and the management of risk-relevant situations.

Electronic technologies found their way into power systems early on, mainly as an effective means for implementing control and protection mechanisms. The applications of those technologies, evolving from analog to digital systems, have expanded at accelerated pace. This evolution has been driven by, among others, increases in processing power, and decreases in costs and size. This massive incorporation of computerised and networked devices has changed the same character of power systems, bringing the electric power infrastructure into a new paradigm. We have denominated this the **E+I** paradigm, a new infrastructural service, namely “Electricity plus Information”, characterised by the integration of both elements.

At the same time, it has enhanced the operational and monitoring capabilities, provided means for protecting against contingencies, and paved the way for new threats, partly due to the fallibility of ICS, partly due to their connectedness and openness that facilitate malicious attacks.

In this light, it is clear that the analysis of the risks of the electricity infrastructure has to take into account the information security aspects of ICS. In order to clarify the topic, the chapter will discuss the diverse conceptual frameworks that exist for dealing with security issues.



For the purpose of analysing the potential impact of ICS failures, the chapter will examine typical applications, their vulnerabilities and the threats that can jeopardise them, and the possible countermeasures.

The chapter ends with a discussion of the main initiatives and groups working on relevant standards, as well as the applicable generic standards in the information and communications fields and their significance in the context of power systems.

## **4.2 The Evolution Towards the E+I Paradigm**

### **4.2.1 ICS and electric power systems**

There is no doubt that the growth of power systems and the establishment of the power infrastructure as we know it today, would not have been possible without the extensive use of ICS. An easy conjecture is that, taking into consideration the capabilities of ICS technologies and the needs of the electric power industry and markets, this trend will continue in the future. An understanding of this evolution will help with assessing the positive and negative consequences of this trend.

The incorporation of digital electronics in electric installations started when the European power industry had already gone through a rather long history. The infrastructure developed since its origins in the late 1880s based on electromechanical technologies. The progress of the sector required more capabilities for the control and protection of the generation, transmission and distribution devices. Electronics provided them first with single devices and later with the first digital computers. In the 60s, the availability of the first computerised systems changed the approach to the implementation of automatic controls. However, the massive use of computerised solutions was “preceded by developments in technologies used to regulate, switch and monitor the grid” (IEEE, 2000).

The evolution of the power infrastructure required technical and organisational innovations that based upon computer and telecommunications technologies. At the same time, the increases in the production of electricity, in the span of the power lines, and in their interconnections have been facilitated and enabled by digital systems.

The net result derived from the use of digital electronics has been, among others, better measurements (e.g. voltage, frequency), quicker operations, more powerful control schemes, and broad access to data.

Therefore from the functional and operative standpoints the positive effect of ICS is clear.

But there remains an open question about the influence of ICS on the vulnerability and risks of the European Critical Electricity Infrastructure (ECEI), considering the pervasive use of ICS in all industrial operations, technical, administrative and market related. For approaching this problem, let us examine the ECEI contextual factors and the ICS technological factors that shape this issue.

The main ECEI contextual factors are:

- Power demand in Europe is growing continually and, although this growth can be estimated, it cannot be easily satisfied at the required quality levels. This forces the operation of many ECEI systems near their functional limits, which requires tighter monitoring and control. (it should be mentioned that this trend also exists in other places, such as the USA).
- The ECEI is a system-of-systems (see Chapter 3), composed of several synchronised zones (UCTE, NORDEL...), each one of which comprises multiple national or regional systems; the coordinated management of all these resources requires an extensive exchange of information in real-time, so as to comply with functional, operative and security constraints.
- The reorganization within and between the power companies induced by the evolution in the European industry in the last 10 years, mainly driven by the liberalisation and unbundling of the sector (the establishment of national electric power markets and the institution of independent regulators and transmission systems operators) in the majority of European countries are demanding new data acquisition and communication means for supporting the increase and quality of the data exchanged among the industrial and market actors.
- More interconnections and new generation and distribution architectures result in an increased complexity in the plans and operations required for securing the system. New control and protection strategies are required, supported by innovative devices and technologies
- Current trends in power generation and distribution, such as the integration of renewable sources (wind and solar), distributed generation and microgrids, require new ICS functions: real-time data for the integration of available power resources, local and wide-area control strategies for preventing and protecting against

security events, and intelligent management of the interconnections and the loads.

- Equipment maintenance, whether electromechanical or ICS, is heavily dependent nowadays on remote access to the facilities and the local use of portable ICS devices.

On the other hand, the incorporation of ICS is affected by two internal factors:

- the advancement and affordability of microelectronics technologies (multiplication of capabilities and radical decrease in prices), and
- the easy availability of inexpensive communication channels (internet through direct links or dial-up connections, cellular telephony, satellite, different wireless communication means).

These external and internal factors positively feedback into each other: as soon as ICS technologies are available, industry makes use of them; while in parallel, there is a continuous flow of new demands (more efficiency, access to more data, new services to customers, etc.) requiring new ICS applications.

## 4.2.2 The evolution of ICS

For understanding the effects of ICS on the electric power infrastructure, one needs first to understand the evolution of the applications used to gather, store, process and distribute data, because there have been remarkable changes, many of them occurring during recent years.

In the near past (let us say up to the late 90s), ICS were “isolated”, i.e. were not connected to open public networks. In other terms, ICS were either stand-alone in close contact with the physical equipment, or remotely connected through communication networks owned and operated privately, by the same power company or by a trusted partner. These systems were usually designed and developed by a single vendor, using proprietary technologies. Protocols have been standardised mainly in the IEC context (IEC, 2003), but the connectivity to open communication networks did not play a role in their development.

As far as communication systems are concerned, in Europe several of the power transmission and distribution operators deploy their own dedicated networks (mainly based on fiber optics). This was seen as a natural extension of the companies’ resources. In recent years, the evolution of the telecommunications markets has as a consequence that many of

these lines deployed by power utilities had an interesting economic value and were sold to telecommunication companies – some of them initiated by the same power operators.

This is affected by a financial factor: companies may find it more convenient to pay for a communications service when needed, than having to arrange, run and maintain their own system. This goes hand in hand with the trend in the corporate world to concentrate on core business. As a consequence, power companies, based on mere cost aspects, are tempted to choose external services. These are usually “open” services, which means that the communication lines are open to universal access. Anyhow, it is technologically possible to set up secure solutions that arrange a private communications channel over a public line – in the so called Virtual Public Networks (VPN).

The new capabilities empowered by the continuous development of the digital technologies have been, and are, appealing for the power industry: they are easy to acquire, yield immediate results, facilitate several processes and technical tasks. However, these advantages come at a price that is not always acknowledged: security. ICT technologies, as a general rule, have not been developed with industrial applications in mind – less so for critical systems. Some applications are arbitrary, providing a small convenience while increasing the risks – for instance, wireless communications. Moreover, information and communication security has not been an issue for the power sector, neither at the corporate or at the technical level: ICS assurance and security have not been a subject of discussion at corporate headquarters, nor were points considered in standards.

One may ask why ICS security has not been a key element of the risk management agenda of the power sector until very recent years. The simple answer is that: 1.) dedicated ICS applications were not a main source of concern, with failures that could be managed within acceptable limits; and 2.) the isolated nature of ICS made them out of reach for external malicious threats, and very difficult to attack without specific knowledge and actions from within the power companies.

A typical application that makes use of communication networks makes use of a limited number of remote control centres for managing a significant number of geographically distributed nodes (e.g. primary substations, power stations). Control centres are the key components of the system from the technical management standpoint. They are the main interface with the operators, have the current and historical information on the system performance, and support the setting and handling of the field equipment by means of supervisory control and data acquisition (SCADA)

system that handle the local remote terminal units (RTUs). In the control centre, the energy management system (EMS) runs the operational applications, keeps the information, and presents synthetic diagrams and reports to the operators.

The links between field equipment and central control rooms transmit signals that are vital to the operation of the electric system, e.g. commands and alarms. And with the increase of smart devices, more data will be available and will flow. On the one hand, intelligent electronic devices (IEDs) that can process the operations in the field are being deployed, complementing or even replacing the old RTUs; on the other, new wide-area measurement systems (WAMS) are proposed for monitoring some vital stability variables; and the EMS of different operators are being interconnected for the need to elaborate common understandings of the systems operational status.

In addition, one also needs to bear in mind that the range of potential communication channels is becoming more varied: apart from owned or leased lines, it is now possible to tap other types of transmission means: cellular telephony and satellites for long distances, different wireless modes for short distances.

In the light of security, one needs to bear in mind the following negative side effects:

- In current control systems, new applications and legacy ICS coexist. Old systems were not designed for security, but their vulnerabilities are generally not publicly known; several technologies employed in new systems were not designed for industrial control, and are typically based on standard technologies with well-known vulnerabilities.
- The architecture of power systems lasts much longer than that of the ICS components. The ICS life-cycle is relatively short, determined by the evolution of technologies. So, original security requirements may not be satisfied with subsequent changes of ICS components, and new vulnerabilities may materialize. This generates an unstable and rather unpredictable environment difficult to assess.
- The current availability of specialized security equipment for industrial automation in general, and power systems in particular, is rather limited. Specialized solutions that take into consideration the specific requirements of industry (e.g. real-time, safety) are in their initial stages. Generic solutions for information systems (e.g. firewalls, antivirus, intrusion detection, encryption) are not directly

applicable, as they can introduce harmful variations in the control functions (for instance, unexpected delays).

“Isolated” control systems, in spite of the potential improvements offered by connected control systems, are still an option of course. The impression is that this will only be justifiable in industries with the highest safety concerns – as for instance nuclear power stations. In other situations, the potential access to real-time information from a multitude of points in the corporate network will give good reasons for the networking of ICS – this in spite of the insight that connections are not fully secure. Two caveats are worth bearing in mind:

- An internal link between the industrial ICS and the corporate network may suffice to allow a cyber-threat to reach the reputed “isolated” system.
- A set of business partners perform tasks in the electric power installations, mainly related to maintenance functions. Their workers will likely use some computing and communication devices (laptops, PDAs, etc.) which can be easily connected to open networks. If no specific provision is taken, the possibility of improper communication links is not negligible.

In summary, the integration of ICS has fundamental consequences for the electric power infrastructure – most of them very positive from the operational and protection point of view, but with potential negative security implications that need to be taken into account.

### **4.2.3 The E+I paradigm**

The massive integration of ICS have propitiated substantial changes in the European electric power systems, a transformation that affects the very own nature of the ECEI infrastructure. The infrastructure no longer consists merely of electricity generation, transmission and distribution, but of electric power along with information. Information is central to the control and protection operations, to the running of the business, to the interrelationships with other companies, to the links with regulators, to the final services with customers. Electric power companies are electricity- and information-based companies. We call this the **E+I** paradigm.

Electric power is obviously the reference point: statistics, tariffs, commercial results, environmental policies, etc., are centred on it. In this view, electricity is about the physical phenomena that determines the dynamics of the current flows, voltage and frequency fluctuations, electromagnetic emissions, and power consumption. In addition, in the context of the national economies, electricity appears as installed power

and energy consumption. The physics of power obviously continues to prevail, but in the industrial and market reality of the power infrastructure it cannot be dissociated from information (and actually digital information treated by ICS): from the electrical variables measured and digitalized to the management processes, and the exchanges of data between the industrial and market actors. The pervasive dependence on information is changing the internal constitution of the electric power infrastructure, and the ways it relates with other socio-technical systems and it interweaves with society. Therefore there is more than just the widespread use of information and communication technologies.

In recent years, following the liberalization of the electricity markets in Europe, the commercial aspect began to take a prominent position. Market agents refer to quantities that are information and that are only indirectly connected to the physical reality of megawatts. Derivatives, pricing structure, broker offers, rebates, stranded costs, settlements, etc., all these market items have an influence upon the overall governance of the infrastructure, equivalent to that of the grid operation. The scenario presents a symbiosis of electricity as industrial product, and electricity as market commodity.

The internationalization and the interconnectedness of the power infrastructure in Europe brought about new changes. The picture was broadened with jurisdictional aspects due to the raising importance of cross-border traffics, the need to coordinate defence plans and security policies, world-wide environmental agreements (e.g. European sulphur protocol), etc. Electricity and Information began to go hand in hand. The discussions regarding policies, and specifically security and risk related ones had to taken into account both aspects.

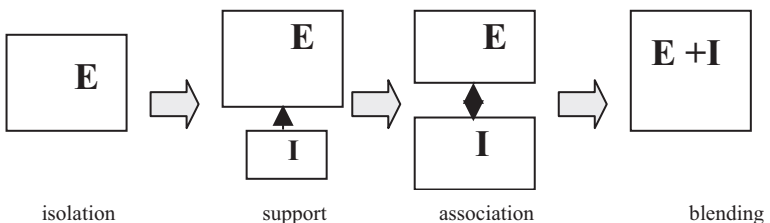


Figure 4.1 Evolution towards E+I

We expect this trend to consolidate in the future. Markets and operations, protection and consumer services, links and merges between companies, investments and incentives, user acceptance and aversion of risk and costs, etc., all is permeated with information. Electricity and

information will constitute a unique vector. This is the emergence of an **E+I** scenario.

Four phases can be identified in the evolution towards the **E+I** paradigm (IEEE, 2000):

1. During the 50s and 60s, power systems were growing at a fast pace in order to satisfy the fast growth of demand, caused by the industrialisation processes in the majority of the European countries. Electronics were used as soon as they were available, as well as on-line tools such as frequency relays and off-line tools such as analog simulators. **E** was isolated, and the loop with **I** passed through human beings.
2. In the 70s, digital electronics began to replace the functions that were previously performed by electromechanical and analog equipment, e.g. direct control over some functions. Analog and digital equipment coexisted for some time. In parallel, computing centres were implemented for data storage and business administrative functions. **E** received direct support from **I**, first at the equipment level, then linked to entire installations.
3. By the mid-80s, fiber optics for communication data, and active protection devices based on digital solutions begin to spread. Power systems become wired and computerised. Reliability rapidly increases, and the major capabilities of the computerised devices support ever more complex functions. The possibility to have remote access to distant facilities pushes the development of communication networks. Dispatch centres begin controlling more and more substations. The diffusion of the internet affects all business processes. **I** transforms into an indispensable partner of **E**.
4. From the late 90s on, companies and national infrastructures become fully digitalized. Data flows grow profusely between the industrial and the business sides of companies. Energy markets function on line. The vast interconnection among national grids is not just accompanied by enabled by ICS. Sensors and actuators can be reached through a variety of communication means. On the one hand, power systems had the possibility to implement more and more powerful functions. On the other, the pervasiveness of information allows new functions across systems. **E** and **I** become fused into a single reality: **E+I**.

The **E+I** scenario presents security challenges that are not only more numerous or more complex than in the previous periods, but are also different in nature. The **E** branch of security cannot be analysed or solved



without consideration of the **I** branch. The **E** and **I** parts cannot be aggregated, but the compound infrastructure **E+I** requires a joint security approach.

## 4.3 The Impact of Digitalization on Security

### 4.3.1 The various roles of ICS

The above discussion shows how digitalization has changed the electric power infrastructure. The situation, characterised by a continuous incorporation of ICS technologies, presents positive and negative aspects: more control and monitoring is possible and new adaptive operating strategies are enabled, but each new equipment adds vulnerabilities, and each new connection is a potential open gate for a malicious intrusion. The more ICS, the more operational and protection capabilities, but also the higher the exposure to risks.

There is an undisputable trend towards more access to real-time data, and more ICS dedicated to the automation and coordination of monitoring and control, partly for the goal of a better efficiency and partly for preventing and remedying contingencies. The net result can be interpreted as an arms race between the incorporation of digitalized capabilities and the addition of vulnerabilities, a process that demands an unremitting endeavour towards the securement of the infrastructure.

So the question is: what is the real contribution, positive and negative, of ICS? What could be an adequate solution? And who is responsible for defining and implementing that solution? In this section we will discuss the roles of ICS and the correlated vulnerabilities and threats. In the following section, the context for the governance of the risks induced by or associated with ICS will be considered.

A first analysis should consider the electric power system as a critical infrastructure, and in this context the uses and effects of ICS should be studied. For this purpose, the electric power infrastructure is regarded as a complex socio-technical system, the relevance of which stretches beyond the implicit business aims of the industrial actors to national security and the welfare of society.

This infrastructure includes many private and public stakeholders, who interact among each other for the fulfilment of a number of objectives:

- Economic objectives: acceptable level of investment and correct performance of the energy market that assures private actors of the reasonable financial returns, customers of the continuity of quality service, and society of support for its growth and efficiency.
- Technical objectives: efficient operation that optimizes the use of the resources, while providing a secure and adequate service.
- Regulatory objectives: fulfilment of all the rules set by the authorities and sector organisations (grid codes, power security, environmental, safety and information security requirements).

In the context of our **E+I** paradigm, the interactions among the stakeholders affect the flows of electric power and information. Next, we will reflect on the various roles covered by ICS, on the requirements demanded by and to the different stakeholders, and on the ways those requirements can enter into conflict or accommodate among them.

### **ICS as enabler of business and technical capabilities**

One should consider the entire life-cycle of the components of the infrastructure, and not just the operational part. ICS are employed from the design of installations, to the empowerment of business processes, and from the integration of technical and administrative functions to the management of assets.

The first consequence of the pervasive application of ICS is that much more data (related to the technical equipment and process and to the business side) are accessible locally and remotely, to the personnel of the company and to other organisations providing services or being interconnected for some operational or business reason.

The following is an incomplete list of the main services (both on-line and off-line) that are enabled by ICS:

1. Services executed by the single electric power company (generation, transmission or distribution of electricity):
  - Business and management functions:
    - Commercial links and trading, customer service, billing
    - Planning and operations (production, human resources, maintenance, procurement),
    - Security, safety and environmental policies execution and control (including physical and logical access control),
    - Asset management.
  - Technical functions:
    - Control systems (including EMS, DMS, SCADAs, RTUs, IEDs, User Interfaces, the local and wide-area networks, ...),
    - Other measurement and protection equipment,

- In-house communications (wired and wireless, within the industrial installations and interconnecting them with administrative functions),
  - Accident and emergency management,
  - Maintenance operations (local and remote),
  - Equipment specification (supported by simulation).
2. Services among electric power companies:
    - Data exchange and coordination of emergency controls (as foreseen in grid codes and the inter-grid agreements, such as the UCTE Operation Handbook (UCTE, 2004)),
    - Grid supervision, protection and control (coordinated by the TSOs, but that requires the active participation of the connected generation and distribution companies),
    - Special Protection Schemes (SPS), including wide area monitoring and protection systems.
  3. Operations related to the electricity markets and the grid:
    - On-line market operations by electricity companies, traders, brokers,
    - Simulation of transients and long term stability of power systems,
    - State estimation and real-time grid security monitoring,
    - Definition and validation of defence plans (against widespread loss of synchronism, under-voltage load shedding, frequency load shedding).
  4. Customer-related services:
    - Smart metering and electronic billing,
    - Energy information services (using data from the customers' meters and market data).
  5. Interrelationships with other infrastructures:
    - Data exchanges with operators and regulators of the other infrastructures (e.g. transport, telecommunications, etc.).

This is of course a long list that will always require updating, which confirms the “Energy + Information” character of the electric power infrastructure and the need to develop a proper strategy for assessing and managing ICS-related risks.

### **ICS as an indispensable tool for managing the security of electricity supply**

The instability of power systems has been one of the key concerns since the very beginning of this industry. The relationship between power reliability and electricity market design is currently a major topic of debate. Liberalisation is driving the European system towards more and

more changeable electricity flows and more stressing operation conditions that are closer to the physical and functional limits of the infrastructure.

The solution has always been to develop adequacy requirements for power security and stability and to apply ICS tools. The management of security is evidently affected by the evolution of ICS technologies. We will consider the following conceptual structure of security of electricity supply (Eurelectric, 2004a). Each of these aspects is facilitated by the application of ICS:

- Long-term security: supported mainly by off-lines ICS tools.
  - Access to primary fuels: models and decision support tools for planning and management.
  - System adequacy:
    - Generation adequacy: this is a resource issue, which can be supported by modelling and simulation tools for predicting market needs and for planning.
    - Network adequacy: this is a resource and co-ordination issue (including the handling of cross-border interconnections), that can be supported by the planning, management and monitoring of the transmission and distribution grids, data and projections from consumers and other network users.
  - Market adequacy: can be supported by facilitating the links between producers and consumers, planning and simulation of market and regulation changes, and the trustworthiness of the market processes.
- Short-term security: supported by online and off-line ICS tools.
  - Operational security: this is a function of appropriate technical reserves, all necessary system services for the operation, and the real-time balance of supply and demand in the electricity market.

This last point deserves a more detailed description: reserves in a liberalized market follow a business logic, as the costs cannot be automatically passed to consumers as in a monopoly market. A solution to this issue requires data and an intervention in the electricity market and in the technical operation of the system. Further support can be given with a smarter management of present and future loads, e.g. by advanced metering of end user consumption and by rich energy information services.

### **ICS as source of security risks**

This vast range of business and technical capabilities and power security functions increases the risk of information and communication

security threats. The scale and magnitude of the impact of ICS security failures can only be ascertained with specific evaluations and with reference to the context in which the ICS operates. The networked nature of the system does not allow for disregarding events that a priori may seem negligible.

It is generally accepted that due to the current state-of-the-art in the development of computer-based systems, and perhaps due to the intrinsic nature of computer programmes, industry cannot help but produce software that contains flaws. ICS are complex by themselves in their specification and functioning. They make use of multiple instruments and components (e.g. operating systems, compilers, debuggers, protocols) whose verification is by and large beyond the control of ICS developers. And the environment where they are applied, i.e. electric power systems, is very dynamic, which makes the operating conditions difficult to predict.

The layering of ICS shows a broad set of opportunities for failures:

- ICS components may include faults deriving from its incorrect design or development, improper application;
- Its deployment in a certain operational medium may cause physical deterioration of the hardware or a negative physical interference (e.g. electro-magnetic effects);
- The combination of various ICS may bring about interaction faults;
- The interaction with human operators is prone to accidental errors, such as input mistakes, and malicious intrusion attempts;
- The connection of ICS to open networks paves the way to logic bombs, viruses, worms and external intruders.

There are mechanisms for coping with these potential failures of ICS, but they are only applied in industries that are considered safety-critical – mainly for cost reasons. And still these solutions are fallible: fault prevention (with specific design rules and techniques such as modularization), tolerance (with the detection and handling of errors and faults), removal (e.g. with verification and validation techniques) and forecasting (with quantitative and qualitative evaluations) have matured during recent decades, but they cannot guarantee fault-free systems. The great majority of these solutions are or make use of computer-based systems, which can be faulty themselves.

At the highest level, the electric power system as an infrastructure, the failures are experienced as service interruptions. These failures, the reason for being concerned about the criticality of the electric system, can be partially traced back to the previous list of ICS failures. Studying this should be the object of thorough risk assessments.

Not only the vulnerability of each company and the attention to business continuity, but also the vulnerability of other infrastructures that depend on the correct functioning of the electric power infrastructure is at stake, as well as the vulnerability of society to the breakdown of a vital service underpinning the well-being of the population and fundamental governmental functions.

### 4.3.2 Lessons from recent incidents

In recent years, both Europe and America experienced a significant number of large blackouts (see Appendix 1 for a detailed account). Although these incidents were not caused by cyber-incidents, it is beneficial to reflect upon the negative aspects of ICS in those circumstances, and the potential positive support that additional ICS could have provided.

The following box presents an account of the main ICS-relevant reasons of the Italian blackout of September 28<sup>th</sup>, 2003.

#### **Reasons for the Italian system collapse and its protracted restoration**

**E4.** The missing adoption of the foreseen (i.e., UCTE) countermeasures resulted in the inefficiency of the control logic of the critical sections to defend the integrity of the grid in front of cross-border interconnections (...)

On September 28, 2003, the missing adoption of the foreseen countermeasures has determined a chain of events which rendered the automatic control of the critical section Rondissone-Albertville and of the foreign critical section ineffective (...)

**E5.** The separation of the national electrical system from the UCTE grid has been characterised by phenomena of transient instability of the Italian electrical system with respect to the UCTE grid. (...)

**E6.** The spread of interruptions in Italy: after the separation of the national electrical system from the UCTE grid, the spread of service interruptions in the national territory was caused by a series of concurrent events: primarily, the anticipated separation of power generation units with respect to the prescribed terms and, second, an ineffective reaction by the load separation system. More specifically:

**E7.** During the service interruption spread phase, the behaviour of 21 power generating groups was patently different from what was established in the technical rules of connection to the national transmission grid.

**E8.** The entire automatic load relief action did not comply with the levels established by the technical connection rules. Moreover, several distributors connected with the national transmission grid were not equipped with automatic load relief devices (...)

**E9.** The failure rate of the load rejection actions by power generating groups was very high. This seriously compromised service restoration. (...)

**E10.** In most cases the independent start of the first blackstart units did not take place. The GRTN managed to restore service only through the lines that connect the north to the rest of Italy. This caused the remarkable delay of service restoration in the centre and south regions (...)

**E11.** During the service restoration phase, the telecommunication systems for remote control of components of the national transmission elements grid experienced instability and overload. Moreover, the emergency supply system of the above telecommunication systems was inadequate. (...)

From hours 08:00 to hours 14:40, it was impossible to use the automatic control system because of lack of supply, due to inadequacy of the emergency supply systems of the relevant telecommunication systems. This required the use of a backup satellite telecommunication system and manual restoration, thus delaying the restoration of service.

**Source: (AEEG, 2004)**

These events presented a common pattern: several ICS (intended as the composition of technologies and procedures for system management, comprehensive of monitoring, actuation and protection devices) appear to be no longer adequate:

- Not all relevant alarms are displayed on the operators' screens, due to either jurisdictional issues or inappropriate procedures. This was very clear in the case of the blackout in Italy, September 28, 2003.
- Current assessments of the electric power system do not identify accidental threats to information and communication, not to mention malicious threats. There is an assumption, not always explicit, that ICS will always work as requested, or that their failures will be covered by other risk management measures. However, in the case of the North America blackout (August 14, 2003) various EMS components failed.
- Defence plans and their implementation by means of different ICS do not match current risks. In several of the blackouts the defence plans plainly failed and automatic protection systems were not able to prevent the collapse of the electric service. Moreover, in

some cases the protection mechanisms aggravated the situation as they were more orientated to the protection of the asset than to maintaining electricity service.

- There are indications that the interactions with the information infrastructure, mainly services in emergency situations, were not analysed in advance in detail from the perspective of risk. In the Italian case, inadequacies in the communications support caused the restoration to be long and cumbersome.
- To better manage contingencies, operators need better access to germane real-time information for improving their understanding of the system. Given the many actors involved, this requires standardised formats for data reporting, also across borders. The most recent versions of some grid codes and the UCTE Operation Handbook point in this direction. However, it can be expected that its realisation will take some time.
- The implementation of more powerful disturbance monitoring equipment is required, to monitor and manage large area disturbances. The relevant technologies have been under development for some years, and Wide-Area Measurement Systems (WAMS) are beginning to be applied for this purpose. They need to be integrated with the ICS. The derived information from real situations or test experiments can have a greater value when shared among operators.

The main lesson from these events is that the ECEI urgently needs more and better ICS: systems that can help in providing a broader understanding of the situation, even across national borders; enhanced implementation of the defence plans; more complete assessment of the potential contingencies; among others. The following box discusses some of the lessons of the blackout from the point of view of the vulnerabilities of Defence Plans.

### **Defence Plan Vulnerabilities**

All control actions (both manual and automated) to prevent a power system from entering an emergency condition, or to restore it into a normal condition after an emergency, are usually defined as Defence Plans. (In the following we will take as example the Italian plans). Manual control actions in response to a complex event, which usually generate a large number of alarms, require at least 10 minutes to be executed. When response times need to be shorter, automated control devices are used. These may be either local, like most protection systems, or use a more complex logic.



A critical section is usually defined as a set of 380 kV lines the loss of which would result in the separation of a portion of the grid. Critical section control is intended to prevent separation by disconnecting some load after a number of lines are opened by the relevant line protection. The load that is disconnected by the critical section control is the minimum required to avoid separation of a portion of the grid and the subsequent triggering of an Automated Load Shedding Plan. Two vulnerabilities of these essential systems are:

Lack of coordination among different systems:

Each critical section control activates its own load shedding plan. The main drawback of such a choice in a highly interconnected grid is that load shedding in one area may bring other areas out of balance. For this reason, the load shedding thresholds are based on sensitivity analysis. Since liberalization, load shedding systems operate on MV distributions; hence they are under the jurisdiction of several different power companies. At the same time, the load shedding control scheme has not been updated, resulting in system inadequacy. This was a main cause for the Italian September 2004 blackout, because only 32% of load was shed, instead of the required 50% of total load.

Communication throughput limitations:

Currently, data acquisition and communication are based upon SCADA systems. Typical control architectures are based on communication systems unable to match hard real-time constraints. For this reason, the trend is towards high speed dedicated communication systems using the multicast protocol IEC 870-5-104 (an IP version of the IEC 870-5-101).

A different approach could be based upon coordination among different systems, i.e. either a centralized or a distributed approach to load shedding. However, this would be very demanding, at least taking into account the strongest real time constraints (10-20 msec):

- extremely large (10-20 kbit) data patterns had to be exchanged and elaborated in 10 msec (transfer rate over 10 mbit/sec);
- over distances in the order of 300-400 km, communication delays would be in the order of 5 msec. Over wider distances this approach would become unfeasible.

### 4.3.3 ICS security and the Grid Codes

There is consensus that the current situation is inadequate: *“The lack or inadequacy of communication, co-ordination and/or data exchange*

*between system operators seems to have played a major role in the escalation of some of the examined events” (Eurelectric, 2004b).*

It is important to note that one of the main recommendations of the specialists that analysed the blackouts is to make reliability and security standards mandatory and enforceable, with penalties for non-compliance (UCTE, 2004). The UCTE Operation Handbook (June 2004) – which may be considered an answer to the request by the Florence Forum in 2002 and 2003 to establish common security and reliability rules – defends the position that reliability and security standards should be binding and legally enforceable. This fits with the proposed Directive of the European Commission on Infrastructure and Security of Supply, which in Article 4 focused on anti-blackout measures and calls for compliance with agreed operational norms for secure network operation. It is worth mentioning that the NORDEL system has a binding System Operation Agreement since 1999.

In the UCTE setting, the rules for access to the national/regional grids are given by the local Grid Codes, while the UCTE Operation Handbook (OpHB) defines the rules for interconnection. The OpHB, which can be taken as representative of the European situation, is a compendium of technical standards, compiled as a means for ensuring electric power system security within a legal framework.

OpHB’s Policy 3 presents the approach to operational security, describing system safety as the primary goal reachable through the co-operation of the various TSOs during normal, contingency and emergency operational conditions. Policy 6 deals with the communication infrastructure provided by UCTE for data exchanges among TSOs.

Key are therefore the information exchanges among the TSOs in the various UCTE and NORDEL policies, but no particular attention is given to cybersecurity issues. Nevertheless, it is easily understandable that issues such as authentication of users, confidentiality and integrity of the data and availability of the communication channels are important concerns. Considering the large number of nodes of such a network, the definition, management and enforcement of a security policy and the application of the due security functions will not be an easy task. In addition, the goal of broad data exchange among all relevant actors is not easily reachable because the practices of TSOs differ and each operator is constrained by the regulatory framework of its country.

Considering that the OpHB will be implemented before long, some reflections should be dedicated to the links between the risks stemming from the operation and performance of the electric system as such, and the risks that stem from failures that are initiated or aggravated by the

associated ICSs. Two aspects can be identified: the assessment of the risks and the management of those risks.

## 4.4 ICS Security Risks

### 4.4.1 ICS security attributes

The security of ICS components is of such importance that it calls for a systematic treatment (see Appendix 5.2 “ICS Security Standards” for a discussion of the continuing standardisation initiatives in the field). There is the awareness that due to the increasing complexity of the topology and operation of the infrastructure, ICS failures may cause extended system instabilities. Furthermore, malicious attacks have now to be taken into full consideration: critical infrastructures, and the electrical system primarily, are potential targets of warfare and terrorist attacks. This needs to be studied from both the physical and cyber perspectives.

The ECEI has not been subject to a thorough assessment, nor has a course of action been set or initiatives been taken for dealing with this issue in its entirety. Some companies may have carried out internal security analyses of accidental or malicious cyber incidents, but a methodical and complete infrastructural assessment appears necessary, due to the internet working of the national systems. A comprehensive approach will require some common understanding of the issues and therefore a shared terminology and appreciation of the problems.

#### **Security requirements related to ICS**

Conventionally, the overall goal of the electric power system is “*the ability to supply adequate electric service on a nearly continuous basis*”. This objective, valid for the infrastructure as a whole, needs to be complemented, in a more comprehensive risk assessment view, with the avoidance of some unacceptable negative situations for the involved stakeholders: financial losses for the power companies; safety and environmental damages; economic, physical or privacy-related detriments inflicted to the end-users.

As ICS are concerned, these high-level conditions can be translated into a set of security requirements. This operation would require completing a proper security assessment. In the following we will make some general

reflections on the typical requirements to be specified in each particular case.

Each ICS, as a component of the general electric power system, is expected to provide some services: generally, the acquisition, storage, processing, transmission of digital data. These services are characterised by fundamental properties (Avizienis, 2004; Laprie, 1992): functionality, performance, cost, security, usability, manageability, and adaptability. These properties interact among themselves in intricate ways, which are not always transparent for the designers, developers and operators of the ICS. For instance, an increase in performance may decrease the security of the system, by demanding the most difficult operating conditions; moreover, an expansion in functionality may mean that more data will be available to the operators, affecting the usability.

The security of ICS can be expressed as a set of constraints on the states that the system can take. The total state of an ICS is determined by its states with respect to computation, communication, stored information interconnection, and physical condition (Laprie, 1995). The consideration of ICS security requirements can be divided between control systems and corporate information systems.

For control systems (i.e. SCADA, EMS, etc.), the following are standard requirements:

- **Integrity**: is the absence of alterations, e.g. to the data or the software components. Data should maintain their accuracy and validity during their entire life cycle, from their generation in a sensor or operator interface unit, through their communication links, to their final usage or storage. The communication part outside the power company industrial perimeter and the protection of data against malicious attacks are aspects that demand greater attention today.
- **Confidentiality**: is the absence of unauthorised disclosure of information. This has not been a concern for industry until now. Process data were not considered assets with a special business value beyond their operational use. Therefore, no attention was given to the need for special protection. But these data can reveal sensitive business information to competitors, or to malicious intruders (for instance with the intention of committing fraud).
- **Availability**: is the readiness for correct service. It is obviously vital for the continuous operation of power systems. An unavailable ICS puts the system at risk. It is useful to distinguish between lack of access to stored data, data processing failures and failure of a communication link. Depending on the context, the dangers may

vary. A special situation is when data is not available when required but with a certain delay; this is an issue of timeliness.

- **Timeliness:** is the readiness of data when required. Control loops have real-time constraints, while for other types of data delays may be acceptable within certain margins. In certain situations, e.g. in emergency conditions, timeliness is a vital provision.

As far as corporate information systems are concerned (i.e. finance, billing, human resources, asset management, the different planning applications, etc...), the security requirements have a slightly different flavour: real-time is not an issue, but usually many more people have access to data, and many more connections exist (including external actors). This requires stricter control of access by personnel and by all external authorized persons to computing and communication resources. Moreover, it should be taken into account that there are increasing exchanges of data with the industrial information systems, and so a breach into a company's own system may cause others also to be at risk.

Therefore the security for ICS corporate systems needs to be managed with proper security assessments with respect to the top security objectives of the electric power company. Integrity is fundamental because violations to the correctness and validity of the values may create significant business risks. Confidentiality of sensitive business data is obviously important because intruders may obtain information about key physical and logical assets and create more damage with that information. Availability of data and key computing and communication resources is by and large needed, yet in this context it should be referred to the situations where the unfeasibility to access some data or resources may be a cause of critical security risks.

### **ICS vulnerabilities**

The above listed requirements may be violated when an external or internal event, either accidental or deliberate, results from a weakness in the ICS.

The following categories of vulnerabilities may be discerned:

- **The engineering design process:** the current state-of-the-art for the design of computer-based systems does not ensure the production of flawless artefacts. In the industrial side, there is a need to consider both software and control issues, two disciplines that have different approaches and methods for the design of ICS. With the intense use of telecommunications, a new factor is added. Data transmission used to be mainly a local networks service, but now, with a multiplicity of communication channels (some of them

open) potentially involved, it should be considered as a complex issue of itself. The deficiency in the design methods apply to both the applications and the security measures (e.g. encryption).

- Software implementation: the best design can be ruined by its implementation. The use of COTS and of standard technologies introduces vulnerabilities, in spite of the best efforts by developers. Some of these flaws may not be apparent for long periods. Their unlikelihood does not make them less risky. In addition, insufficient validation and verification may pose a threat. Together they create a lack of security assurance for ICS. New standards are intended to mitigate this problem.
- The communication links: the use and protection of data transfers is a source of increasing concern, mainly because of three causes: the easiness to deploy communication nodes, the lack of security provisions in current protocols, and the reliance on third parties for data transmission services. The latter requires trusting others to adequately manage security mechanisms. The variety of communication channels is expanding, both wired and wireless, and the majority have neither enough protection, nor capabilities for assuring their availability in critical situations such as emergencies.
- The physical security: apart from remote access, another line of attack is physical intrusion, interference or destruction of an ICS. It should be realized that people outside the electricity companies have access to the installations.
- The maintenance process: ICS needs to be maintained. While wear-and-tear process is not as important as for physical electricity system components, it does affect ICS hardware devices. However, software elements need to be maintained with escalating rate. This is critical for industrial ICS: updating or upgrading them may create undesired effects, not doing so may leave them open to attacks or failures.
- The man-machine interface: most ICS need to interact with operators or other personnel. As more data is generated or processed, there is the temptation to present ever more information in the human interface. But the situation might become difficult to understand and even lead to wrong interpretations. Contingency management and emergency situations are particularly demanding in this respect.
- The administration of security: a security policy needs to be implemented, enforced and verified. The management process

itself is prone to faults. Managing a meta-functional property such as security is much more difficult than managing more concrete elements, which can be followed by means of measurable variables.

### **Attacks to control systems**

Not many incidents have been reported, especially in Europe. However, it is revealing to mention some of the incidents that are publicly known:

- Unknown intruders hijacked the servers of an electricity company in November 2000 and used them for hosting games and playing online. The attackers exploited a vulnerability in the file storage service (Source: National Infrastructure Protection Center, December 2000, <http://www.nipc.org/>)
- A server in a control centre at Ohio's Davis-Besse nuclear power plant was infected with the Slammer worm. Apparently the worm reached the server through the corporate network, and propagated till blocking the SCADA traffic for five hours. (Source: NERC, SQL Slammer worm lessons learned for consideration by the electricity sector, June 2003, <http://www.nerc.com>).
- A former disgruntled employee took control remotely via a wireless link of the SCADA system of a sewage treatment plant. At the utility it was not possible to explain the failure. (Gartner Research, Prepare for cyberattacks on the power grid, October 2002, <http://www.gartner.com>)
- Hackers tried to repeatedly breach into the computer systems of the California Independent System Operators (Cal-ISO) between April and May 2001. On May 7 and 8 California suffered widespread blackouts but Cal-ISO said that there was no connection between the two facts. Afterwards, Cal-ISO detected and corrected several cyber-vulnerabilities. (Source: Cal-ISO, June 2001, <http://www.caiso.com>)

### **Threats to ICS**

Vulnerabilities themselves can lead to accidental failures. In these situations, operational conditions or external causes affect the service delivered by a component, leading it to an incorrect state. In addition, there is a risk of deliberate activation of the faults. These intentional acts may be malicious attacks (by direct intervention of the human attackers, or by the use of malicious logic, e.g. viruses, worms...) or human errors (e.g. operators who intentionally do something without realising that they are causing the system to fail).

As for the malicious threat agents that can affect ICS, the range is vast. And they can be employing the same tools for very different purposes. A typical list of threats includes:

- Terrorism (countries or groups trying to bring about fear by disrupting society),
- Espionage (countries or companies trying to obtain confidential information about e.g. network topology or market operations),
- Criminal organisations (intending for instance to commit fraud or blackmailing electricity companies),
- Hackers and hacktivists (technically or politically motivated groups that try to break into ICS systems, e.g. to deface public sites).

At the infrastructure level, it is possible to distinguish (Amin, 2002) between attacks upon the power system, attacks by the power system, and attacks through the power system. The first type of action has as an aim to disturb electric power service, for instance by affecting power delivery installations (e.g. substations) and/or the electricity market. The most likely example is a terrorist attack.

The second case is the use of the electric power installations for a different purpose. For instance hacktivists could use part of the infrastructure as a platform for forwarding a political message to the population (e.g. environmental activists).

The third case is to the exploitation of the electric infrastructure for affecting related services. These services may even be related to electric power, as in the case of Power Line Communications (PLC).

#### **4.4.2 Dealing with ICS security risks**

The blackout events demonstrated the lack of a set of uniform risk evaluation methodologies in power systems and their supporting ICSs, and the scarcity of data and analysis of cybersecurity events that can contribute or lead to power system faults (Amin, 2005). A comprehensive view of the cyber risks that could jeopardize European electric power system will require the application of a compatible set of risk assessment approaches. If vulnerabilities, threats and potential failures are ascertained with incompatible methodologies, it will be difficult to add up the results, determine and evaluate best practices, and validate security assurance practices (see Appendix 5.1 “Security Conceptual Frameworks” for a discussion of the links between the concept of security as used in the



electric power sector and in the information and communications technologies one).

In the power industry, the general practice for security assessment is to use a deterministic approach (IEEE/CIGRE, 2004): the power system is designed and operated to withstand a set of contingencies referred to as "normal contingencies". These are selected based on past events, their apparent likelihood of occurrence, and the potential scope of their consequences. In practice, the criterion means that the loss of any single element in a power system "*should not endanger the security of interconnected operation*" (UCTE, 2004). This is usually referred to as the N-1 criterion because it examines the behaviour of an N-component grid following the loss of any one of its major components. The major shortcoming of this criterion is that it does not consider multiple failures in different equipments, when it is known that this is the case in the more significant disturbances, where an original failure is complicated by further control and protection equipment faults, human errors, malfunctions in procedures, etc. This is partly covered by the application of the N-k criterion (i.e. considering more than 1 component failure). But the rapid multiplication of the cases limits this to a very restricted set of cases. The corollary is that a significant set of contingencies will not be analysed.

It should be considered that the N-1 security criterion is implemented in different ways in the various European countries: the elements of the electric power grid. The quantity of the contingency situations that are taken into consideration also differ. Differences in approach mean that dissimilar information in quantity and quality is collected and processed. As an increase in the exchange of information among transmission system operators is being fostered, a certain harmonization in the definition of contingencies would be required. These information exchanges will need to cover various situations in grid contingency (i.e. planning, operation, emergency) that may involve several operators.

The components considered for the application of the N-1 criterion are the typical electric equipment (OpHB mentions "generating set, compensating installation or any transmission circuit, transformer"), but not the ICS. Yet ICS are crucial components of the electric power infrastructure that cannot always be reduced to sub-systems of other components. Let us consider the case of remote control: the communications infrastructure, either owned or leased, is not part of the field equipment nor of the remote control centre – and it can fail independently, potentially exposing the power system to insecure situations. One clear example is the need for real-time data exchange during an emergency situation.

On the other hand, it is clear that the “*inappropriate application of the N-1 principle... clearly contributed to the events in the US/Canada and Italy... Already ongoing investigations on a more flexible probability-based approach, in addition to the N-1 principle, should continue; where the duration, profile and consequences of a blackout can be taken into account in defining the necessary level of defence.*” (Eurelectric, 2004b). This necessary level of defence will require the treatment of each scenario with its particular potential risk, while the typical deterministic approach to risk treats all contingencies as equally likely.

As many incidents were caused by a pattern consisting of an initial fault in a power system that was compounded by concurrent or subsequent failures of monitoring devices and/or incorrect trips of automatic protection elements, a more comprehensive approach to electric power risks appears necessary. This approach needs to consider at least the coexistence of electrical and ICS failures and their interdependencies. The methodologies of recent decades are not conceptually wrong, but they appear only partly useful for current electric power systems: systems-of-systems that are complex, rapidly evolving, and heavily dependent on information and communication.

Inadequate assessments lead to an incomplete understanding of the risks and an underestimation of the role and importance of ICS, in particular of those linked to the protection of the electric infrastructure. These are not fault free devices – they fail, they are vulnerable to accidental faults and to malicious attacks, including both physical and cyber incidents.

This lack of attention to ICS vulnerabilities and threats leads to an underrating of some of the more serious contingencies from the standpoint of critical infrastructures: escalation failures, where a local event develops into a global disturbance; cascading failures, where adjunct systems propagate malfunctions possibly extending to domino effects; and failures linked to a common corridor, where an ICS (typically a communication infrastructure) causes the conjoint failure of other systems dependent on the same basic service.

Although there exist several risk assessment methodologies for power systems, like load flow analysis and transient stability assessment, and testing/compliance control procedures for automation and protection equipment, there is no wide-ranging methodology for evaluating risks arising from power system failures and automation system all together. To the contrary, even reliability and security related terminologies used in the two domains greatly diverge.

### 4.4.3 Impacts and countermeasures

#### Potential impact of ICS threats

A distinction can be made between the immediate effect of the threats to the ICS and the secondary impact on the infrastructure.

Among the immediate effects one can mention:

- Denial of service: an accident or a deliberate act can keep a component from providing its intended service. This may preclude other components or the operators to perform their functions. This may take different technical forms, such as flooding a communications gate or overloading some computing resources. A denial of service can be dangerous still with a limited duration.
- Value alteration: some data in an ICS are changed. This obviously can cause immediate problems for the control of installations, the business administration, the market trading, or the protection of the transmission grid.
- Leakage of information: an intruder gets access to data in violation of authorisation rights. This may be intermediate data which can be used for further penetration into the system, or vital information related to the control of the technical installation or the running of the business. It is evident that the disclosure of key information is a dangerous event.
- Illegitimate use: internal or external users exceed their access permits and compel some computing or communication resource to perform some illegitimate action, or use some information for illicit purposes.

From the infrastructure viewpoint, the impacts can be classified by which part of the system they affect:

- The operation of an electric power installation: a generation, transmission or distribution facility is affected by the ICS failure, causing an unacceptable disruption of the electricity supply service. This is feasible when the control and protection equipment (e.g. SCADAs) fails in one of the previously mentioned ways. In a normal operation condition, any disturbance of the operation of a control device may provoke the failure of an installation. In case of an accident or an emergency, the disturbance of protection equipment might have catastrophic effects.
- The operation of an electricity business activity: a corporate information system suffers a failure that causes a major dysfunction of a corporate action, potentially interfering with the management of the technical system and the market processes.

This can have direct effects on the financial and contractual position of the company and on its corporate reputation; and ensuing effects disrupting the infrastructure.

- The operation of the electricity market: the ICS of the market operator or of one of the participants can disrupt the market functioning. This can take different shapes: corrupting information, masquerading a legitimate market agent, blocking the access to market real-time data.
- The management of the infrastructure: a Transmission System Operator receives wrong data or no data at all from the infrastructure generation and distribution companies; or the coordination among TSOs is disturbed by failures in the communication links. These situations can jeopardize the infrastructure in normal and anomalous situations alike, as it blinds or misguides the system operators.

### **ICS security countermeasures**

There are several types of strategies for tackling ICS vulnerabilities and threats. Among them:

- Management measurements:
  - Security policies: mainly with the application of ISO 17799. Security policies are needed for producing a systematic and reasoned set of functional and assurance measures. This includes the unambiguous identification of all assets, roles and responsibilities. One should consider that these policies need to be certified, mainly in an infrastructure environment where many actors depend on each other.

In the new scenarios, security policies will have to exceed the limits of companies, and establish rules for all interconnected actors, including for instance maintenance services and end-customers. As a consequence of the networking effect, the same company will be affected by the other linked actors, resulting in a web of partially overlapping policies. This new reality is not well studied as or today.

- Security management: the entire life-cycle of the infrastructural system needs to be managed. This is not just a matter of combining isolated measures. Management is in charge of the performance of assessments and of their evaluation in the regulatory and economic context. Management is also in charge of monitoring implemented policies and their efficiency with the purpose of finding potential improvements and unsatisfied security requirements. Management should also ensure that all

technical procedures are observed, including configuration, maintenance, emergency procedures, in light of the security requirements.

- Security assessments: assessments are a must. Without vulnerability, threat and impact assessments, companies cannot know the whys and hows of their security policies and measures. Assessments, and their structure in security cases where the entire rationale behind the evaluation can be documented, are fundamental to certification because they act as proof for regulators. In addition, one should consider that reality is now moving fast, vulnerabilities and threats change continually, and the significance of risks and their requirements should be expected to evolve. Assessments will need to be prepared to change in accordance.

This may include the use of modelling and simulation tools for predicting and understanding the behaviour of complex systems in normal and emergency conditions. These tools can be useful for facilitating the communication between the different actors, and most importantly between industry and public authorities. The preparation for contingencies can be supported by these instruments.

- Engineering measures:
  - Design for security: the improvement of technology is fundamental to the implementation of security measures. This includes the progress in the techniques used in the design of systems. Software engineering, control processes and new monitoring and protection schemes all need to be designed with methods that assure their validity. Although formal methods are difficult and costly to apply, lessons will need to be learnt from safety critical fields where their use is standard (e.g. air traffic control, avionics, etc.)
  - Implementation and procurement using security standards: standards will be decisive for the development of markets for security technologies. As in other sectors, the electric power industry will need to employ assurance levels for the production and procurement of components. Communication protocols, SCADAs, interfaces: all critical equipment will need to be certified according to security standards, according to their level of criticality. Third party assessment will become fundamental.
  - Operation and maintenance according to security principles: ICS will need to be controlled within the business processes and following the security framework defined in the security

- policies. Some arrangements have been proposed (as for instance CobiT (Van Grenbergen, 2003), and SysTrust (Forwnfelter, 2002)). These approaches put together administrative and technical controls. Considering the life-cycle of ICS components, with continuous patching, updating and upgrading actions, a balanced control framework is fundamental.
- Use of proper security technologies: this includes: operating systems and other basic software (current commercial options do satisfy minimum security conditions), cryptographic systems for encoding all information that is sent over public networks or to non-trusted environments. One should remember that several needed technologies are unavailable or in their first phases of development, such as specialised network security tools for industrial environments (e.g. anti-virus, firewalls, intrusion detection, etc.).
  - **Infrastructure measures**:
    - Define and enforce cybersecurity codes (preferably by self-regulation) for the overall infrastructure to be applied by all companies – according to their function. These security codes should include at least:
      - The obligation to certify cybersecurity policies, with a clear definition of roles and responsibilities. Key personnel should receive appropriate training. The infrastructure should develop an accreditation system.
      - The obligation to maintain an updated inventory of key assets (e.g. versions of software packages) and network connections, and of carrying out audits for verifying that records correspond to the real field equipment.
      - A set of continuously updated best practices: access controls, network security, disaster recovery plans, vulnerability assessment, etc.
    - Define a joint effort for the exchange of information on cybersecurity events, vulnerabilities and threats. This may take the form of a public-private partnership per country, consolidated at the European level

## 4.5 Conclusions

The proposed **E+I** paradigm, if correctly identified, signifies that electric power companies, the sector regulators and authorities, and the entire sector, will need to take information and network security as a first priority. ICS will not be an add-on, an element from other industry that can be contracted, a minor nuisance that can be solved with some minor intervention. Information and network security will be at the centre of the business and the corporate strategies, and at the focus of the concerns of the national authorities and the consumers.

What should be done? The best possible horizon is one where power companies and the electric infrastructure as a whole benefit from the ICS technological advancements, while taking the right security measures for dealing with the risks that the incorporation of those technologies will entail. This implies that:

- Power companies will need to develop specific information and network security policies as an integral part of their corporate strategies. This lies beyond the historical culture of these companies
  - Observance of this security policy by company personnel and by the staff of all other companies with access to the company's installations needs to be enforced.
  - Companies will need to manage ICS security with the commitment and participation of the top management.
- The ICS technical solutions will need to be based on proper security technologies. Power companies will need to promote, support and adopt ICS security standards.

The governance of the ICS risks is one of the most important components of the E+I risk governance process. The assessment and protection against these risks will need the involvement of all stakeholders.

## Chapter 5

# Governing Risks in the European Critical Electricity Infrastructure

*Marcelo Masera, Ype Wijnia, Laurens de Vries, Caroline Kuenzi,  
Maurizio Sajevo, Margot Weijnen*

### 5.1 Introduction

In this chapter we will develop a view on the risks and the risk decision processes in the European Critical Electricity Infrastructure (ECEI). We will show that, due to their nature and complexity, the management of some of those risks (the ones with an infrastructure resonance) cannot be left alone to the risk managers within each constituting national or regional power system. The risks to the infrastructure impact society as a whole and have to be governed accordingly – i.e. with the participation of all actors or with acknowledgment of all actors' goals and interests.

We will set out with a discussion of the types of risks and their characterisation. We will propose an approach based on a constructivist conception of risks. The second section of the chapter develops the taxonomy of risks and proposes a risk network for the ECEI, ending with reflections on the valuation and characterisation of risks.

The third section is dedicated to risk governance. Starting with a problem statement we then introduce our conceptual understanding of 'risk governance'. This is followed by a proposal for a risk governance process for ECEI. Two alternatives for implementing this process are explored: a modification of the current Florence Forum, and the institution of a new body, so called 'European Council for the Security of Electric Power', in charge of self-regulation in this area. The chapter explains the characteristics of both alternatives and their presumed mission, objectives, membership and tasks.



## 5.2 Risks in the European Critical Electricity Infrastructure

In this section we will develop an overview of the risks that might affect the ECEI. First, we will define what we mean by ‘risk’, keeping in mind that this book focuses on risks with a European dimension, i.e. events that might cause large-scale effects, involve multiple stakeholders, and have an international scope. The second step will examine the risk space, and show its dimensions and lower and upper limits. As the risk space is very large, we need a categorisation to reduce its vastness into one of manageable size. For each of the risk categories we will test if the normal risk management practices currently in place are adequate.

### 5.2.1 The concept of risk

When discussing risks to complex systems like infrastructures, it is fundamental to make explicit what is meant by risk. Risks are mental “constructions” (OECD, 2003) that do not have the same connotation for all human beings or groups. Societies choose what to consider and what to ignore as risk (Thompson, 1990). For example, in the debate about the risks of nuclear power, a large part of the misunderstanding between experts, authorities, industry and the public could be attributed to the different use and connotations of the concept of risk. Experts used risk as a product of probability and consequence, whereas the public used the concept of risk to indicate the disaster potential (Perrow, 1984).

A few other uses of risk are listed below (based on Slovic and Weber, 2002)

- Risk as a hazard: How should we rank the risk of a terrorist attack to power systems against the risk of a heavy storm affecting them?
- Risk as probability: What is the risk of a blackout caused by a heavy storm?
- Risk as consequence: What is the risk of electricity supply shortages?
- Risk as potential adversity: How great is the risk of liberalising the electricity markets?

The differences in definition can cause misunderstandings and miscommunications amongst the many different stakeholders of electric power systems, but these problems can be resolved by making explicit the sense of what risk is intended to denote in a certain context.

Besides these different meanings of risk, there are also different views on the essence of risk – and this affects how risks are assessed and managed. The first conceptual approach assumes that risk is an entity that can be objectively measured or calculated. In this approach, risks are typically expressed as the product of probability and consequence. This objective risk has three main uses:

1. Financial managers use risk to express uncertainty in financial returns. For example, power companies usually weigh the cost of investments in assets against potential benefits stemming from them. Financial risks not only have negative aspects, but also a positive side given by the potential revenues generated by the investment.
2. Safety engineers use risk to express expected fatality rates. Risk is the product of a negative impact (e.g. casualties, injuries, damages to goods or the environment) and the probability of this impact. In power companies this might be the case of the explosion of a transformer in a substation.
3. Decision analysts use risk to express the attitude of decision makers at uncertainty in decision outcomes. For example, a decision maker who values an uncertain outcome below its expected value is said to be risk averse. In power systems such decisions might refer to the supply of fuel, or to the level of technical power reserves.

However, there are good arguments to challenge the assumption of objectivity, as it is not the product of probability and consequence that determines if a risk is acceptable or accepted. For example, some people take very high risks to their health by smoking, but protest against the possible health effect of electromagnetic (EM) radiation caused by High Voltage transmission lines. The objective risk of smoking is thousands of times higher than that of exposure to EM radiation.

The second conceptual approach therefore states that risks are subjective, meaning that a risk only makes sense when perceived by an individual, the subject. The perception of the risk is shaped by the so called psychometric factors of the risk, which are shown below in Figure 5.1 (Slovic and Weber 2002).

Those nine psychometric factors can be compressed into two dimensions, unknown risk and dread risk. Aspects like *Unknown to exposed*, *Not observable*, *Delayed effect*, *New risk*, *Not known to science* are part of the dimension “unknown risk”, whereas aspects like *Uncontrollable*, *Catastrophic potential*, *Involuntary*, *Fatal consequences*,

*Not equitable, Dread, Increasing risk* populate the dimension “dread risk”. The Figure 5.2 below (Slovic and Weber 2002) shows some common risks valued against those two dimensions.

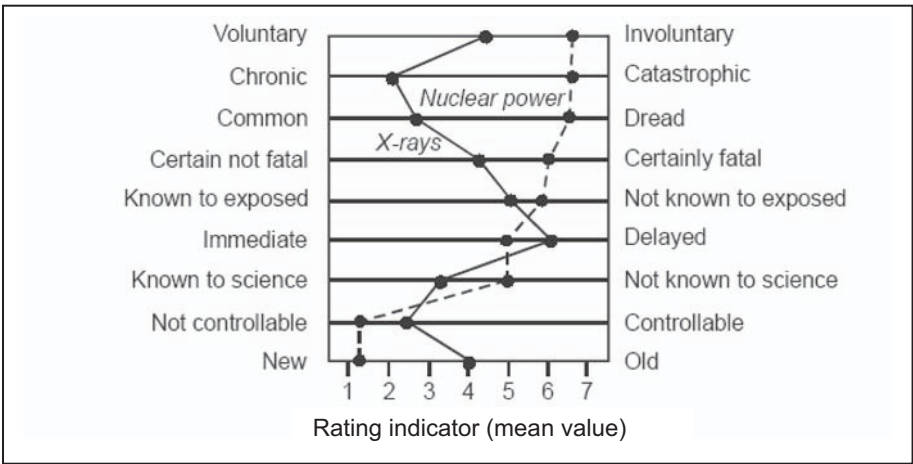


Figure 5.1. Risk perception (Source: adapted from Slovic and Weber 2002)

This concept of subjectivity is very powerful for risk communication, but it does pose serious problems for risk management. For example, if the perception of the risk is determined by its catastrophic potential – as in the case of nuclear power –, no amount of risk mitigation measures will reduce this perception. This means that for some subjects the risk will be intolerable which leaves cancelling the activity as the only risk management solution. However, stopping all activities that have a catastrophic potential might reduce the standard of living by a considerable amount, a sacrifice that few citizens are willing to make.

This is why a third conceptual approach is used, in which risk is assumed to be a social construction that people invented to deal with the dangers and uncertainties of life. In this constructivist approach, risk is characterised with the purpose of creating a better understanding of hazardous situations, in order to help in making better decisions. The dangers and uncertainties related to risks are real, but the risks are only mental constructs. What is considered important is to handle risk situations in such a way as to reach the best possible decision outcomes through a process that includes the analysis of risk situations and the deliberations among stakeholders.



Figure 5.2. Risk values (Source: adapted from Slovic and Weber 2002)

This view on risk is advocated by the USA’s National Research Council in a famous study of 1996. They state that “the purpose of risk characterization is to enhance practical understanding and to illuminate practical choices” (National Research Council, 1996). A risk can thus be defined as *a potential problem that needs to be decided about*. “Risk characterization must be seen as an integral part of the entire process of risk decision making”. This constructive approach to risks combines aspects of both objectivism and subjectivism, but it differs from the first two conceptual approaches to risk in the fact that it is decision driven, and geared towards considering all relevant concerns (and therefore all relevant stakeholders). Its purpose is pragmatic, in the sense of effectively supporting risk decision making. In other words, this approach treats risks as the object of an analytic-deliberative process: the so called risk governance process.

Arguments for supporting this constructive approach can be found in the implicit value judgements made in objective risk assessments, which can be the object of debate among the diverse parties involved (whether directly affected by the potential outcomes, or having a legitimate interest in how the risks are treated). For example, when expressing the safety risk of a certain technology, one could use different risk metrics, such as expected fatalities or loss of life expectancy. These metrics can back decision outcomes that might differ widely, as the second one would allow homes of the elderly to be situated near the risky technology (loss of life expectancy is limited), whereas the first one would forbid that (high fatality rate expected due to the vulnerability of the elderly).

Another argument is that risk decisions not only reflect the objective aspects of risk, but also the relative power of the various stakeholders. Risk situations are usually complex, surrounded by uncertainties, and entailing high stakes (both losses and benefits). For example, in the debate about the allowed level of pesticides in drinking water the protest of the water companies in the United Kingdom vanished once it became clear that they could charge the public for the risk mitigation measures (Hood *et al*, 2001).

In the rest of this chapter we will apply the constructivist approach to risk and risk governance:

- The situations to consider are those that the stakeholders consider to be relevant. In acquiring an understanding of these situations all relevant viewpoints and knowledge must be included.
- Governing risks implies a decision-oriented process that acknowledges the opinions and interests of all stakeholders, if it cannot actively involve all stakeholders.

### 5.2.2 Dimensions and size of the risk space

In an attempt to create an overview of the failure risks in the electricity infrastructure Wijnia and Herder (2005) distinguished eleven dimensions to characterise the risk space. The dimensions relate to different aspects of the failure risk. For each dimension, variables are given to denote the upper and lower limits of the (mono-dimensional) risk space. Table 5.1 presents an example.

As we can see, in some dimensions the upper and lower limits differ by more than a factor of  $10^6$  (one million). This makes it very difficult for decision makers to keep the portfolio of risk measures consistent, or at least coherent. For example, in valuing different risks, experience tells that

people will not allow for a spread in their judgements larger than a factor of 1000.

Table 5.1. Dimensions of the risk space (Source: Wijnia and Herder 2005)

Dimension	Lower limit (example)	Upper limit (example)
Consequence of failure	Voltage sag	European blackout
Failure duration	10 ms (voltage sag)	Weeks (France 1999)
Probability (1/yr)	<10 <sup>-6</sup> (Nuclear meltdown)	>10000 (medium voltage interruptions)
Mitigation effort	100 € per annum (switchgear maintenance)	>1 G€ (new high capacity power plant)
Complexity	Single criterion threshold (load level exceeded)	Multi criteria weighted sum (maintenance concept)
Scope	Technical (device settings)	Ethical (Can we continue operating overhead lines if this might increase the probability of leukaemia)
Time horizon	Tomorrow (new customer application)	25 years (network design for distributed generation)
Actors	Single actor single objective	Multi actor multi objective
Risk perception	Perception in line with objective risk analysis	Perception deviating from objective risk analysis
Uncertainty	Almost certain	Uncertainty about consequences and likelihood
Ambiguity	Shared objectives	Conflicting objectives

### 5.2.3 Taxonomies of risk

It will be evident that to manage the total risk space some sort of classification scheme is needed to group the risks into a manageable number, as no risk manager is able to rank thousands of risks. For this categorisation a few options exist.

For example, one could use a risk taxonomy that is similar to the asset hierarchy as used in Failure Mode and Effects Analysis (IEC 1985). In such taxonomy, risks can be viewed at different levels: system, sub system, equipment, component and so on. This approach has the clear benefit that it is conceptually easy. However, even in a modest High Voltage network (1 million customers, 70 nodes and 130 circuits) the number of possible

multiple failures explodes: it grows from 200 single failures, to 39800 double failures and 7880400 triple figures. As in the studies of blackouts these higher order failures seem to be the drivers (Dobson *et al.* 2002). From a manageability viewpoint, however, this approach does not seem to be workable.

Another option is to structure the risks according to the organisations designed to manage them. For example, power companies often have different departments for *new connections, maintenance, replacements, fault restoration, control and operation, new infrastructure and information sharing*. Each of these departments has its own set of drivers, to which it reacts by deploying more or less activity. In Table 5.2 (below) such a high level list is presented (Wijnia and Herder, 2004).

Table 5.2. Risk drivers (Source: Wijnia and Herder, 2004)

Outcome (budget)	Driver	Outcome (budget)	Driver
New connections	Number of new houses Number of new small businesses Number of large businesses	Fault restoration	Failure rate Failure type Number of assets Accessibility fault location
New infrastructure	Number of new areas Occupation rate Use of new areas	Protective measures	Third party damages Terrorism Vulnerability assets Failure rate
Reinforcements	Load growth Failure rate Critical level (neg) Failure acceptance	Control centre	Number of assets Information availability (neg) Activity level
Replacements	Leakage Failure rate Risk level asset location Number of assets	Information availability	Public requests Third party activities near assets
Maintenance	Leakage Failure rate Risk level asset location Legal demands Number of assets		

However, as one can easily see in this table, the drivers are not exclusive for the different activities. This implies that if single actors are

left to themselves to manage the risk drivers, some risks would be mitigated twice, possibly in ways not mutually consistent. Real difficulties arise when a measure to reduce one risk simultaneously increases another one, and when a risk exceeds the confines of a single company. The problem of risk management in an inter-organisational context is aggravated when companies hesitate to share information related to their assets, as is shown by the reaction to some CIP initiatives. However, in the Netherlands, for instance, almost half of the service interruptions are caused by third parties damaging cables in excavation works. Such damages could be prevented if information on asset location was shared and made easily accessible.

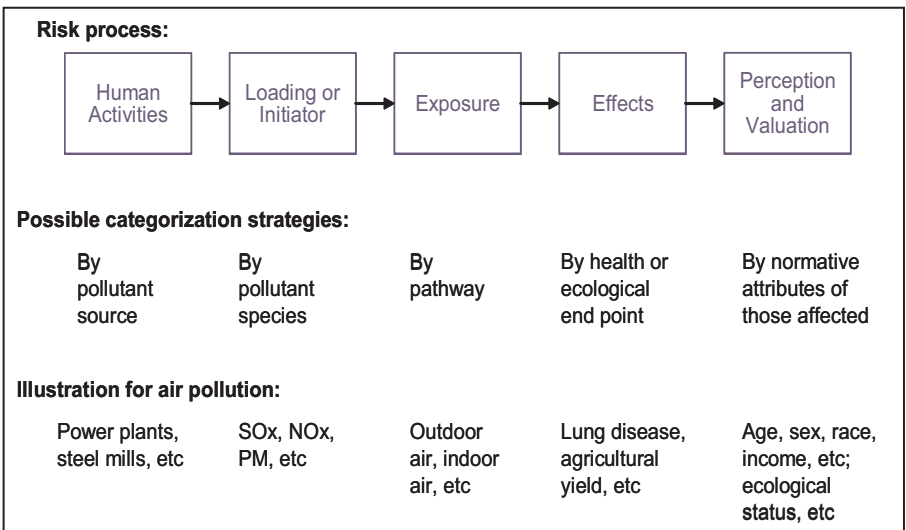


Figure 5.3. Risk process (Source: Morgan *et al.* 2000)

The problems in categorising risks are widely acknowledged. Following the constructivist approach, Morgan *et al.* (2000) argue that risk managers should try a few categorisations until they find one that best suits the decision problem at hand. The framework that is offered to facilitate these different categorisations is the risk process. In this view a risk is a chain that connects the initiating activity to the effect caused in society (Morgan *et al.* 2000). The risk process Morgan uses to structure air pollution risks (see Figure 5.3) can be modified to fit the electricity infrastructure (Wijnia and Herder 2004). Figure 5.4 shows the categorisation strategies.



Although a risk process does facilitate multiple categorisations of risks, it does not allow for interactions between risks or risk coincidences. To overcome this problem Wijnia and Herder have further developed the risk process into a risk network (2004), shown in Figure 5.5. In such a risk network feedback loops occur between the different steps. For example, a lightning strike on a transformer causes it to explode. The flying debris hits the bus bar and switchgear, causing them to fail. Although the system is designed to cope with the failure of one transformer, multiple failures normally result in the blackout of a region. The risk network including feedback loops is shown in Figure 5.5.

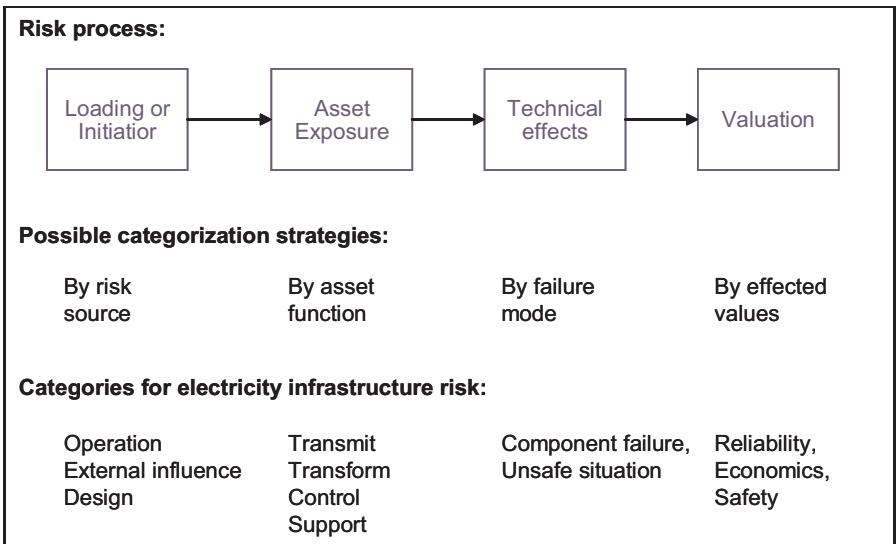


Figure 5.4. Categorisation strategies for the risk process (Source: Wijnia and Herder, 2004)

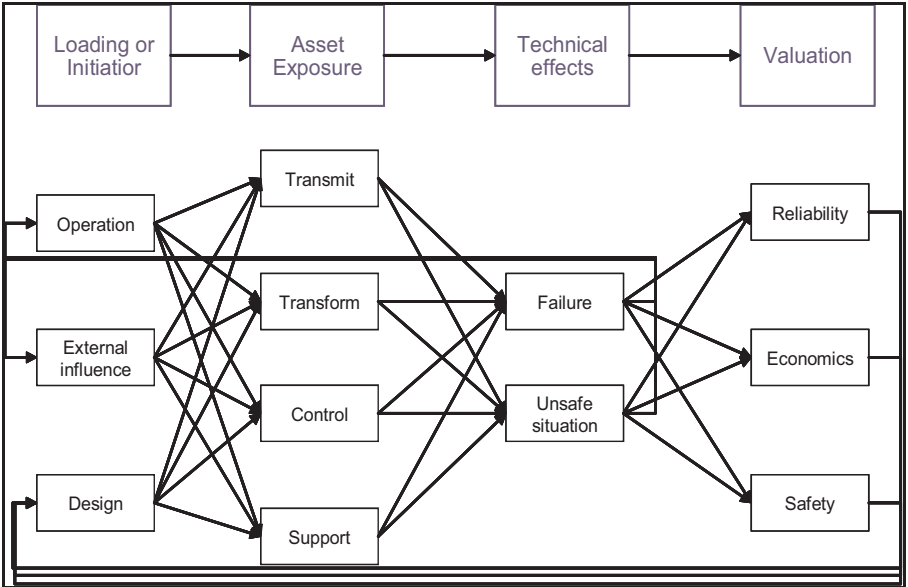


Figure 5.5. Risk network (Source: Wijnia and Herder, 2004)

If we consider the risk space depicted in Figure 5.5 as a network of steps in risk processes, any risk can be construed as a path through the network.

### 5.2.4 The risk network of the ECEI

In order to gain a full picture of the risk network of the ECEI, it is important to review and complement the framework. First of all, many new activities have become a part of the infrastructure system. Whereas the system used to be viewed and operated as a correlated set of electric power generation, transmission and distribution activities, this technocratic view is no longer applicable since the introduction of competition in (parts of) the system and the introduction of new activities and functions such as trading and power exchanges, respectively. Both the introduction of new activities in the system and the unbundling of activities that used to be integrated necessitate a review of the risk governance framework. This implies that the Asset Exposure step has to be expanded to include the other assets involved. Secondly, at the overall system level, a single asset failure could hardly create a European-wide

problem. Therefore it is more useful to look at system exposure. Finally, as it is the central theme of this book to address the risks in the ECEI, it is necessary to expand the causes, technical effects and valuation into a detail level that is easier to visualise.

This would result in the following categories of causes:

- Deliberate system damage (e.g. terrorism, environmental extremism, theft, hacking, malware including computer viruses)
- Natural hazards (e.g. storm, ice storm, earthquake, volcano, inundation)
- Systemic failures (e.g. oscillations, common mode failures, fault propagation, cascades, escalation)
- System aging (wear and tear)
- Human resource factors (e.g. workforce decrease due to ageing, knowledge losses)
- Strategic behaviour with risk acceptance (e.g. closing plants to drive price upwards)
- System design flaws<sup>1</sup> (e.g. rational behaviour leading to unacceptable risks like underinvestment in generation capacity due to uncertainty)

For functional asset groups the categorisation is:

- Fuel supply system
  - Pathway (road, rail, water, pipeline)
  - Storage facilities
  - Handling (shipper, truckers)
  - Logistics
- Power generation system
  - Energy conversion system (boiler, fission reactor, gas turbine, generator, etc.)
  - Technical control system (control room, software, instruments, operator)
  - Economic control system (electricity price, fuel price, demand, expected values, long term certainty)
  - Maintenance system (maintenance crews, data, equipment)

<sup>1</sup> The difference between systemic failures and system design flaws might be confusing. What we mean by systemic failure is a system, working well for most of the time, failing in unanticipated ways in rare circumstances. A system design flaw will create a failure even in normal or anticipated conditions.

- Electricity transmission and distribution system
  - Pathways (cable, line, transformers)
  - Technical control system (control room, software, instruments, SCADA, operator)
  - Economic control system (demand, generation, market differences, long term certainty)
  - Maintenance system (maintenance crews, data, equipment)
- Electricity market system
  - Data (market prices, plant availability, load levels)
  - Actors (operators, traders, risk managers)
  - Market operation system (procedures, rules)
- Enterprise business systems
  - Administrative systems (accounting, asset management)
  - Commercial systems (metering, billing, energy information services)

In this approach, ICS (i.e. the information and communication systems) based risks are integrated within the mentioned asset groups.

For technical effects the categorisation is:

- Asset damage (e.g. collapsed transmission towers, broken wires, turbine explosion, generator fire)
- Local energy imbalance (e.g. resulting in heavy imports, low voltages)
- Asset overload (mechanical stresses, thermal overload)
- Power oscillations
- Production capacity shortage
- Cybersecurity damage (data or ICS availability, integrity or confidentiality impairment)

The Valuation step consists of:

- Economic damage (e.g. loss of production due to outages, asset replacement value, loss of revenue, fraud)
- Power outages
- Blackouts
- Environmental damage (radiation, CO<sub>2</sub> emission, fuel leaks)
- Public safety (e.g. electrocution, injuries from explosion)
- Public confidence (trust in the correct functioning of the ECEI)

Although power outages and blackouts both are an aspect of reliability, the valuation is quite different (de Bruine, 2004).

Figure 5.6 shows the high level risk process of the ECEI including the high level categories proposed.

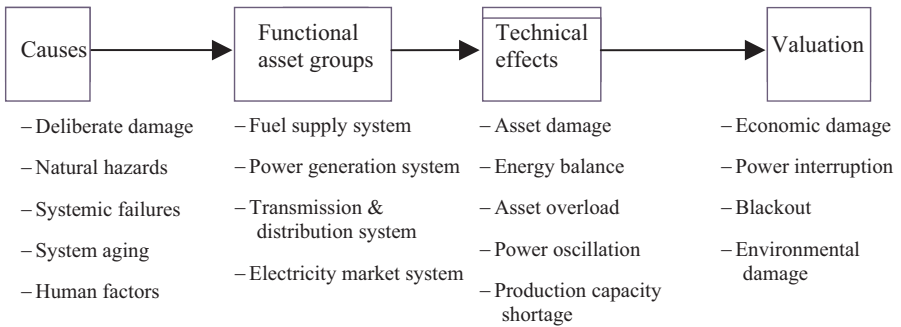


Figure 5.6. ECEI high level risk process

From the ECEI risk process depicted in Figure 5.6 the ECEI risk network can now be constructed, as shown in Figure 5.7. The risk assessment can then be started with the search for relevant pathways through the network, i.e. the identification of relevant risks, on the basis of the relative strength of the coupling relations between the elements in the risk network. For example, one can imagine that strategic behaviour of actors in the ECEI aiming at influencing the market is most likely to appear in the power production system, resulting in the shutdown of plants to drive the price upwards. This might result in local energy imbalance, resulting in large power flows in the interconnectors. This could also cause power oscillations in the European system, which consequently could also result in interconnector overload. Opening a very heavily loaded interconnector will result in an immediate power shortage in the importing region, possibly ending in a total blackout.

The risk network pictured in Figure 5.7 consists of a total number of 1260 paths (7 times 5 times 6 times 6). It would go beyond the scope of this book to examine all paths. Instead, we will start with the causes and determine the strongest paths.

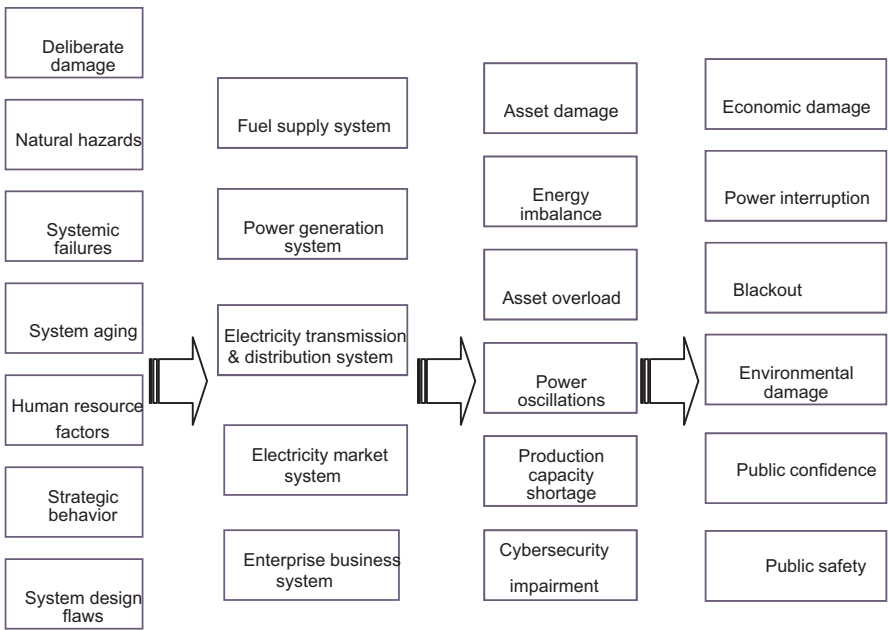


Figure 5.7. ECEI risk network

### 5.2.5 Important risk paths in the network

#### Deliberate damage:

Deliberate damage can affect all components of the power infrastructure, whether in the socio-economic or in the physico-technical domain, and can be accomplished by physical or logical (cyber) means. This category covers a vast range of potential malicious activities, from organised crime to terrorism to sabotage by disgruntled employees. In comparison with other causes, it is undoubtedly more difficult to judge the likelihood and potential target of such malicious activities.

Deliberate damage will mostly impair assets, thus resulting in direct economic damage. A single attack will generally not induce system breakdown: this requires a set of simultaneous attacks (in a limited period of time) on multiple essential components. In case of attacks on the fuel

supply system or the power generation system (e.g. nuclear plants) serious environmental damage could result.

Attacks on the market or business information systems could result in information losses. Although the unavailability of (some part of the) ICS can cause major problems for single companies, it seems that only the attack of the market system might produce a major disturbance at the overall system level. In any case, even though attacks might not break down the infrastructure as a whole, their repetition may instil fear within the society and hence have serious political effects.

### **Natural hazards:**

Natural hazards strike locally. This means that their result is mostly asset damage and thus economic damage. However, extreme weather conditions (e.g. winter storms, extremely hot summers) can hit large parts of the infrastructure, possibly resulting in severe power outages such as the one in France in November 1999 (Le Du *et al.*, 2000)

### **Systemic failures:**

Systemic failures act upon the system as a whole. As they only appear in tightly coupled systems (Perrow 1984), the fuel supply system appears to be the least vulnerable to this risk. Systemic failure can be a serious issue when considering the rapid and ubiquitous introduction of new technologies (for instance, new information and communication systems). A typical scenario will see the same technical solution (e.g. a communication protocol) employed all over the infrastructure. This situation will be critical when correlated to potential security breaches. A single failure mode can then escalate and cause serious consequences (e.g. a large scale blackout).

### **System ageing:**

System ageing affects all assets, including ICS. It can result in loss of asset performance, especially in the power generation system, leading to a production capacity shortage. In Europe, the ageing of many power generation plants (including most of the nuclear power installations) and of a great many sets of transmission and distribution networks is of particular relevance. In other systems, ageing is not likely to have a major direct influence, unless a large number of assets fail simultaneously. The possibility that this situation occurs as a result of ageing, however, is considered remote at the present state of the ECEI.

### **Human resource factors:**

The transmission and generation systems are operated by an ageing workforce. In many power utility companies, more than 50% of the technical staff is due for retirement within the next 10 years. This could result in a net loss of (tacit) knowledge and skills which, in turn, could impinge on the capacity to restore faults, and therewith decrease the reliability of the (sub)system and increase the associated economic damage.

### **Strategic behaviour**

Strategic actor behaviour as a cause of risks is most likely to occur in the power production system (de Vries, 2004). Whereas strategic behaviour may be perfectly rational and acceptable from a business perspective, in this context we are specifically referring to strategic behaviour that is in conflict with the public interest of availability and reliability of service, such as underinvestment in generation capacity or shutdown of generation plants for maintenance in situations of imminent shortage. Such behaviour may result in a local energy imbalance and in production capacity shortages, which in turn may create situations conducive to an increased likelihood of rolling blackouts (de Bruine, 2004).

### **System design flaws**

System design flaws can occur in all parts of the system, both in the socio-economic and in the physico-technical domains. In view of the long experience with the design and operation of the technical system, system design flaws in the electro-mechanical parts of the fuel supply system, the power generation system and the transmission and distribution systems are considered highly unlikely.

Less unlikely, however, is a system design flaw in the market system or in the ICS components. Computer-based systems are notoriously prone to design flaws – and this is aggravated by the pervasive use of identical technical solutions throughout the infrastructure system (brought about by e.g. standardized information exchange protocols). With respect to the design and management of network bound markets, there is only limited experience available. In fact, most of the electricity infrastructure related markets in Europe are still in a rather turbulent transition phase from monopolies to competitive markets, with large differences in market structure between regions and Member States. As only time will tell if the



newly installed systems of market control and network regulation are adequate and robust, system design flaws in the socio-economic subsystem cannot yet be ruled out as a potential source of major risks to the security of electric power supply in Europe.

## **5.3 Risk Governance of ECEI**

### **5.3.1 From risk assessment and risk management to risk governance**

Once a risk is recognised, the stakeholders concerned will deal with the situation – sometimes because it directly relates to their activities, sometimes obliged by some legal or normative measure. If a risk has the potential to critically affect society at large, governments will typically come into action for the benefit (protection) of the whole population.

The two main activities for coping with risks are risk assessment and risk management. As explained in (Renn, 2005), “the major task of risk assessment is to identify and explore, preferably in quantitative terms, the types, intensities and likelihood of... the consequences related to a risk”, and “the task of risk management [is] to prevent, reduce or alter these consequences by choosing appropriate actions”.

When risk situations are complex and the stakeholders numerous, as in the case of critical infrastructures, it is not straightforward which means and ways could be effective for reaching a common appreciation of the risks and for making decisions on appropriate and workable solutions.

In these circumstances, society has to develop suitable approaches that at the same time allow for a proper understanding of the risks, as much as possible based on scientific and technical knowledge, and for decision making on lines of action that solve the problem while respecting the concerns of all stakeholders. This has been the history of Western societies in the last century for dealing with problems such as toxic and carcinogenic substances, nuclear power plants, environmental pollution, etc. This style has come to be known as risk governance.

Governance refers to “structures and processes for collective decision making involving governmental and non-governmental actors” [Nye and Donahue, 2000]. Therefore, governing risks implies that all actors accept a collective approach to evaluating the risks and making decisions about the options for managing them. This requires a deliberate method that incorporates the different viewpoints.

In the case of the European Critical Electricity Infrastructure, the situation is further complicated by the international dimension of the problem, the correlation of different types of risks (systems adequacy, market design, cybersecurity), and the evolving nature of the regulatory and institutional environment.

### **5.3.2 What is risk governance?**

Risk management refers to the evaluation and selection of options by a responsible subject (the “risk manager”), who takes into consideration all relevant aspects of a certain risk situation, including the perception of risk by interested parties and the assessment of the risks. Therefore the main assumption of risk management is that it is evident who is to be held responsible for dealing with a given risk.

Risk governance is a superordinate of risk management – i.e. it pertains to a superior logical level. Risk governance is applicable to systems-of-systems, such as infrastructures, which are characterised by the absence of a central actor who can determine the problem and impose risk solutions.

Due to the distribution of responsibilities among different actors in an infrastructure system-of-systems like the ECEI, an explicitly designed risk governance structure is needed to bridge the responsibility gaps between the different actors and the different (hierarchical) levels within the overall system. Hence, a major difference between risk governance and risk management is the number of actors involved in the identification, decision upon and implementation of the risk options. Risk governance also requires the consideration of contextual factors such as institutional arrangements (e.g. the regulatory and legislative framework that determines the relationships, roles and responsibilities of the actors and co-ordination mechanisms such as markets, incentives or self-imposed norms) and political culture. Risk governance requires a more multifaceted risk process, where the various actors debate and decide on the coordination of their respective risk management practices.

Therefore, the term risk management is used to designate the activities undertaken by single parties with the goal of treating a specific set of risks for which they hold explicit and exclusive responsibility. The term risk governance, on the other hand, refers to the way a multi-actor system should be organized in order to manage the risks that confront the multi-actor and multi-level system-of-systems that they collectively form. This distinction is highly relevant to the electricity supply industry because its security performance is a function of the system as a whole, whereas an

effect of liberalisation is that each actor controls only a part. Consequently, individual actors can only manage certain local risks; other risks with broader system implications will need to be dealt with at the overall system level.

Due to the involvement of a collection of actors, risk governance requires normative principles for defining and guiding the process by which conflicts are addressed, decisions are taken and stakeholders are accorded participation. The typical steps of a risk management process (i.e. identification of risk management options, their assessment with respect to certain criteria, their evaluation and selection, their implementation and lastly the monitoring of their performance) have thus to be reviewed and adapted to match the requirements of the risk governance process.

Figure 5.8 shows the relationship between risk management and risk governance. Building upon the infrastructure model presented in Chapter 4, 5.8 also consists of layers. Again, at the bottom is the physical system – i.e. in our case the different systems that compose the European electric power infrastructure. The next level contains the actors who have immediate control over the physical system – i.e. the actors participating in the different operations of the electric power infrastructure: generation, transmission and distribution, market. The top level in 5.8 is the system-of-systems level: the super ordinate layer where decisions are or should be made that affect the infrastructure system as a whole, and where, for instance, we can logically anchor the combination of incentives and constraints (such as regulations) that guide the actors.<sup>2</sup>

In this conceptual framework, risk management is only involved with the bottom two levels depicted in Figure 5.8. It can be considered a performance loop, in which a company considers the performance of its assets and adjusts its operation, maintenance and investment activities accordingly, in the context of a superior risk governance loop.

Risk governance can be regarded as a similar performance loop at the system-of-systems level. Here, it is the collective set of all actors who decide which objectives to follow, which overall policies to apply, and who judge whether the electricity sector as a whole has performed according to its standards. This loop therefore encompasses all risk-related aspects of the performance of the electricity supply system. Whereas the risk governance performance loop is wider than the risk management loop,

<sup>2</sup> The top level is not drawn explicitly in Chapter 3. There, the incentives and constraints are considered part of the relations between the actors. For the purpose of this chapter, however, it is practical to make the institutional environment more visible.

the means for intervention are in effect more limited, and the procedures for reaching to a decision are far more complicated.

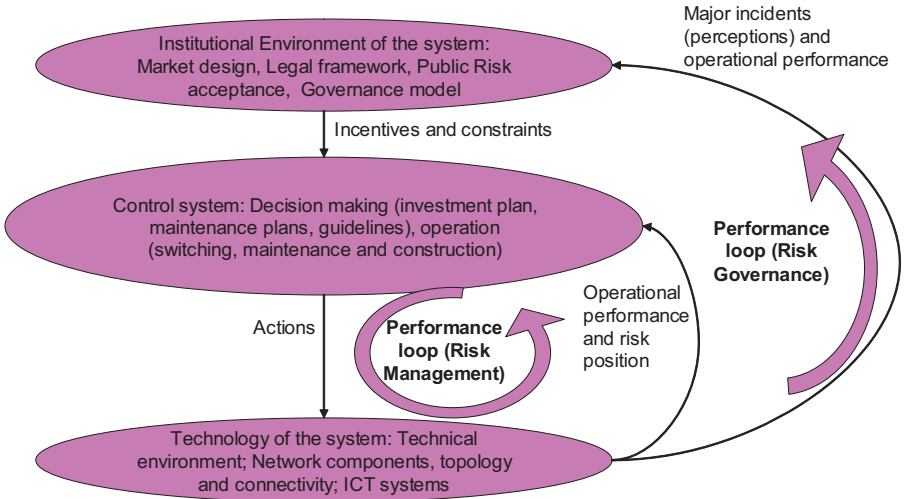


Figure 5.8. The risk management and the risk governance loops (based on Wijnia and Herder, 2005)

From the governments’ viewpoint, direct intervention in the electricity sector is limited to changing the incentives and constraints that act upon the electricity supply industry, and not to the definition of technical measures or standards. Control in this case would be relatively easy with respect to the monopoly functions such as network management, as this needs to be regulated anyway. But the opportunities for intervention in a competitive market are limited. Government intervention is obviously easier in those cases where the industry has not (yet) been privatised, but there is a high probability that public ownership patterns will gradually be phased out.

From the standpoint of the industrial actors, the main difficulty stems from their multiplicity and diversity. Reaching agreements about which risks need to be addressed, by means of which measures, and about who is

to evaluate their effectiveness, might be hampered by conflicts of (business) interests resulting in tedious discussions in which consensus cannot be reached. The solution to this problem can be given by establishing an institution responsible for putting into service and steering the governance process. This will be discussed in following sections.

### **5.3.3 The context for the risk governance of the ECEI**

The risk governance of the ECEI will take place in a multidimensional landscape that is determined by several factors: the European Union policies that have reformed the sector and transformed the playing field in the last years (see chapter 1 for a detailed explanation); the regulatory setting that comprises national legislation and regulation and international norms and treaties; the electricity market itself which is still transient and therewith poses a source from which new risks may emerge.

#### **Regulatory and institutional context**

The European electric power infrastructure is demarcated from the regulatory and institutional perspective by the following elements (for a detailed account see Appendix A.3):

- European legislation: the different Directives, Regulation and Decisions that establish the European internal electrical market (see Chapter 1);
- European institutions: Electricity Regulatory Forum of Florence and European Regulators Group for Electricity and Gas (ERGEG);
- Other regional institutions in Europe: Euro-Mediterranean Partnership, Euro-Mediterranean Energy Forum, Council of European Energy Regulators (CEER);
- Technical associations: European Transmission System Operators (ETSO), Union for the Co-ordination of Transmission of Electricity (UCTE), NORDEL, TSOI, UKTSOA;
- National law: with different styles/frameworks from country to country;
- National official actors: competition authorities, network regulators and other authorities directly and indirectly dealing with security of energy supply, TSOs (and their Grid Codes), electricity and energy markets authorities and other specific actors;
- Other international institutions: World Forum on Energy Regulation, World Energy Council (WEC), Energy Regulators

Regional Association (ERRA), Committee on Sustainable Energy of the UN's Economic Commission for Europe (ECE), OECD 's International Energy Agency (IEA).

### **Market context**

Governance of critical infrastructures, and in particular risk governance, has to cope with the reality of electricity industries which have been (partially) opened-up to competition, have partially undergone privatisation, are subject to decisions of a variety of national and international regulators, are increasingly exposed to the volatility inherent in electricity trading and which are increasingly reliant on their being internationally connected.

The main elements of the reform of the electric power system therefore set the “guide rails” within which risk governance has to operate. These ingredients consist of the following (See Ocaña, 2004), p. 2):

### **Liberalisation and unbundling**

Liberalisation refers to the introduction of competition into the electricity supply system. Depending on which parts or functions of the electric power system are liberalised (i.e. only generation, only distribution, or both), there are different degrees and models of market opening. Liberalisation often goes hand in hand with privatisation – some European countries such as the UK have even privatised their high-voltage grid. Unbundling means breaking up vertically integrated utilities in such a way that the core business activities are separated – either in terms of accounting, information systems, employees, operational entities or ownership. Again different degrees of unbundling can be imagined based on what is actually separated: generation from transmission, generation from distribution; distribution from end-user supply. Additionally, the transmission function can be broken up into grid ownership (ownership of physical assets) and system operation and planning (independent system operator).

### **Third Party Access (TPA)**

Third Party Access can be viewed as a special case of liberalisation and relates to those parts of the infrastructure which constitute a de facto monopoly such as transmission capacities. TPA endows potential users with a right to access the transmission and distribution networks.

Depending on whether access conditions and prices are regulated or not, two different TPA models exist: regulated TPA and negotiated TPA.

### Potential set-up of regulatory institutions

Within a perfectly competitive electricity market a regulator would be perfectly superfluous. However, imperfections exist, which are potentially increased by the difficulties and uncertainties which arise from the period of transition following market opening. As it seems that serious imperfections persist long after market opening, resulting in a lack of competition at the national market level as well as in a lack of integration of the European electricity market, the effectiveness of changing existing regulation seems limited, particularly as each regulator has only national responsibilities and powers. Without the introduction of some form of regulation that spans the entire interconnected system – almost impossible, given the number of countries involved – changing and aligning the set-up of (national) regulators is a key ingredient of effective risk governance (see OECD/IEA, 2001).

### Structural changes to reduce the market power of individual companies

While many electricity markets were highly concentrated from the outset of the liberalisation process, the recent wave of mergers and acquisitions generally has only aggravated the degree of market concentration: in France, Greece, Ireland, Spain, Cyprus and Malta, for instance, the largest three generation companies hold a market share of more than 75% (See Commission of the European Community (2004), p. 4). The implications are clear: Where there is market power there is a risk for it to be exercised – which is normally in the form of high electricity prices. Antitrust law will have to provide the means to effectively fend off abuse of market power.

Within Europe there are different market models and regulatory approaches. How the reform of the electricity supply industry has been and is still conducted and how the market is subsequently organised have a direct impact on the owners and operators of the industry's core assets. For these assets to receive the investment they need to ensure ongoing operability requires that owners and operators can afford such investment. The adequacy and timeliness of investment, in turn, is the most important factor within liberalised markets to effectively and efficiently ensuring security of supply (See OECD/IEA, 2002, p. 9.). When regulators and

competition law combine to prevent the necessary levels of investment through price controls, supply security is endangered.

### **Other contextual factors affecting the risk governance of ECEI**

Other external factors shape the field for the risk governance process:

- One factor affecting risk governance is represented by the rapidly changing energy and environmental regulatory context. Other related sectors such as the natural gas sector are also being liberalized; the tradable CO<sub>2</sub> emissions scheme presents a new challenge, not least because the future emissions cap is uncertain. The political uncertainty about the phasing-out of nuclear power, and the difficulties due to environmental opposition to the placing of new power stations and transmission lines in certain countries, further add to the uncertainty for investments in the electricity supply industry.
- A second factor is the increasing reliance upon other infrastructure systems such as the natural gas and the ICT infrastructures. While these are becoming more complex themselves, the increasing interdependence leads to the development of an even higher level ‘system of systems’ (higher level than the ECEI itself), a system of multiple interlinked and interdependent infrastructures. Thus the complexity is multiplied and the performance under stress becomes much more difficult to predict and analyse. Risk governance decisions become more intertwined, and have to take into account many more aspects beyond the technical considerations of electricity generation and transmission.
- A third factor is society’s dependence upon the electric power infrastructure as a vital service – this is at the basis of its consideration as a “Critical Infrastructure”. As the reliable provision of electricity supply services is increasingly taken for granted and necessary for an ever-increasing number of economic and social activities, the social costs of service disruptions rise proportionally. Having become accustomed to a reliable electricity supply, modern society cannot function without it anymore. Therefore a thorough analysis of the changing risks and possible strategies for society to deal with them is in place, considering that the same economic welfare, social wellness and political stability of European countries might be at stake. Last but not least, the new threat of terrorism poses an uncertain but potentially large threat



that requires the intervention of national governments and the European Union.

### 5.3.4 ECEI: A proposal for self-regulation

The core of the findings of this book can be summarised in three items:

- The ECEI is subject to risks that are relevant to stakeholders in various jurisdictional areas, and these risks are of multiple nature.
- The potential implications of the risk situation are different for the various types of actors: mainly economic and commercial for the industrial ones, macro-economic and national security risks for governments and environmental and service continuity risks for society at large.
- EU and national authorities can set the framework for the electric power operations and market; sector regulators can define the objectives with respect to power security and adequacy; but the final responsibility for determining which measures to adopt and investing in their implementation will mainly be in the hands of the power companies (which are mainly privately owned).

The question to pose at this stage is: Which is the most appropriate approach for dealing with the ECEI risks? During the last years there has been a long debate on the best means and ways for governing the European Union (see for instance <http://europa.eu.int/comm/governance>). In this context, the EU regulatory functions and their effectiveness were reviewed (EC, 2001). Based on this, and on parallel developments in the world (see for instance the revision of USA's energy policy during 2005), we propose that the most convenient way would be a **self-regulation** approach.

When considering the alternative instruments that can be employed for governing the ECEI risks, one can make the following observations:

- New regulation does not appear necessary, as the current risks require an operative response. The sector is already regulated, and should there be a need of additional legislation or regulation, consultation with industry will be enriching as a result of their experience in governing risks at a local level.
- A sectoral voluntary agreement seems preferable. The modalities for its implementation should be in accordance with current legislation, and specifically compatible with European competition law. However, a simple voluntary agreement might be insufficient to meet the risk governance requirements. If the protection of the

electric power infrastructure is to be effective, it is clear that the actions agreed upon will have to be compulsory to all parties. Therefore, the voluntary accord should result in mandatory rules. The participants to the voluntary agreement – ideally all the actors in the ECEI – by taking part in it, commit themselves to respecting the joint decisions. In this way, when deciding upon an instrument, it should be ascertained that all parties are bound by the decision and will implement the needed measures.

- Our choice would be a **sectoral voluntary agreement involving self-regulation**, which can provide to the practices, common rules, codes of conduct and other agreements reached in the governance process, a mandatory character. This should prevent the danger of “free-riders” ignoring the codes or finding loopholes for circumventing their obligations. Therefore a main task is to apply rigorous enforcement and compliance monitoring. Self-regulation does not involve legislative acts – it provides flexibility, without denying the possibility to recur to legislation when self-regulation proves insufficient or inefficient. This connection can ensure the most efficient mix of instruments, and a fertile co-regulation environment where the public and private sectors collaborate for the best of their interests.
- Self-regulation can be a powerful tool in the hands of the electric power sector. The challenge is to apply the best business practices for managing risks, and in parallel to protect society. In this collaborative effort, industry will have to assume a society-wide responsibility for the risks to the infrastructure and involve all relevant stakeholders. The final success of a self-regulatory process will depend on the ability to define and implement the proper governance means.
- Considering the different governmental styles developed by policy analysts (O’Riordan, 1987), we can identify the proposed approach as a “corporatist” one. This is characterised by the search of consensus by structured procedures, which are planned and controlled. Experts and stakeholders have well-defined roles in the risk decision-making and communication processes. The orientation is towards sustaining trust to the decision-making body. Reliance is put on available expert judgement and participation, with communication focused on fair representation of major societal interests.

### 5.3.5 Implementation of ECEI risk governance

The necessary risk governance of ECEI will have to be implemented by either making use of existing arrangements, or by means of new dedicated ones. In the following we will discuss both possibilities.

With respect to the existing organisation of the power sector in Europe we conclude that there is no institution able to fulfil the risk governance requirements, unless profound modifications to their character and purpose are undertaken. For instance the Florence Forum could execute that task, but after a transformation that should at least include a change of its informal nature to a decision-oriented one, new risk-related objectives, and an industry-led disposition.

As an alternative we have hypothesised the constitution of a new entity, the so-called **European Council for the Security of Electric Power** (ECSEP), with the specific purpose of implementing the previously described self-regulatory risk governance process. To the effort that will be needed for introducing a new actor in the already crowded ECEI institutional landscape, this option presents the advantage of offering a dedicated solution to a particular problem. This approach is similar to the one taken in North America with the North American Electric Reliability Council (NERC), formed in 1968 for assuring the reliability, adequacy and security of their electric power systems.

#### **Alternative A: Modification of existing institutions**

The regulation of the European electric power sector in the framework of EU directives has been centred on two issues: the formation of electricity markets (including the tariffs of electricity supply and cross-border topics), and the respect of public service obligations (including the security and quality of supply).

The purpose of this regulation effort has been to ensure the competitiveness and efficient performance of the wholesale and retail markets, and the satisfaction of basic rules concerning the reliability and adequacy of the power infrastructure. The concurrent fulfilment of both objectives can not always be solved in a straightforward way: the effectiveness and productivity of markets (that push for cost reduction), can contradict the needed investments for the long-term security of supply, and in particular for the risks described in this book.

The actuation of electric power security of supply is partially in the hands of the national regulators and partially in those of the TSOs, and in

their associations: CEER for the regulators and UCTE/NORDEL for the TSOs.

For instance, the regulators can develop incentive schemes for stimulating the optimal use and expansion of the infrastructure (e.g. generation plants), or foster the development of quality and reliability standards. The CEER working group on security of supply has defined a set of objectives that includes, among other points, the identification of barriers to security and of means to cope with them, the proposal of security principles and guidelines (Mayer, 2003).

For short-term security issues, grid operators hold the responsibility, in the context delineated by the regulators. TSOs on the other hand set in their Grid Codes (with the caveat that in some countries it is produced by the national regulator) the frame for dealing with security from the operational viewpoint, and their associations set the procedures for coordination, harmonised approaches and the exchange of information (e.g. UCTE's Operation Handbook).

It is noteworthy that in these scenarios the business actors that operate the generation and distribution parts of the infrastructure and that interact in the power exchanges, are absent. Their expected role apparently is to comply with the norms or to respond to the incentives and constraints, following the market rules.

However, those business actors are the ones that make risk management decisions, adopt technical measures and determine for a great part the security of the infrastructure. As demonstrated in the case of the blackouts studied in Appendix 1, and the consequences of the evolution of the power market and technologies in Chapters 2, 3 and 4, there are systemic risks that need to be considered at the infrastructure level, i.e. observing ECEI as a critical infrastructure composed of interconnected systems. The addition of local risk management decisions might hardly produce an appropriate answer to systemic infrastructural risks. A risk governance approach is needed.

Which of the existing institutions then accommodate the participation of all stakeholders?

The organisations of regulators are obviously the actors which accommodate for participation of a large variety of stakeholders in the electricity sector. CEER, the Council of European Energy Regulators, is a non-profit association of the energy regulators of the EU and the European Economic Area (EEA) member states. ERGEG, the European Regulators Group for Electricity and Gas, set by the European Commission in November 2003 as an independent advisory group that should provide

assistance in the consolidation of the internal market, facilitating consultation, coordination and cooperation between the national regulators. It obviously acts in accordance with CEER. From the risk governance standpoint, it is worth noting some statements by the CEER working group on security of supply (Mayer, 2003):

- “The roles and responsibilities of all the stakeholders in relation to security of supply need to be clearly defined”
- “Security of supply is addressed most effectively in a broad integrated market. With appropriate harmonization a single country should not act unilaterally in the interest of security of supply that in turn jeopardises security of supply in other Member States”
- “Specific procedures for continuous monitoring and reporting of the security of supply situation must be defined and put in place. Measures should be coordinated across the Internal Electricity Market in order to minimize the risks and maximise the benefits”.

ETSO is the association of the four regional organisations that compose the ECEI synchronously interconnected areas: UCTE (the Union for the Co-ordination of Transmission of Electricity, association of the TSOs of the continental counter of Western and Central Europe), NORDEL (Nordic TSOs), UKTSOA (Association of UK TSOs) and TSOI (Association of Irish TSOs). Other industrial actors are not represented. ETSO pursues scientific aims on a non-profit basis, and has among its objectives the “study and development of common principles regarding the harmonisation and establishment of rules in order to enhance network operation and maintain transmission system security”, taking action only when the goals “cannot be sufficiently achieved by its members acting independently”. Therefore, ETSO can be a great contributor to ECEI governance, but its constituency is limited.

Eurelectric is the Union of the Electricity Industry, a professional association that represents the interests of its associates, based on national representation. Members are from Europe and four other continents. Its mission is “to contribute to the development and competitiveness of the electricity industry”. It represents the industry at large before authorities, specifically at the EU level. Eurelectric is a centre of expertise on electricity matters, with a broad view of the industry’s different areas. Its interests are in supporting the European market liberalisation, integration and sustainable development. Its activities related to policy initiatives (including security of supply and sustainability), power generation and the

market, and its roadmap (“Closing the circle of competitiveness”) towards the re-orientation of the European electricity policy, can serve as substantial input to the risk governance needs. However, its constituency is also limited, and it cannot be asserted that its nature matches the requirements for dealing with risks in a concrete way.

The only organisation that is open to all ECEI stakeholders is the European Electricity Regulatory Forum (also known as Florence Forum). The Florence Forum is focused on the improvement of the electricity market, proceeding by recurring meetings where specific subjects (such as cross-border trade, tariffs for cross-border exchanges, and management of interconnection capacity) are discussed and agreed positions are communicated to the European Commission.

From the risk governance perspective, the Florence Forum falls short of fulfilling its requirements. First of all, it is not a decision-oriented organisation, as it was set up as an informal roundtable for the discussion of points of common interest and for the exchange of experiences concerning the implementation of the EU Directives. Secondly, risks issues have only marginally been the subject of debate. On the positive side, it is possible to highlight the Forum experience in promoting and building upon the co-operation and co-ordination among the different actors.

If the Florence Forum (FF) were to be employed for deploying a risk governance strategy, it will have to receive a new charter, greatly altering its original design. This so called Florence Forum-bis will have to show several – if not all– the characteristics foreseen for the new institution, ECSEP, described in the following. For instance, it will have to be able to establish security standards, to assess their impact and to enforce their compliance.

### **Alternative B: Proposal for an European Council for the Security of Electric Power (ECSEP)**

#### **Mission and objectives**

As an alternative to the FF we propose to consider the creation of a new agency, the European Council for the Security of Electric Power (ECSEP). Its mission should be to guarantee the governance of the risks that might threaten the security, adequacy, stability and reliability of the European Critical Electricity Infrastructure (ECEI). ECSEP may be instituted by the European electric power sector by means of a voluntary agreement, in an effort to self-regulate the infrastructure with respect to all kinds of

potential risks: system capacity inadequacies, system failures, natural hazards, human errors or deliberate attacks that might jeopardize the fulfilment of the infrastructure service objectives.

ECSEP is envisaged to be a decision-oriented, voluntary association of ECEI regulators and market and industrial participants, including consumers and other end-users, convened with the purpose of selecting courses of action, monitoring their compliance and effectiveness, and interacting when needed with European and national authorities, standardisation bodies, and other infrastructures.

The management and assessment of the risks will require the participation of all related stakeholders in the decision making process, including organisations such as ESTO, Eurelectric, UCTE, NORDEL, and all relevant authorities, and representatives of the customers.

The risks to be treated are those with European-wide relevance, i.e. those that have the potential to cause a cross-border contingency, and that therefore surpass the power of national organizations. Nevertheless, since decisions made in ECSEP would reflect a common position by all interested parties, they would undoubtedly provide the guard rails for the measures to be taken throughout the ECEI, from the synchronization zones, to the national and regional systems, down to the single companies.

### Membership, operation and regulatory framework

The members of ECSEP constituency (the constituents) should include: electric power utilities (generation, distribution), transmission system operators, national regulators, electricity market actors, and representative end-users of the countries which together form the interconnected European grid.

ECSEP will count on the joint effort of its members, who will voluntarily commit to accept and enforce its resolutions. This commitment should stem from the willingness of the ECSEP members to cooperate towards the achievement of common goals, and the awareness that the overall security of ECEI depends upon the harmonized aggregation of their singular actions.

ECSP will have to closely interact with the other organisations that are at the core of the ECEI industrial environment and infrastructure operation: Eurelectric, ETSO, CEER/ERGEG, etc.

The aforementioned and other relevant organisations (vendors of equipment, research centres, national authorities) should be invited as observers and contributors to the ECSEP activities, when pertinent for the consecution of the established goals.

For assuring the achievement of the common goals, ECSEP would have to have the power to monitor and enforce compliance, but also to verify that the different organisations possess the appropriate capabilities. Compliance can be guaranteed by a set of different mechanisms: peer pressure, penalties, economic incentives, etc. The verification of capabilities can be linked to certification, auditing and other qualification procedures.

It is also expected that ECSEP members would reciprocally promote the implementation of the agreed measures. Necessitated by the increasing number and importance of international interconnections of the ECEI with Central and Eastern Europe, Middle East and North Africa, ECSEP and its members might even have to play a role in promoting the adoption of its recommendations and standards in those regions, e.g. by advising the EU and national authorities on agreements to be forged through multi-lateral or bilateral treaties. As long as such measures are lagging behind the needs of the ECEI, the ECSEP might need to advise on alternative courses of actions to secure the ECEI, such as on strategic reserves to be maintained.

ECSEP would need to be granted some regulatory powers by all countries concerned and the European Union. It is recommended that the management of ECSEP as an independent authority be guaranteed by a checks-and-control balance between an independent executive board (responsible for the planning and execution of ECSEP activities) and a stakeholders group (responsible for nominating the board members, setting the strategic objectives, and approving the financial statements). This structure is similar to the one put in place by several agencies of the European Community.

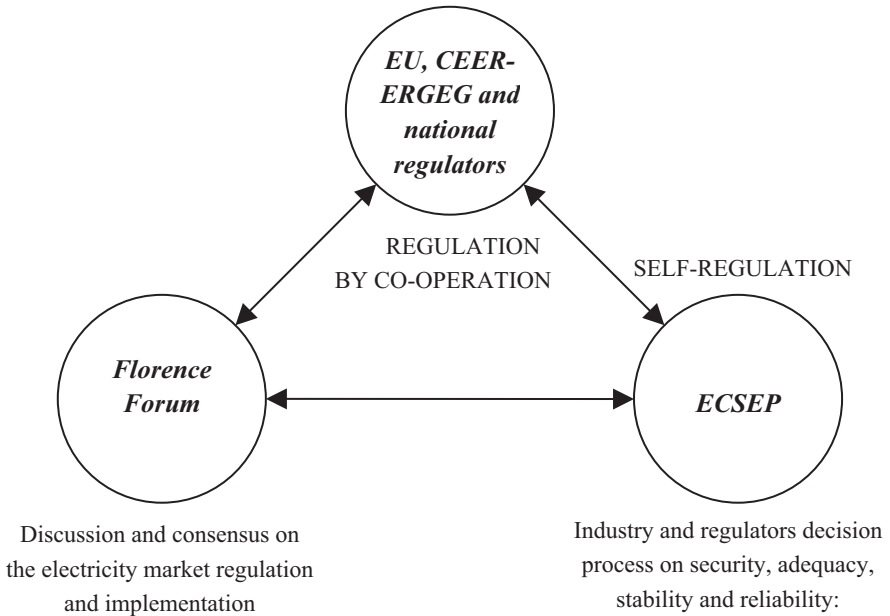
From the regulatory standpoint, ECSEP should be seen as a parallel and synergetic effort to the EU electricity directives (for a detailed view see Appendix A.3) and national legal provisions, and to the Florence Forum. European and national law provides the generic framework for the development of the European electricity infrastructure and markets. This is complemented by the actions of the national regulators, who ensure that the infrastructure operations and service provision to the customers are performed according to the standards dictated by the national legislative and regulatory frameworks.

The main distinctions that can be made between ECSEP and the Florence Forum (FF) in its current arrangement are (see Figure 5.10):

1. ECSEP is centred on risks issues, while FF looks at the general market arrangement and its regulation;



2. ECSEP is set up to lead, make decisions, enforce their application and foster initiatives that advance the power security of ECEI, while FF can just recommend, based on consensus, reforms to the European regulation or its implementation, in what is known as the Florence Regulatory Process; and
3. ECSEP focuses on self-regulation and the prescription of measures spanning from best practices to technical standards, and from accreditation to training, all related to power security; while FF constitutes a neutral and informal framework for exchange of opinions and experiences related to more general issues: public service obligations, transmission pricing and cost accounting, ancillary services, and other cross-border issues.



*Figure 5.10.* ECSEP position in the power regulation scenario

## **5.4 Conclusions**

The European Critical Electricity Infrastructure requires a systematic and thorough approach to risk governance. This chapter has described the problems, the elements that would have to be taken into consideration, and has proposed a risk governance process. Two alternatives were discussed for the implementation of the risk governance process: a modification of the Florence Forum, and the institution of a new body, the European Council for the Security of Electric Power (ECSEP).

The assurance of the appropriate reliability of the electric power system and its adequacy in the long term, and the management of the related risks exceeds the powers and responsibilities of the single actors, be it a power company or a nation. Some of these problems, due to their scope and significance, have to be treated at the EU level, with coordination of public and private actors. Other risk issues, however, have to continue to be dealt with according to the current arrangements: national regulators, international arrangements (i.e. UCTE, NORDEL).

Nevertheless, there is a remaining set of highly important questions: risks that can disrupt the European system and considerably affect the welfare and security of their societies. These are the ones which could benefit most from a risk governance approach to be initiated and led by an institution such as ECSEP or the modified Florence Forum.

Several questions remain unanswered and will be the object of further investigation:

- What should be the legal status of ECSEP or the new Florence Forum? It should guarantee the authority to coordinate the risk governance process, and to elaborate binding and enforceable measures. It should be noted that in this context Europe is more than the European Union.
- What roles and responsibilities should be given to the different members and is there a need for a voting mechanism which departs from the principle of unanimity? If so, how should that mechanism be constructed so that it is both fair and efficient? How should ECSEP/FF be financed? What will be the link between ECSEP or the Florence Forum and the design of the electricity markets? Several risks are closely related to market issues and various countermeasures are market instruments. One should consider that strictly speaking there is no “common” economic history with regard to the liberalisation of the European electric

power system within the European Union (which could result in a priority claim). The different national situations might present difficulties for the progression of the ECSEP/FF risk governance process. The European electricity market seems to be running at a highly uneven pace: the different national markets which compose the European market seem to be in quite different stages of liberalisation, but some risks situations (in fact most of those requiring risk governance) are European-wide by nature. Electric power risk governance and market liberalisation authorities will have to coordinate their actions in many circumstances. Which other models might be envisaged for staging an adequate risk governance process in the ECEI? Both the modified FF and the ECSEP models, as they both rely on self-regulation, allow for the electricity markets to unfold and respond accordingly if new risks are seen to emerge. In fact, the emergent behaviour of the ECEI system-of-systems itself is a major obstacle in defining and deciding on appropriate risk governance structures and processes.

- How should the ECEI risk governance process be linked with risk governance in other critical infrastructures? At the higher system-of-systems level where the ECEI is interconnected with other critical infrastructures, an overarching risk governance process will be needed that addresses the complexity of intersectoral interconnections and interdependencies and coordinates the governance of the risks emerging from these interactions. At this point in time, the option of European regulation to ensure cross-sectoral coherence and consistency of sectoral and infrastructure-specific risk governance processes should not yet be ruled out as a possibility or even as a necessity.

## Chapter 6

# Concluding Remarks and Recommendations

*Marcelo Masera, Adrian Gheorghe, Margot Weijnen*

### 6.1 Introduction

There is a manifest need to secure the European Critical Electricity Infrastructure. Our analysis of the ECEI system and its dynamic behaviour inevitably led to the conclusion that the reliability and quality of electricity service provision to the European citizen are not adequately secured if all actors are allowed to run their activities at subsystem levels in the “old ways” of the pre-liberalisation era. The established lack of supply security applies to the short term as well as to the long term security of electricity service provision. There are multiple reasons for this conclusion: the emerging European Critical Electricity Infrastructure (ECEI) - including the European electricity market - is a fundamentally different construct from the old situation of interconnected national grids. Even if the latter situation seems comparable with the current ECEI in terms of geographical scale and scope, the complexity of the ECEI is beyond comparison, as it reaches far beyond physical network complexity. With the liberalisation process, many new players have entered the playing field, new roles have been introduced, the rules of the game have changed and are still changing. The complexity of the multi-actor network is unprecedented, and its behaviour is highly unpredictable. On the one side, this unpredictability is a consequence of the multitude of actors involved, our lack of insight in their intentional relationships, their strategic behaviour and learning behaviour. On the other side, the evolution of the multi-actor network and the socio-economic subsystem in which it is embedded are subject to many uncertainties pertaining to market development and evolving regulation, technological innovation and institutional change. Given our lack of experience with liberalised electricity markets in Europe, it is evident that we are not able to identify all the risks that are generated by the dynamic interactions between the physical and socio-economic subsystems that constitute the ECEI.

Acquiring such a picture is a daunting task, which is further complicated by the fact that both the physical subsystem and the socio-

economic subsystem of the ECEI are complex aggregate systems in themselves: the physical system evolved from the subsequent interconnection of local, provincial, national and regional subsystems; the “European market” is a complex aggregate of national and regional markets, as a result of the European Union framework being implemented in dissimilar ways by the different countries. At the present low level of market integration (Boisseleau, 2004), the envisaged perfectly competitive internal electricity market seems a distant dream that may never come true. In short, we are only beginning to gain an understanding of the ECEI we have created and, as long as we do not understand and cannot predict its emergent behaviour, we cannot pretend to know and be able to adequately handle the risks threatening the well-functioning of this complex system.

It is evident that the repercussions of infrastructure failure and ensuing service disruptions can be extremely serious, especially in advanced economies like those of many EU Member States. The security of the ECEI is central to the welfare of Europe, and guaranteeing that security requires appropriate action. On the one hand, this is a challenging task that will require a sustained effort by many governmental, business and social actors. In a sense, this is going to be a continuous quest, demanding resources, capabilities, skills, and a coordinated European endeavour. On the other hand, the emergence of the ECEI may be seen as a sign of the emergence of a new type of post-industrial society that opens up a reservoir of new opportunities and potential benefits. The ECEI, including the completion of the internal European electricity market, might greatly contribute to a shared sense of social cohesion in Europe, if its adequate performance can indeed be secured. The High Level Group chaired by Wim Kok (November 2004) pointed out that *“Along with investment in R&D, completing the internal market [for network industries] is the key to boosting productivity and innovation”*. Securing the ECEI security is therewith a crucial condition for realising the Lisbon strategy for growth and employment.

The argumentation line developed in this book sets the basis for a vision:

- Securing an adequate performance of the ECEI requires risk governance;
- Risk governance entails that, while pursuing their private objectives, the many stakeholders of the ECEI coordinate their actions in respect of societal goals;
- Risk governance of the ECEI requires the coordination of various technical, organisational and market actions within a composite institutional and regulatory framework;

- Risk governance of the ECEI, with a view to the evolution of its physical asset base as well as market evolution, requires the generation of new knowledge and technologies;
- The concept of the ECEI opens new business opportunities – at the same time in spite and because of the potential risk situations;
- Europe is in a favourable position for taking a worldwide leadership in the various knowledge areas pertaining to risk management and risk governance of complex infrastructure systems-of-systems such as the ECEI.

The political culture in Europe is supportive of respecting public values, in contrast with the private value dominated political culture across the Atlantic. At the same time, the risk governance situation faced by Europe is more challenging, given the strong role of the European nation states and the fact that the ECEI involves both EU Member States and non-EU members.

Our analysis of the ECEI risk situation leads up to the following policy priorities to be implemented at the European level:

1. A new institutional body dedicated to risk governance of the ECEI is urgently needed. The institution of a European Council for the Security of Electric Power is suggested as an option;
2. Smart policies are needed to effectively support the development of a secure ECEI without hampering technological innovation and market development;
3. A multidisciplinary knowledge network and R&D programme on “Security of Critical Infrastructures” are needed to support policy making on critical infrastructure protection and innovation, and to ensure a coherent and consistent policy framework accounting for interconnected and interdependent critical infrastructures.

## **6.2 A European Council for the Security of Electric Power**

Risk governance will not develop by itself. It needs dedicated action with strong commitment by the highest national authorities. Risk governance is about decision-making, involvement of stakeholders, and enforcement of the jointly agreed rules.

We recommend instituting a body with the particular purpose of arranging the risk governance process which is still lacking in the ECEI. This body, that we call the European Council for the Security of Electric Power (ECSEP) was described in Chapter 5. Its explicit task would be to stage a multi-actor risk governance process, in which the electric power

sector, national governments, the European Commission, national and European competition and regulatory authorities, and industrial end-users as well as consumers are involved.

The real value of the proposed strategy is two-fold. First, certain contingencies may have a continent-wide impact and therefore require sophisticated international coordination. This requires a comprehensive risk governance framework and mechanisms for its implementation in the ECEI. Second, the involvement of all stakeholders will provide better assurance that the outcomes of the risk governance process will be acceptable to all parties.

The credibility of the initiative will mainly rely on the dedication demonstrated by the actors responsible for the security of the nation states, and the ones responsible for the reliability of the (national) electricity infrastructure. ECSEP should emerge from the participation of the actors directly involved in operating the ECEI (both the technical systems and the market) and the sector regulators. It will be evident that such a strategy cannot succeed without the full support of the EU and national policy decision-makers.

Risk governance of the ECEI is a necessity for ensuring adequate performance of the ECEI – for the benefit of the European citizen and as a crucial condition for economic growth – and will influence all aspects of the infrastructure:

- Further development of the electric power sector legislative and regulatory framework;
- Evolution of the European electric power market(s);
- Incentives for investment in maintenance, capacity expansion (e.g. new power stations and transmission lines), and innovation;
- Management of congestion on transmission lines (especially interconnectors);
- Assignment of responsibilities and liabilities with respect to all risks, and in light of their insurability;
- Development of new (value added, IT-enabled) ECEI-bound services tailored to the needs of different end-users and catering for the increasing reliability and quality of service required by the service economy; and
- Facilitating public risk acceptance and trust in the electric power infrastructure.

A non-trivial point is that a European initiative will have the potential to influence the electricity systems that are or will be interconnected with the European infrastructure, namely MedRing, Balkans, Eastern Europe and Central Asia. As European security might be affected by the

weaknesses of those systems, the risk governance process will have to address this issue and advise EU and national authorities accordingly.

Our plea for self-regulation may not be self-evident: the criticality of the ECEI to the European economies and society at large may lead policy makers to preferentially consider a hierarchical command-and-control structure for risk governance in the ECEI. The reason why the authors do not opt for the command-and-control type of solution is primarily found in the emergent system dynamic behaviour of the ECEI. The risk governance process should neither impede the market(s) to unfold, nor hamper technological innovation of the ECEI at any level of the system.

A relevant technological innovation trend in the ECEI is that the physical system is equipped with deeply distributed autonomous “intelligence”, enabling a rapid and effective autonomous response to disturbances by local control agents. In analogy with the situation of deeply distributed intelligent agents in the physical system, the adequate performance of the ECEI is also known to rely more and more on the intelligent response of operators in the system control rooms.

In complex systems such as the ECEI and other critical infrastructures, research has shown that distributed autonomous control of the physical networks and distributed responsibility and response capabilities in the social networks are more likely to provide an adequate system response to disturbances than centralized hierarchical control systems (Van Eeten, 2003). Given these findings, the risk governance body to be established should make the best possible use of the knowledge and information available with the actors operating the infrastructure, i.e. the industrial actors. A self-regulatory approach furthermore allows for a certain fluidity of the risk governance process, which is needed as the nature of risks to be governed may change with market and technological developments.

The main challenge for the ECSEP, or an alternative body leading the risk governance process, is to ensure that:

- clear security of supply performance standards for the ECEI are formulated and adhered to;
- roles and responsibilities for risk management are unambiguously allocated, ensuring that high professional standards and a strong sense of responsibility are maintained in all risk-related decisions; and
- stakeholders can exchange risk-relevant information in a secure way, for supporting more knowledgeable risk assessment and risk management practice, and adequate disturbance alert systems and crisis and emergency management capabilities.



It is of crucial importance that the ECSEP or its alternative also addresses the issues of ECEI long term adequacy. To this end, the ECSEP will rely on an effective knowledge network to be formed to support the ECEI risk governance process and innovation of the ECEI.

Summary of recommended actions:

- The institution of a European Council for the Security of Electric Power (ECSEP), as a self-regulatory industrial body; and
- Appropriate actions at the European and national levels facilitating the constitution and effective organisation of ECSEP or an appropriate alternative body.

### **6.3 Policies supporting the development of a secure ECEI**

The risks that confront the ECEI should not only be seen as a challenge; they represent a momentous opportunity for developing a new business landscape. The real challenge is to, concurrently, satisfy the demands for security, implement all necessary technological and organisational solutions, and develop the market of security products and services. Europe has a long tradition of excellence in safety critical and risk-related industries. The ECEI problematique opens a new land of business prospects, which are not exclusive for the electric power infrastructure, but extend to other infrastructures. Europe can take advantage of this opportunity.

This development will be synergetic with the expansion and improvement of our critical infrastructures, and can have a direct effect on the growth of the economy and the creation of technology- and knowledge-related jobs. The result could be a virtuous circle between the need to develop and secure the infrastructures, the European internal market, the uptake of the results from science and technology, a boost to industrial competitiveness, and the materialization of new and innovative businesses.

This market for infrastructure security-related technologies and services will be composed of a diversity of activities, most of them still difficult to envisage. Nevertheless, the following business opportunities can be anticipated:

- Technological products for the detection, monitoring, surveillance, control, etc. of infrastructural systems, based on the conjunction of information and communication technologies, nano-technologies, bio-technologies;

- Services for the risk and security assessment and assurance of infrastructural systems (including real-time discovery of vulnerabilities and threat actions);
- Financial and insurance services related to the procurement, deployment and maintenance of secure infrastructural systems;
- Services related to the design and operation of on-line markets with risk constraints;
- Education and training programmes and services, e.g. geared towards emergency preparedness and crisis management.

These markets will be affected by two factors: policies related to critical infrastructures and emergency management, and the institutional arrangement for risk governance. The latter point was treated in section 6.2. As it regards the first, some initiatives are planned to be implemented at the European level in the near future – the most significant being the organisation of the European Programme on Critical Infrastructure Protection, the launch of which is expected for 2006.

One typical intervention will be the promotion of standards related to security and risk. In this respect, an example is given by the constitution in December 2003 by the European Committee for Standardization (CEN) of a Working Group dealing with the “Protection and Security of the Citizen” which functions as a forum.

These policies can influence the adoption of innovative technologies and services, in the respect of fair competition laws. If Europe succeeds in implementing security of supply performance standards as a distinguishing factor for the ECEI sector (industrial companies, market actors, technology and service providers), which do not impede the markets to unfold and even stimulate technological innovation and the emergence of new services, the ECEI will significantly contribute to the future competitiveness and wealth creation in Europe.

The ECEI is not the only complex infrastructure system-of-system that is crucial to the economic welfare and social well-being in Europe. For other critical infrastructures, a similar challenge of risk governance to secure both short and long term adequacy must be faced. In this respect, the major challenge is to ensure the emergence of a consistent framework of infrastructure protection policies and risk governance processes, such as to ensure that the new risks emerging from interconnections and interdependencies between critical infrastructures are effectively governed. Given the established approach of sector-specific infrastructure policy making, with sector-specific regulatory and legislative frameworks as a result, the challenge of establishing risk governance at the level of interconnected infrastructure systems-of-systems is evidently a tough one. It needs urgent policy attention, as current several processes of

infrastructure convergence unfold, which are effectively blurring the traditional demarcation lines between the different infrastructure sectors. The authors are referring to ongoing processes of physical infrastructure convergence (infrastructures becoming multi-functional), organisational convergence (e.g. the emergence of multi-utility firms) and market convergence.

Summary of recommended actions:

- Design of a system of incentives for the adoption of infrastructure security measures, coordinated at the national and European levels, in the arrangement of Critical Infrastructure Protection policies.
- Develop an “Infrastructure security business” policy that encourages innovation in the securing of infrastructures and the development of new security capabilities that can satisfy the needs of ECEI and other complex infrastructure systems.

#### **6.4 A multidisciplinary R&D Programme and a Public-private Knowledge Platform addressing the “Security of Critical Infrastructures”**

Risk governance and Critical Infrastructures define a new and broad field of knowledge to be extracted from a variety of sources and disciplines and to be combined in order to arrive at applicable solutions. The knowledge needed to identify the right problems and to generate innovative solutions is concerned both with empirical data and tacit knowledge from the practitioners’ world and with new concepts and frontier science generated by academia and other knowledge institutions. The two worlds can greatly enrich each other and need to be amalgamated if Europe is to come up in time with effective countermeasures to many of the risks to the ECEI that were identified in this book. A public-private knowledge platform would be the ideal setting for the intended knowledge exchange between practitioners from the ECEI sector and academics from a variety of disciplines. A European Technology Platform type of structure may be conducive to forging such a partnership, which could then set out to define the needs for research and technology development and design appropriate knowledge development programmes.

Europe urgently requires **research** and **education** at the crossroads of the many disciplines that are concurrently needed for dealing with critical infrastructure management and the governance of the involved risks. *Professional capabilities and proficiency* are needed at the intersections determined by:

- Engineering science disciplines (e.g. systems engineering, electrical and electronic engineering, control engineering, computer and information science, telecommunications, ergonomics, logistics),
- Organisation, management and economics (business management, risk and security assessment and management, market design, evolutionary economics, business economics, public management, decision making and negotiation, the economics of security and risk, insurance, human factors), and
- Socio-political sciences (legal requirements, governance process and national security, national and European decision-making processes, risk-related ethics and values, risk perception and social acceptance, national defence and intelligence, development of European institutions, geopolitics).

In addition, new relevant fields are emerging that require a dedicated effort, for instance system-of-systems engineering, complexity sciences (i.e. the science of complex adaptive systems), assurance of infrastructures and infrastructure related risks, etc.

For the infrastructure sectors, the institution of public-private knowledge platforms, both at the sector-specific level of the ECEI and across infrastructure sector borderlines, holds more value than the strict knowledge exchange function. Such knowledge platforms create a neutral ground for the gathering, analysis and exchange of information on risk and security issues, which may greatly contribute to harmonising public and private strategies towards Critical Infrastructure risk governance. As one of the main problems faced in the risk governance of critical infrastructures is the gap between societal goals and business interests, the importance of a neutral ground where this gap can be discussed and possible strategies be debated, is not to be underestimated. The goals of private actors may not fully correspond to the objectives identified for fulfilling the infrastructure objectives by the risk governance process. For instance, a certain lack of availability of electricity may be acceptable from the business viewpoint, but it is unacceptable from a government or consumers' perspective.

Filling this gap requires dedicated action. This needs to have a European dimension, because failures and risk situations in Europe's Critical Infrastructure affect several countries. A dedicated public-private knowledge partnership will contribute to creating trust between private and public partners for the exchange and discussion of risk-related issues.

The emergence of appropriate multi-disciplinary knowledge and technology development programmes from a Critical Infrastructures knowledge platform is not trivial either. As the academic world is mainly

organised along disciplinary lines, and the worlds of infrastructures and infrastructure governance along sectoral lines, such a co-ordinated knowledge effort will not emerge spontaneously. A focused strategy is needed towards matching the supply and demand of multi-disciplinary knowledge needed to fuel ongoing innovation of Europe's Critical Infrastructures and to ensure adequate risk governance.

Summary of recommended actions:

- Promotion of centres of excellence dealing with multi-disciplinary themes on Risk governance and Critical Infrastructures.
- Development of dedicated knowledge networks between these centres of excellence, infrastructure network managers and system operators, infrastructure service providers, technology providers, governmental bodies and other main stakeholders, for the definition of research programmes and dissemination of research results.
- Promotion of cross-sectoral knowledge platforms and Communities of Practice, involving practitioners from the infrastructure sectors, governmental bodies (e.g. regulators) and academic experts, in a public-private partnership setting, in order to stimulate processes of cross-sectoral learning (e.g. through exchange of best practices).
- Promotion of university curricula in relevant fields pertaining to the design and management of Critical Infrastructures, for the preparation of designers, managers and policymakers dealing with the future generation of ECEI and other Critical Infrastructures.
- Promotion of intensive education and training efforts geared towards the needs of practitioners in the Critical Infrastructure sectors.
- Development of a European R&D programme for the "Security of Critical Infrastructures", taking advantage of existing projects and initiatives under the Information Society Technologies, Environment and Energy Sustainability programmes of the European Commission, and similar national programmes. This programme should include a co-ordinated and multidisciplinary R&D approach to develop proper answers to the complex problems presented by infrastructures.

## Appendix 1

# Learning from the Past – Electric Power Blackouts and Near Misses in Europe

*Markus Schläpfer, Hans Glavitsch*

### A.1.1 Introduction

During the last three years Europe experienced a significantly increased number of wide-area power outages affecting more than 60 million people. The root causes of these low-probability incidents were manifold and every specific sequence of event can be seen as the result of a complex and highly dynamic interplay of multiple faults and contributing factors. However, the blackouts exhibit a number of underlying common patterns and reveal different weaknesses and vulnerabilities of today's European Critical Electricity Infrastructure (ECEI). At the same time the incidents expose the strong dependence of our modern societies on a highly reliable electricity supply. This appendix provides an insight into the most recent and most relevant power outages and near blackouts in Europe by covering the following incidents:

- Blackouts:
  - The interruption of supply in South London, August 28, 2003
  - The power outage in Southern Sweden and Eastern Denmark, September 23, 2003
  - The Italian blackout of September 28, 2003
  - The blackout in Southern Greece of July 12, 2004

- Near Misses:
  - The emergency conditions in Spain, December 17, 2001
  - The rolling load shedding in Italy, June 26, 2003
  - The grid disturbance in Austria, August 27, 2003

Based on publicly available information it is shown how these severe disruptions evolved, how the failures of the electricity supply cascaded into other infrastructures and how much society has been affected. Furthermore, the findings of the authoritative investigations are summarized including their derived recommendations to prevent similar events. The appendix concludes with several lessons learned in the context of this book, by focusing on the influence of the ongoing market liberalization and the pervasive use of information and communication systems (ICS) on the reliability of the ECEI.

## **A.1.2 Recent Electric Power Blackouts in Europe**

### **A.1.2.1 The blackout in South London, August 2003**

#### **A faulty protection device disconnects half a million customers - sequence of events**

During the early evening of Thursday, 28 August 2003, a combination of technical failures led to an electricity supply outage in South London. The sequence of events started with a manual rearrangement of the electricity transmission in order to disconnect an apparently faulty transformer from the grid (see table A.1.1). Thereby, a malfunctioning line protection device interpreted the resulting change of the power flow incorrectly as a fault and automatically disconnected the line. The supply for nearly half a million customers including parts of the subway and the rail transportation system was immediately lost. The system could be restored within less than one hour.

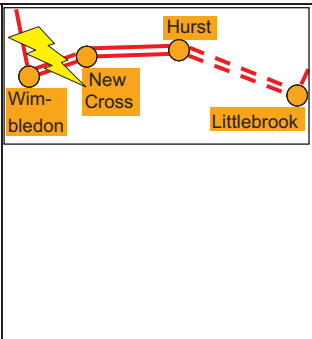
Table A.1.1. Sequence of events in the course of the London blackout (National Grid, 2003), (Ofgem, 2004)

Stage	Time	Location	Events
Preconditions	Aug. 28, 2003 Before 18:11		<ul style="list-style-type: none"> <li>The operation of the electric power system in South London is well complying with the security standards.</li> <li>Total load in South London: 1.1 GW.</li> <li>Two circuits (Wimbledon - New Cross No. 1 and Littlebrook - Hurst No. 2) of the 275 kV transmission network out of service due to scheduled maintenance.</li> <li>A significant supply to the subway is dependent on a single circuit connected to the substation at Wimbledon.</li> </ul>
	18:11		<ul style="list-style-type: none"> <li>Ambiguous alarm in National Grid's control centre<sup>1</sup>: gas accumulation in the oil inside the equipment of a transformer or its associated shunt reactor at the Hurst substation.</li> <li>To avoid potential safety and environmental impacts, National Grid has to shutdown the transformer according to the operational procedures.</li> <li>Therefore National Grid in a first step asks EDF Energy<sup>2</sup> to disconnect the distribution system from the affected transformer (fulfilled at 18:17).</li> </ul>
Grid faults	18:20		<ul style="list-style-type: none"> <li>As a second step National Grid disconnects the Hurst substation from Littlebrook by rearranging the power flow; during this "switching time" (typically 5 to 10 min.) the supplies at Hurst, New Cross and partly Wimbledon depend on one circuit (Wimbledon - New Cross).</li> <li>Shut down of the (assumedly) distressed transformer.</li> </ul>

<sup>1</sup> The National Grid Company owns and operates the affected high voltage transmission system.

<sup>2</sup> EDF Energy owns and operates the affected distribution network.



<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Blackout</p>	<p>18:20</p>		<ul style="list-style-type: none"> <li>• The automatic backup protection device of the operating Wimbledon – New Cross circuit interprets the resulting increase of power flow (well within the operational limits) incorrectly as a fault and immediately disconnects the line.</li> <li>• As a consequence New Cross, Hurst and partly Wimbledon are totally isolated; <b>the area blacks out</b>.</li> <li>• Loss of supply: 724 MW (appr. 20% of the demand in London).</li> </ul>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Restoration process</p>	<p>18:26</p>		<ul style="list-style-type: none"> <li>• Start of the restoration by reconnecting the Hurst substation with Littlebrook.</li> <li>• It turns out that the shunt reactor and not the transformer was the faulty equipment; thus no switching action would have been required.</li> </ul>
	<p>19:14</p>		<ul style="list-style-type: none"> <li>• All supplies to the consumers are restored.</li> </ul>

**Chaos on public transport but no severe accidents - major impacts**

Some 476,000 customers lost their electricity supply (Ofgem, 2004). Despite the relatively short duration the impacts of the blackout were significant as the incident just happened during the rush hours time. About 1,800 trains with thousands of commuters were affected as well as parts of the subway. Consequently, passengers had to be evacuated from the tunnels (BBC News, 2003a). Other people were stuck in elevators as the power went off. The outage of the traffic lights led to chaotic situations on the streets of South London (CNN.com, 2003a). Critical services such as hospitals had to switch on back-up power generators (BBC News, 2003a). The disruption of the rail services continued after power was restored due to disordered timetables.

**Identified root causes and derived recommendations – results of the blackout investigations**

The **National Grid Company plc (National Grid)**, who owns and operates the high voltage transmission system in England and Wales, clearly designates the technical failure of the backup protection device disconnecting the Wimbledon - New Cross No. 2 circuit as the root cause of the blackout (National Grid, 2003). The reason for this malfunction was

the recent installation of a device with inappropriate settings. The investigation finds fault with the fact that this incorrect and obviously not well documented equipment rating was not discovered by the quality checks and commissioning procedures. As opposed to this, it is stressed that the preceding maintenance activities and the disconnection of the affected transformer have been appropriate and complying with National

*“...the direct cause of the loss of supply was the incorrect operation of a backup protection relay...”*

(National Grid, 2003)

Grid’s planning standards and operational practice and are therefore not causes of the blackout. As a consequence, National Grid aims at a close cooperation with other network operators and with all the parties

involved (e.g. EDF Energy, railway and subway operators and emergency services) to improve the overall security of the electricity supply and to enhance the emergency communication. In addition, the management and operation of the automatic protection devices shall be checked and the alarm presentations in the control rooms shall be reviewed.

In accordance with National Grid the **Office of Gas and Electricity Markets (Ofgem)**, the British regulator, names the erroneous installation of the incorrectly rated backup protection relay and the failure to recognize this error as the causes of the power outage (Ofgem, 2004). The investigation report reveals that the relay was only tested according to the contractor’s procedure rather than according to National Grid’s established standard procedure. The latter required it to be tested with its service settings applied, which probably would have allowed to discover the error. In this respect Ofgem also states that the testing documentation was not sufficient. Furthermore, the report highlights the ambiguity of the alarm in the control centre and the adverse design of the substations<sup>3</sup> which made the complex switching action necessary.

*“It is inevitable that errors and omissions can be made by any party involved in the specification, engineering, installation, setting and commissioning of protection systems for power networks.”*

(Ofgem, 2004)

<sup>3</sup> The substations in South London have a “mesh” structure requiring a number of switching operations before an item can be isolated (unlike double busbar substations which generally require only one switching operation).

## **Lessons learned from the blackout in South London**

The blackout in South London was triggered by the unexpected operation of a faulty rated protection device during a critical switching action on the transmission network. The following more generic lessons can be learned from the analysis of this incident:


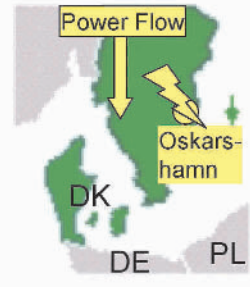

1. Hidden failures of protection devices which remain undetected during normal operating conditions can have catastrophic impacts on the power system under conditions of stress.
2. An effective communication between the actors involved in a contingency (e.g. between the operators of the transmission system and the distribution system respectively) is decisive for keeping the disruption within a limit and to restore the system as quickly as possible.
3. The societal impacts of a blackout are strongly dependent on the time of its occurrence and are significantly exacerbated if vital services such as the public transportation system are affected.

### **A.1.2.2 The blackout in Southern Sweden and Eastern Denmark, September 2003**

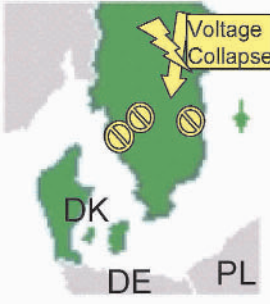
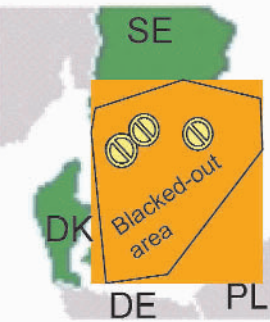
#### **A coincidence of technical failures leads to a widespread blackout – sequence of events**

Around noon on Tuesday, 23 September 2003, the tripping of a large nuclear power plant (NPP) and an almost concurrent short-circuit in a substation in Western Sweden caused a large-area and long-lasting power outage in Southern Sweden and Eastern Denmark, including the capital city of Copenhagen. The most severe outage in 20 years within the Nordic power system affected 4 Million inhabitants. About 6'350 MW of load were lost. The full restoration of the system took more than six hours (see table A.1.2).

Table A.1.2. Sequence of events in the course of the Nordic blackout<sup>4</sup> (Svenska Kraftnät, 2003), (Elkraft System, 2003)

Stage	Time	Location	Events
Preconditions	Sept. 23, 2003		<ul style="list-style-type: none"> <li>• Stable operation with big security margins.</li> <li>• Moderate demand: 15 GW in Sweden and 1.9 GW in Eastern Denmark.</li> <li>• Several generation units and three 400 kV lines out of service in Southern Sweden and Eastern Denmark due to planned maintenance; similarly, the three HVDC circuits from Zealand (Eastern Denmark) and Southern Sweden to Germany and Poland are not available.</li> </ul>
	Before 12:30		
Coincidence of grid faults	12:30		<ul style="list-style-type: none"> <li>• Unit 3 of NPP Oskarshamn trips due to internal valve problems in the feedwater circuits; 1.2 GW are lost.</li> <li>• The applied grid security standards allow the system to cope with this "standard contingency" by automatically increasing production at other power stations.</li> <li>• More power is flowing on the western side to supply the demand in the south.</li> </ul>
	12:35		<ul style="list-style-type: none"> <li>• Double busbar fault in the 400 kV substation in Horred: below its maximum loading the mechanical structure of a switch breaks apart and causes a short circuit between two adjacent busbars, which are immediately separated by automatic protection devices.</li> <li>• As a consequence, two units of the NPP Ringhals (totalling 1.8 GW) and two important 400 kV lines connecting Central and Southern Sweden, all connected to these busbars, are lost.</li> </ul>

<sup>4</sup> The maps used as a base for the charts in this and the following tables of this appendix are taken from: <http://en.wikipedia.org>. The charts are therefore subject to the GNU Free Documentation License, see <http://www.gnu.org/copyleft/fdl.html>.

<p>Voltage collapse</p>	<p>12:35-12:37</p>		<ul style="list-style-type: none"> <li>• The generation loss causes low voltages and transient power oscillations; frequency drops down to around 49.00 Hz.</li> <li>• Practically no production left in Southern Sweden; the area is briefly supplied from Zealand's power stations via the Øresund connection and from Central Sweden via the eastern transmission lines.</li> <li>• As the grid along Sweden's west coast loses its transmission capacity the eastern side carrying energy in the north-south direction becomes heavily overloaded; finally this leads to a voltage collapse south of Stockholm.</li> </ul>
<p>Blackout</p>	<p>12:37</p>		<ul style="list-style-type: none"> <li>• Circuit breakers are automatically triggered from distance protection devices reaching the low impedance threshold; this separates the grid into two parts.</li> <li>• Insufficient generation in the southern part of the grid (South Sweden and Eastern Denmark); within seconds the frequency and voltage drops to levels where generators disconnect.</li> <li>• <b>The entire subsystem collapses;</b> only some minor hydro power station feeding small islands survive; due to the rapid voltage collapse in Zealand the local power stations can not switch on the stable house-load operation.</li> <li>• Loss of supply in Sweden: 4.5 GW; in Denmark: 1.9 GW.</li> </ul>
<p>Restoration process</p>	<p>12:37</p>		<ul style="list-style-type: none"> <li>• Start of the restoration based on the intact northern part of the grid.</li> <li>• The loss of the remote control of a Swedish substation, the incapability of Zealand's power stations to switch on their house-load operation and the failure of the black-start facilities in another Danish generation unit delay the restoration process.</li> </ul>
	<p>appr. 19:00</p>		<ul style="list-style-type: none"> <li>• Power system back in full operation mode; however, some customers are not supplied until 22:00.</li> </ul>

## South Sweden and Copenhagen without electricity - major impacts

In Sweden around 1.8 million people and in Denmark around 2.4 million people have been affected (Elkraft System, 2003). Non-supplied energy totalled to 10 GWh in Sweden and 8 GWh in Denmark (Svenska Kraftnät, 2003). Similarly to the blackout in London, trains stopped and the subway in Copenhagen stuck so passengers had to be evacuated (BBC News, 2003b). Furthermore, people were trapped in elevators and in major cities traffic came to standstill as traffic lights failed (CNN.com, 2003b). The airport of Copenhagen had to be closed. Hospitals had no problems due to the successful switching on back-up generators (CNN.com, 2003b).

### Identified root causes and derived recommendations – results of the blackout investigations

In October 2003 **Svenska Kraftnät**, the state owned Swedish Transmission System Operator (TSO), published a short investigation report on the course of events (Svenska Kraftnät, 2003). The report clearly designates the coincidence in time of the two non or only weakly interrelated technical failures (namely the outage of the two units at the NPP Oskarshamn and the double busbar fault at the Horred substation) as the root cause of the blackout, since the Nordic electric power system

simply is not designed and operated to cope with such a low-probability event.<sup>5</sup> Based on its findings Svenska Kraftnät derived a set of recommendations for different system improvements. Technical measures include the building of a new 400 kV transmission line to the South of Sweden, the upgrading of generation capacity in the area and the

*“The cause was a close coincidence of severe faults leading to a burden on the system far beyond the contingencies regarded in normal system design and operating security standards”*  
(Svenska Kraftnät, 2003)

development of more intelligent system protection schemes. Management and operation related improvements include a review of the reliability standards as applied by the Nordic Transmission System Operators, enforced inspections as well as a better supervision of out-sourced maintenance. As a measure related to the legal framework Svenska

<sup>5</sup> The grid is operated under the security constraint of the *N-1 criterion*: the random outage of a single, grid or production unit shall not result in a supply failure, overload or other disruptions (Nordel, 2004).

Kraftnät recommends mandatory technical rules for power plants in order to switch on stable house-load operation during external grid disturbances.

In accordance with Svenska Kraftnät the report of **Elkraft System**, the former Eastern Danish system operator, determines the two almost simultaneous technical failures at the NPP Oskarshamn and at the Horred substation (see table A.1.2) as the causes of the power outage (Elkraft System, 2003). Elkraft System also confirms that after the double busbar fault in Horred the power outage was not avoidable according to the present system design and security criteria. As lessons learned from the blackout the report stresses the importance of adequate design quality and maintenance for critical grid

*“The power failure on 23 September stresses the importance of having sufficient production in the vicinity of the electricity consumption centres...” and “...demonstrates the importance of strong transmission connections.”*

(Elkraft System, 2003)

components and the possibility to implement voltage-controlled load shedding for the handling of severe voltage drops. Furthermore, the need for an intelligent wide-area disturbance response concept including the coordinated disconnection of transmission lines and power stations is stressed. The priority for the disconnection or reconnection of consumers shall be checked and the communication between the different control rooms with respect to the information of the consumers shall be improved. Concerning the restoration phase Elkraft System outlines the necessity to assure a high reliability of black-start units and the ability of other generators to switch on house-load operation. In its report Elkraft System also highlights the basic problems of limited generation in the area of high loads (which is adverse to the voltage support) and of limited transmission capacities (which favours the cascading spreading of line outages). Moreover it is mentioned, that there is a need to assess the influence of the recent electricity market developments on the system using pattern and to revise the adequacy of today’s technical specifications and operational practices.

### **Lessons learned from the blackout in Sweden and Denmark**

The blackout in Southern Sweden and Eastern Denmark was caused by the coincidence in time of two technical failures, the system simply was not designed for. The following generic lessons can be derived from the incident:

1. The current reliability policy for the interconnected Nordic power system and the associated security standards strongly focus on individual, anticipated or “high-probability” events, such as the random outage of a single transmission line, a generation unit or a transformer. The system is not designed or operated in order to cope with the coincidence in time of several independent component outages. However, the blackout in Southern Sweden and Eastern Denmark makes aware that such “low-probability-high-impact scenarios” might happen and therefore questions the adequacy of this reliability framework.
2. Limited reactive power support in the area of high loads is a significant risk factor for voltage instabilities.
3. High system loadings increase the risk of cascading transmission line outages.
4. The lack of generators being able to switch on their house-load during a grid disturbance and insufficient units with black-start capabilities complicate and delay the restoration process after a large-scale blackout.

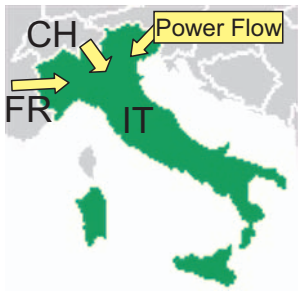
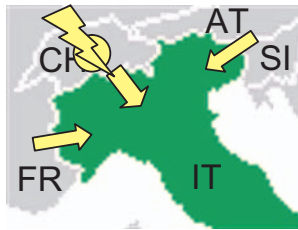
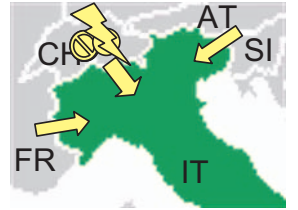
### **A.1.2.3 The Italian blackout of September 2003**

#### **From a tree flashover to a nationwide blackout – sequence of events**

In the early morning of Sunday, 28 September 2003, a huge power cut plunged Italy into darkness. The blackout, which was triggered by the trip of a transit transmission line in Switzerland as a result of a tree flashover, occurred at 3:27 AM in the northern part and spread rapidly over the whole country except Sardinia (see table A.1.3). 56 million people have been affected, while the energy not supplied totalled to 177 GWh. Restoring power to the whole country took up to 18 hours.



Table A.1.3. Sequence of events in the course of the Italian blackout (UCTE, 2004a)

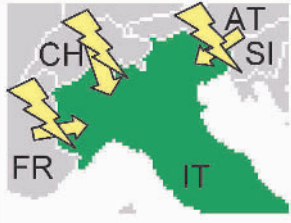

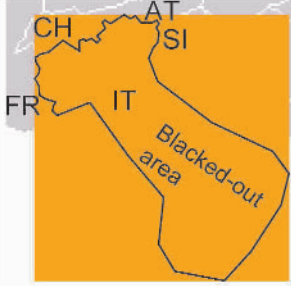
Stage	Time	Location	Events
Preconditions	Sept. 28, 2003 03:00		<ul style="list-style-type: none"> <li>Stable operating conditions.</li> <li>Total load: 27'444 MW.</li> <li>Total import: 6951 MW, 300 MW more than scheduled.</li> <li>Power flow CH - I : 3'610 MW, exceeds the agreed exchange by 550 MW.</li> </ul>
	03:01:42		<ul style="list-style-type: none"> <li>Trip of the highly loaded 380 kV line Mettlen - Lavorgo caused by tree flashover (at 86% of the max. capacity).</li> <li>Unsuccessful re-closing because of a too high phase angle differential<sup>6</sup> (42°).</li> <li>As neighboring lines take over the power flow, the nearby 380 kV transit line Sils-Soazza becomes overloaded (110% of its max. capacity); the operators are unaware of the urgency to relieve the overload within 15 min.<sup>7</sup></li> </ul>
Cascading line tripping	03:11		<ul style="list-style-type: none"> <li>Phone call between ETRANS<sup>8</sup> and GRTN<sup>9</sup>: ETRANS requests to reduce the Italian import by 300 MW to meet the agreed schedule.</li> </ul>
	03:21		<ul style="list-style-type: none"> <li>GRTN reduces the Italian import by about 300 MW.</li> </ul>
	03:25:21		<ul style="list-style-type: none"> <li>As the measures taken are insufficient to relieve the overload, the Sils-Soazza line trips following a tree flashover. The conductors of the line were sagging due to overheating.</li> <li>Three overloaded 220 kV lines towards Italy trip automatically.</li> </ul>

<sup>6</sup> A phase angle differential is an electro-technical phenomenon in AC operation indicating the time lag of the sinusoidal oscillating voltage between the two ends of a transmission line.

<sup>7</sup> After this time span the line sag due to increased thermal heating would exceed the operational limits, as has been calculated by UCTE in the course of its investigations.

<sup>8</sup> ETRANS is the coordination body between the Swiss grid companies (and not a TSO itself).

<sup>9</sup> GRTN is the Italian TSO.

	03:25:28		<ul style="list-style-type: none"> <li>The Italian grid loses its synchronism with the UCTE main grid leading to an almost simultaneous disconnection of all remaining interconnection lines by regular function of the protection devices.</li> </ul>
Loss of angle stability	03:25:33		<ul style="list-style-type: none"> <li>The Italian grid is completely separated from the UCTE network.</li> <li>Instability phenomena in the northern part of the Italian network lead to severe voltage drops.</li> <li>Increased frequency and unpredicted flow patterns within the UCTE grid due to the sudden power surplus (former export to Italy) lead to a precarious situation; some generation units shut down.</li> </ul>
Blackout	03:27		<ul style="list-style-type: none"> <li>Despite primary frequency control, automatic disconnection of the pump storage plants in Northern Italy and automatic load shedding (10 GW), the voltage and frequency drop within the Italian grid cannot be mastered and generation plants start to trip; <b>the blackout spreads over the country.</b></li> </ul>
Restoration process	03:28 - 08:00		<ul style="list-style-type: none"> <li>Northwest of Italy completely re-energized and connected to the UCTE grid.</li> <li>Restoration is affected by the outage of the telecommunication network, lack of information on the root cause of the blackout, failure of black-start units and by the fact that only a small number of generators managed to switch on their house-load operation.</li> </ul>
	08:00 - 12:00		<ul style="list-style-type: none"> <li>Load in the northern area restored.</li> <li>The failure of the telecommunication system still complicates the coordination of the restoration activities.</li> </ul>
	12:00 - 17:00		<ul style="list-style-type: none"> <li>Restoration of the whole mainland completed.</li> <li>Interconnection with the UCTE grid completed.</li> </ul>
	17:00 - 21:40		<ul style="list-style-type: none"> <li>Restoration of the Sicilian grid.</li> <li>Italian power system under control and cessation of the emergency conditions.</li> </ul>

### Thousands stuck in trains and subways but no severe damages – major impacts

Almost the whole country with its 57 million population experienced the blackout. Hundreds have been trapped in elevators, for example. Fortunately people did not panic as the lights turned off and the half a million people celebrating the all-night “Notte bianca” festivities in the streets of Rome kept cool (Il Corriere della Sera, 2003a). Because the blackout happened on a Sunday morning the financial damage could be kept within a limit. No effects on the financial markets are reported. The estimated economic loss totals to about 120 million Euro due to spoiled foodstuffs and belated opening hours of shops and restaurants (Confcommercio, 2003). Continuously working industries like steel, cement or plastic factories lost about one hundred thousand Euros for every single firm (Unindustria Padova, 2003). The impact on other critical infrastructures varied depending on their susceptibility, see table A.1.4.

Table A.1.4. Impact on electricity dependent infrastructures

Infrastructure	Impact
Transportation	<ul style="list-style-type: none"> <li>• About 110 trains with more than 30'000 passengers stopped (Il Corriere della Sera, 2003a)</li> <li>• Subways in Rome and Milan stuck (Il Corriere della Sera, 2003a)</li> <li>• Flights have been cancelled or were delayed (La Repubblica, 2003)</li> <li>• Outage of traffic lights partly led to chaotic situations in major cities, but no severe accidents (Il Sole, 2003)</li> </ul>
Water Supply	<ul style="list-style-type: none"> <li>• Interruption for up to 12 hours mainly in Southern Italy (La Repubblica, 2003)</li> </ul>
“Open Access” Information and Communication	<ul style="list-style-type: none"> <li>• Telephone and mobile phone networks in a critical state but operable (Il Corriere della Sera, 2003a)</li> <li>• Internet data transfer rate down to 5 percent of its normal value (La Repubblica, 2003)</li> </ul>
Health Services	<ul style="list-style-type: none"> <li>• No serious problems due to the use of diesel-driven generators in hospitals (Il Corriere della Sera, 2003a)</li> </ul>

## Identified root causes and derived recommendations – results of the blackout investigations

The **final report of the UCTE Blackout Investigation Committee**<sup>10</sup> (UCTE, 2004a) stresses that the blackout has to be seen against the background of the discrepancy between the original design of the UCTE system and today's using pattern. It is outlined that the aim of the synchronous interconnection in Continental Europe was to assure mutual assistance in maintaining system reliability, to increase the economic efficiency by sharing reserves and to allow limited international trade. However, mainly as a result of the ongoing market liberalization

*“Today's market development with its high level of cross-border exchanges was out of the scope of the original system design.”*

(UCTE, 2004a)

international trading increased leading to drastically higher cross-border flows. The UCTE Investigation Committee clearly states that neither management nor operational procedures, which traditionally both are designed for national needs, have been adequately adapted to this new

situation.<sup>11</sup> Italy covers a high amount of its annual electricity consumption by imports (around 15% in 2002) as a result of the significant differences of the production costs between Italy and the rest of Europe<sup>12</sup>. Within this context the report names four root causes of the blackout and lists a number of recommendations:

1. *Unsuccessful re-closing of the Mettlen-Lavorgo transmission line due to a too high phase angle differential (42°):*

Attempts to bring the line back into operation failed because of an automatic gear refusing to switch the breakers (see table A.1.3). This device aimed at protecting nearby generators from a transient stress arising during the re-closure of the line. The higher the bulk transmission the higher the phase angle, and the more violent the transient. Depending on the network topology and on the location of the power injections, the device was set to react at 30°. The UCTE Committee recommends the enhancement of the N-1 criterion as

<sup>10</sup> All network operators involved in the incident are members of the UCTE and therefore subject to its reliability standards.

<sup>11</sup> For more details on this issue see chapter 3.

<sup>12</sup> Italy phased out of nuclear energy in 1990 with only limited investments in alternative generation capacity.

defined in the UCTE Operation Handbook (UCTE, 2004)<sup>13</sup> by incorporating the phase angle.

2. *Lacking a sense of urgency regarding the overloaded Sils-Soazza line and call for inadequate countermeasures in Italy:*

To restore the N-1 security after the loss of the Mettlen-Lavorgo line corrective measures outside Switzerland would have been necessary, namely ETRANS to ask GRTN for the shut down of the pump storage plants in Northern Italy. The UCTE Committee notes

“...the TSOs operate the system closer and closer to its limits as allowed by the security criteria, which in essence have remained unchanged.”

(UCTE, 2004a)

that this procedure was identified by ETRANS and successfully demonstrated in a previous case. However, the Swiss operators did not follow this procedure but only requested to reduce the Italian import by 300 MW. Moreover, they have been unaware of the fact that the overload of the Sils-Soazza line was technically allowable for not more than 15 minutes. According to the report the whole procedure demonstrates the inadequacy of joint emergency procedures and information exchanges<sup>14</sup> between neighbouring TSOs. In this respect UCTE recommends mandatory emergency procedures and the enhancement of the N-1 security criterion by taking the interference between different control areas more into account. Therefore, the exchange of real time data shall be extended among neighbouring TSOs and the frequency and quality of the DACF<sup>15</sup> calculations be increased. Furthermore, the report recommends the determination of an allowable time delay to return the system to the N-1 secure state after a contingency.

3. *Angle instability and voltage collapse in Italy:*

The disconnection of the Italian grid from the UCTE network came along with severe dynamic interactions between the two systems

<sup>13</sup> The N-1 criterion as defined by the UCTE Operation Handbook is similar to the one provided by Nordel, see p.165.

<sup>14</sup> It still remains unclear whether ETRANS informed GRTN about the outage of the Mettlen-Lavorgo line during the phone call – GRTN did not have direct visibility on the Swiss system.

<sup>15</sup> The Day Ahead Congestion Forecast (DACF) allows the TSOs to carry out reliable load-flow forecasts and to identify congestions by exchanging relevant grid information with other TSOs (UCTE, 2004).

leading to instability phenomena in Italy. On this account 21 out of 50 large thermal generation units were lost before the nominal 47,5 Hz frequency threshold was reached, impeding the successful island operation of Italy. The report states that the risk of such instability phenomena is due to highly loaded systems by long distance transmission. The Committee recommends the integration of voltage stability issues into the short-term contingency analysis and the acceleration of the ongoing Wide Area Management System (WAMS)<sup>16</sup> installation, a support tool for dynamic analysis and monitoring of the UCTE system.

4. *Possibly inadequate right-of-way maintenance practices:*

The report states that the first line flashover “may have been caused by insufficient right-of-way maintenance”.

The UCTE Committee additionally identified a number of shortcomings not only related to the mechanisms triggering the blackout itself but also related to the performance of the whole UCTE system during the event and to the restoration process in Italy. These weaknesses include too sensitive settings of generator protection devices and inadequate generation in regions of high loads.

The **Swiss Federal Office of Energy (SFOE)** designates likewise the insufficient coordination of the Swiss, Italian and French operators as decisive for the evolvement of the blackout, albeit it mainly blames the time delay between the request by ETRANS to reduce the Italian import and its fulfillment by GRTN (SFOE, 2003). The requested measure itself - namely to adjust the import by 300 MW in order to comply with the agreed schedule - is not judged as inadequate. SFOE also stresses the unresolved discrepancy between the international trading interests and the technical constraints of the interconnected electric power system which is seen as the underlying reason for the blackout. The report thereby refers primarily

*“Present-day standards  
and legal instruments are  
lagging well behind economic  
realities.”*

(SFOE, 2003)

to the load flow on the Mettlen-Lavorgo line which was well above its safe reference value just before the breakdown. The reference load flow serves as the basis for traders to specify volumes of electricity exports to Italy. The reason for the unplanned deviation was that the volumes and locations of power injections realized

<sup>16</sup> The WAMS consists of time synchronized logging devices at certain places in the grid. The recordings allow to trace frequency variations and are used to monitor inter-area oscillations and to support off-line stability analysis (UCTE, 2004a).

as the result of trading operations were different from those used for the calculation of the reference flows. Would the loading of the Mettlen-Lavorgo line have been compliant with the reference value, the phase angle over the line would have been smaller than 30°. This would have made the re-closure of the line possible and the blackout would have been avoided. Furthermore, the report points out that the Italian and French regulators agreed on electricity export capacities to Italy for the year 2002 and again for 2004 without including Swiss authorities in this decision-making process. As a result the Swiss network operators have been faced with more unforeseen transit power flows. SFOE recommends Switzerland to create a strong regulatory body with the ability to regulate and control the market as an equal partner together with regulators of neighbouring countries and advises the different owners of the Swiss transmission network to set up a single, independent grid operator.

The **Italian Regulatory Authority for Electricity and Gas (AEEG)** and the **French Regulatory Authority for Energy (CRE)** conducted a joint inquiry<sup>17</sup> into the blackout, which was restricted on the initial phase of the event leading to the separation of the Italian grid (AEEG and CRE, 2004). In their report AEEG and CRE do not see the increased cross-border trades nor the discrepancy between scheduled commercial flows and physical flows as causes of the blackout but rather accuse the Swiss network operators of having omitted appropriate preventive measures, of having failed to meet the UCTE rules and of having committed operational mistakes. By way of justification it is stated that the assumptions for the

*“It shall be enforced an independent assessment and control of UCTE rules.”*

CRE and AEEG, 2004

line sag calculations in Switzerland have not been adequate to the actual high loads and that the phase angle difference over the Mettlen-Lavorgo line (see table A.1.3) was predictable.

It is underscored that there was no official agreement between GRTN and ETRANS on the adjustment of the pumping stations in Northern Italy. However, because this measure would have been necessary to restore the N-1 security, it is concluded that the Swiss operators did not comply with the UCTE rules before the incident. Furthermore, the time delay between the line outage and the phone call and the inadequate request to reduce the Italian imports by only 300 MW are highlighted. This deviation from the scheduled exchange is judged as

<sup>17</sup> A joint report with SFOE as initially planned has not been accomplished due to disagreements on information exchanges and on the direct participation of the TSOs in the inquiry.

normal and inevitable for the operation of the interconnected system. AEEG and CRE recommend in their report that the existing UCTE rules shall be made unambiguously clear and controlled by the national regulators. For example, a maximum allowable time period to bring the system back to N-1 security conditions shall be defined. The two regulatory authorities also highlight the urgent need of an adequate coordination among the TSOs in Continental Europe concerning operational day-ahead grid planning and real time operation so that all the physical transit flows are under the control of the TSOs. AEEG and CRE refer to procedures for capacity allocation, transaction nominations and grid operating condition forecast as proposed by ETSO in its coordinated congestion management project (ETSO, 2004).

In addition to the joint investigation with CRE, the Italian regulatory authority **AEEG** analyzed the subsequent technical events in Italy after the separation from the UCTE grid as well as the restoration process (AEEG, 2004). Key findings include the insufficient effectiveness of automatic load shedding procedures and the early trip of 21 generation units (see above), which did not comply with the technical rules of connection to the national transmission network. Furthermore, AEEG finds fault with the inability of generation units to perform black starts and with the high failure rate of other units to switch on their house-load. AEEG also highlights the failure of the telecommunication systems for the remote control of grid components and its emergency backup power supply (between 8:00 and 14:40 the remote control system was not available, what made the use of a backup satellite telecommunication system necessary, further compromising the restoration process).

### **Lessons learned from the Italian blackout**

The case of the Italian blackout pinpoints different system weaknesses and operational risks as resulting from the recent developments of the European electricity market with its high level of cross-border exchanges. In this context, the following lessons can be learned:

1. Highly loaded transit lines due to long distance power transfers – as resulting from commercial transactions between different countries –



increase the risk of severe grid disturbances in case of a contingency situation.

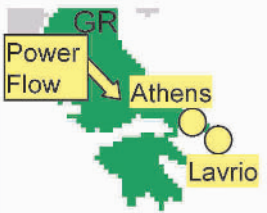
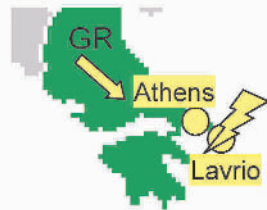

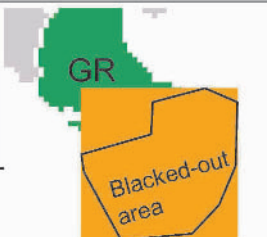
2. The real-time monitoring of the system is mostly limited to the control area of a TSO (i.e. a country in most of the cases) and is therefore not adequate anymore to today's high-level of cross-border exchanges.
3. Insufficient coordination between the TSOs in case of a contingency actually propels the occurrence and spreading of a blackout.
4. The TSOs have only limited influence on the cross-border electricity trades and are therefore more and more confronted with the risk of unexpectedly congested tie-lines.
5. The settings of generator protection devices are in many cases too sensitive so that the support of the grid stability is limited.

#### **A.1.2.4 The blackout in Southern Greece of July 2004**

##### **A power cut hits Athens, just one month before the Olympic Games - sequence of events**

On Monday, 12 July 2004, just four weeks before hosting the Olympic Summer Games, Athens together with Southern Greece was hit by a major electric power breakdown. The blackout was caused by voltage instabilities. Until noon the significantly increasing demand mainly due to the use of air conditioning systems burdened the system heavily. A synchronisation problem with a power plant at 12:15 deteriorated the voltage level even more. The remaining generation units were unable to support the reactive power which finally led the system into a voltage collapse. About 5 million people have been affected. The restoration process started immediately. At around 16:00 all costumers were successfully re-supplied (see table A.1.5).

Table A.1.5. Sequence of events in the course of the Hellenic blackout (Vournas, 2004)

Stage	Time	Location	Events
Preconditions	July 12, before 12:12		<ul style="list-style-type: none"> <li>• High demands due to hot weather conditions (air conditioning systems).</li> <li>• The unavailability of four 150 kV lines due to various failures and maintenance and the outage of a 125 MW unit on the Peloponnes are leading to unusually high loadings and low voltages in the grid around Athens.</li> <li>• At 7:08 unit 2 (rated 300 MW) of the Lavrio power plant shuts down due to a failure in the auxiliary equipment; technical problems delay the start up.</li> <li>• Until noon the demand in Greece raises to 9'160 MW with the result that voltage declines to 90% of the nominal value.</li> <li>• At 12:01 unit 2 of the Lavrio station is brought back to service what stops the voltage drop.</li> </ul>
	12:12		<ul style="list-style-type: none"> <li>• Unit 2 of the Lavrio power plant – still on manual control - fails again because of a too high water level in the steam drum.</li> <li>• As a consequence the reactive power supply in the Athens area becomes insufficient and voltage declines again.</li> </ul>
Voltage collapse	12:25 – 12:37		<ul style="list-style-type: none"> <li>• The Hellenic transmission system operator (HTSO) requests a load shedding of 100 MW.</li> <li>• At 12:30 80 MW are manually disconnected.</li> <li>• The demand raises to 9'320 MW and voltage drops further.</li> <li>• At 12:35 HTSO requests an additional load shedding of 200 MW, which cannot be fulfilled anymore.</li> </ul>
	12:37 – 12:38		<ul style="list-style-type: none"> <li>• Unit 3 of Alivieri power station trips automatically at 12:37 and subsequently the remaining unit is manually shut down (the cause of this tripping is not clear).</li> <li>• Voltages are collapsing.</li> </ul>
Blackout	12:39		<ul style="list-style-type: none"> <li>• The system is split by the undervoltage protection devices of the 400 kV lines.</li> <li>• The remaining generation units in the separated southern part disconnect; <b>the blackout spreads in the area of Athens and the Peloponnes island.</b></li> </ul>

			<ul style="list-style-type: none"> <li>• The sudden power surplus causes frequency disruptions in the neighboring systems of the former 2<sup>nd</sup> UCTE zone.</li> </ul>
Restoration	12:39 – 16:00		<ul style="list-style-type: none"> <li>• Taking the intact northern and western part of the Hellenic grid as a base, the power can be restored successively within two to three hours with some exceptions.</li> </ul>

### Traffic jams and failed air conditioning - major impacts

The blackout hit more than 5 million people in Southern Greece. It caused chaos on the roads in the Athens metropolitan area as a consequence of failed traffic signals and stalled electric trolleys (USAToday.com, 2004). Hundreds of passengers of the Athens subway had to be evacuated. The emergency services received hundreds of calls about people trapped in elevators (BBC News, 2004). The blackout also caused some cell phone networks to overload (USAToday.com, 2004). The airport of Athens as well as the hospitals successfully switched on their back-up generators (BBC News, 2004).

### Identified root causes and derived recommendations – results of the blackout investigations

In the wake of the blackout the **Minister of Development of Greece** appointed an Investigation Committee, whose final report “On the Reasons for the Interruption of Electricity Supply on July 12” is publicly available. This section is based on an English summary of this report, provided by Vournas (Vournas, 2004). The report highlights the vulnerability of the Hellenic grid with respect to voltage instabilities, as has been shown by several events in the recent past, and designates the insufficient technical

*“The Hellenic system is prone to voltage instability.”*

(Vournas, 2004)

upgrades of the system as “a major factor leading to the blackout”. The reason for these voltage problems is given by the long distance power

transfer from the generation areas in the North and West of the country to the load centres around Athens in the South. According to the report technical reinforcements such as the building of a new transmission line, a substation and several capacitor banks<sup>18</sup> have been planned (also in the

<sup>18</sup> Capacitor banks are a source of reactive power and are important for voltage support.

context of the Olympic Games in Athens 2004) but not fully implemented before the blackout.

### **Lessons learned from the blackout in Greece**

At least in the public domain, the blackout in Greece is not as well documented as the other investigated incidents and many factors and interrelations in the course of the event remain unclear. However, some generic lessons can be learned from this case, including:

1. Long import distances without adequate reactive power support lead to a significant risk of voltage instabilities.
2. Exceptional climatic conditions such as unusually high temperatures may seriously endanger the reliability of the electric power system, if not adequately taken into account within the planning process.

## **A.1.3 Near Misses**

### **A.1.3.1 Emergency conditions in Spain, December 2001**

#### **Sequence of events and root causes as identified by the investigations**

This section is based on a report on recent electric power blackouts published by Eurelectric (Eurelectric, 2004a).

On Monday, 17 December 2001, unusually cold weather conditions led to high demands in Spain. Therefore, the unavailability of 2147 MW of thermal power (of which 1656 MW in the South and East) together with the simultaneous shortage on hydropower after a long period of drought resulted in high power flows from the Northwest to the Southeast of the country. As voltages declined, the generators in the area increased the reactive power support by decreasing their active power output. However, the adverse consequence of this action was an increased import of active power from the Northwest leading to a significant voltage drop in the area of Levante and Madrid.

Since the demand was further growing during the late afternoon even to a historical peak value, Red Eléctrica, the Spanish TSO, had to apply all

available corrective and preventive measures to overcome the low voltages such as the disconnection of interruptible loads as contractually allowed, the cancellation of exports and the increase of imports from the neighbouring countries. However, at 18:45 the Spanish power system was still running under emergency conditions being prone to the risk of voltage collapse and Red Eléctrica had to request load shedding from the distribution companies in the regions of Madrid (300 MW) and Levante (200 MW).

The restoration process was immediately started. About 50% of the load was restored at 19:40 and the remaining 50% at 19:55. The energy not supplied totalled to about 300 MWh.

The investigation report of **Eurelectric** (Eurelectric, 2004a) identifies the low hydro reserves due to the extremely dry season, the unavailability

*“Not only the peak load has increased constantly since 1998, the generation capacity has not practically grown up in the last three years.”*

(Eurelectric, 2004)

of the thermal units mainly due to market induced changes of the operational regime and the historical peak load as the reasons for the event. The report also mentions that the generation capacity was not adequately upgraded in view of the

increasing electricity demand in Spain during the years before the incident. Eurelectric highlights the efficient cooperation between the TSO and the generation and distribution companies, the well prepared contingency operation procedures (e.g. clearly established load shedding plans) and the permanently actualised grid recovery planning. According to the report these measures were decisive for avoiding the voltage collapse, and for quickly restoring normal operating conditions.

## Lessons learned

A combination of exceptional climatic conditions (unusually cold weather after a long-lasting period of drought) and limited generation capacity brought the Spanish power system into a state of emergency, which could only be managed by applying appropriate load shedding. The following three lessons can be learned from this near miss incident:

1. Inadequate generation capacity or insufficient reactive power support in a region with high loads increases the risk of voltage instabilities.

2. Similar to the blackout in Greece of July 2004, this incident shows the vulnerability of the electric power systems with regard to unusual climatic conditions.
3. An effective cooperation between the TSOs and the distribution and generation companies is decisive during contingency situations.

### **A.1.3.2 Rolling load shedding in Italy, June 2003**

#### **An exceptional heat wave over Europe strains the Italian power system - sequence of events**

This section is based on an English summary of the final investigation report of the Italian Authority for Electricity and Gas (AEEG) on the technical sequence of events (AEEG, 2003).

As the days before, on Thursday, 26 June 2003, exceptionally high temperatures led to an unusually high electricity consumption in Italy mainly due to the increased use of air conditioning systems and ventilators. At the same time, thermal generation capacity was limited, partly due to high ambient and cooling water temperatures after a long period of drought. For the same reasons France had to reduce its exports to Italy in order to cover its own demands. This practice was foreseen in the contractual agreement between the French and the Italian power providers.

In order to prevent a potential collapse of the Italian power system along with the disconnection from the UCTE grid GRTN (the Italian TSO, see the Italian blackout case, Section A.1.2.3) had to carry out far-reaching emergency measures such as the disconnection of 39 major “interruptible” industrial customers as contractually allowed, amounting to about 450 MW. However, between 9 a.m. and 4.30 p.m. rolling load sheddings of 90 minutes duration had to be applied to general users amounting to about 1700 MW.

#### **Major impacts**

The energy not supplied due to the rotating outages totalled to 12.9 GWh (GRTN, 2004). About 7.3 million customers have been affected (AEEG, 2003). According to Italian newspapers many people have been trapped in elevators, the outage of traffic lights in the cities of Rome, Milan and Turin led to chaotic situations, computers crashed, refrigerators

defrosted and fueling stations shut down (e.g. *Il Corriere della Sera*, 2003b). Most people were not informed about the planned outages before Thursday morning or experienced the interruptions even without any warning (*Il Corriere della Sera*, 2003b). Electricity was guaranteed only to critical services such as hospitals, the police and the public transport.

### **Root causes as identified by the investigation**

In its report, **AEEG** names the inadequate national generation capacity and the high dependence on imports, which are reduced during summertime, as the “origin of the event” (AEEG, 2003). The authority blames ENEL – the single Italian power provider – of having taken 2300 MW generating capacity out of service for a longer period than is usual for normal maintenance, and of having omitted to hold an equivalent amount of national production capacity in reserve in view of the envisaged reduction of imports from France. In this respect, AEEG also criticises GRTN of having insufficiently reallocated the import capacities in order to compensate the reduction from France. Finally, the investigation shows that GRTN failed to manage the national reserve capacity by setting up appropriate contractual arrangements with the power producers as foreseen by national directives.

### **Lessons learned**

The case of the planned electric power outages in Italy is characterized by the interplay of a long period of hot weather conditions - leading to high electricity consumption and limited thermal generation capacity - and the insufficient management of reserve capacity. On a generic level, the following lessons can be learned:

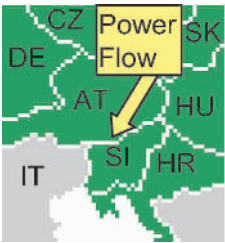

1. Long-lasting exceptional climatic conditions over large geographical areas, such as heat waves and droughts, pose a serious risk to the ECEI.
2. Inadequate reserve capacity in a region which is highly dependent on imports endangers the security of supply.
3. Timely information to electricity customers about planned supply interruptions is decisive to keep damages within a limit.

### A.1.3.3 The grid disturbance in Austria, August 2003

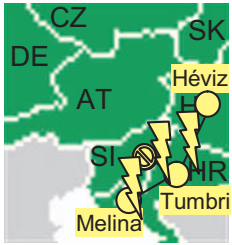
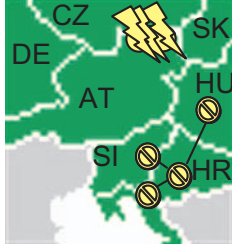
#### Sequence of events

The grid disturbance on Wednesday, 27 August 2003, started with an automatic shut down of a NPP in Slovenia. The outage was immediately followed by an overcurrent trip of a 400 kV circuit between Hungary and Croatia (due to a welded contact of the line protection device). Subsequent system overloading led to the automatic tripping of 3 lines between Austria and Czech Republic. Only the fact that the loading fell rapidly enough below 115% of its nominal value (see table A.1.6) could prevent from the impending tripping of all lines between Austria and Hungary and a potential system collapse, what would have become reality after only 2 seconds. However, a large number of transmission lines in the eastern part of the UCTE system (comprising Germany, Austria, Czech Republic, Slovakia, Hungary, Slovenia and Croatia) became overloaded leading to precarious situations. Furthermore, some cross-border flows in this area changed their direction. The normal operational conditions could be restored within a time span of about 2 hours without any loss of load.

Table A.1.6. Sequence of events in the course of the Austrian near miss (Verbund-APG, 2004)

Stage	Time	Location	Events
Preconditions	Aug. 27, 2003 before 09:15		<ul style="list-style-type: none"> <li>• Stable operating conditions complying with the predetermined grid security constraints (N-1 criterion).</li> <li>• High cross-border power flows from northeast to southwest (HU-HR-SI-IT; AT-SI-IT).</li> <li>• Single busbar operation at the Tumbri substation in Croatia due to scheduled maintenance.</li> </ul>
Outage NPP Krsko and line trippings	09:15:10.001		<ul style="list-style-type: none"> <li>• The Krsko nuclear power plant in Slovenia is automatically switched off due to an improper setting of a switch on a steam valve during testing procedures.</li> <li>• As a consequence, the load flow on the 400 kV line Hévíz – Tumbri increases.</li> </ul>



	09:15:10.438		<ul style="list-style-type: none"> <li>• Due to overcurrent and a welded contact an automatic protection device disconnects the single busbar at the Tumbri substation; the 400 kV lines Héviz – Tumbri, Tumbri - Krsko 1+2 and Tumbri-Melina are lost.</li> <li>• The load flow in Southern Austria increases (coming in from Hungary); the thermal limits are exceeded.</li> </ul>
Automatic protection device in Austria	9:19		<ul style="list-style-type: none"> <li>• To prevent thermal destruction an automatic protection device in Austria is triggered and disconnects three lines between Austria and Czech Republic.</li> <li>• The current falls again below 115% of the thermal limits and the automatic tripping sequence stops; <b>otherwise all the lines to Hungary would have been tripped within the next 2 seconds and cascading outages and blackout situations in AT and SI could have occurred.</b></li> </ul>
Severe disturbances in the neighboring systems	9:19		<ul style="list-style-type: none"> <li>• Redirection of power flows (AT-SI-HR and IT-SI-HR).</li> <li>• Cross-border flows CZ-DE and SK-HU heavily increase leading to line overloads in these areas (not N-1 secure anymore).</li> <li>• Reactive power flow from HR and SI towards AT increases leading to a large voltage drop.</li> </ul>
	9:20		<ul style="list-style-type: none"> <li>• Minimum voltage level reached in Southern Austria and Slovenia.</li> <li>• Additional active and reactive power deliveries from almost all available power plants in the region manage to stabilize the system.</li> </ul>
Restoration	11:21		<ul style="list-style-type: none"> <li>• Line Héviz-Tumbri closed.</li> <li>• Loading conditions between SK and HU is even worse and the north-south interconnection is seriously endangered.</li> </ul>
	11:49		<ul style="list-style-type: none"> <li>• All the tripped lines between AT and CZ re-closed.</li> </ul>

## Identified root causes and derived recommendations as identified by the investigations

The Austrian TSO **Verbund-APG** initiated an investigation of the

*“The real transit flows usually differ by hundreds of megawatts from the schedule, heavily loading the transmission network, which keep permanently the risk of disturbance on a raised level.”*  
(Verbund-APG, 2004)

event in collaboration with the affected TSOs in Croatia (HEP), Czech Republic (CEPS), Germany (E.ON Netz), Hungary (MAVIR), Slovakia (SEPS) and Slovenia (ELES). The resulting report (Verbund-APG, 2004) classifies the faulty test procedures at the NPP Krsko, the single busbar operation and

the welded contact of the line protection at the Tumbri substation as occasional. It stresses rather the adverse effects of the permanently high cross-border flows from north to south on the evolvement of the disturbance (see table A.1.6). According to the report this power flow often deviates significantly from the schedule. Furthermore, the investigation finds fault with the insufficient real-time system monitoring and data exchange capabilities of the involved TSOs.

In order to prevent the reoccurrence of a similar event the limitation of the cross-border flows in the affected region is recommended. As further actions the upgrading of the 380 kV north-south connection within Austria, a better coordination among the TSOs regarding switching operations with wide-area influences and the improvement of real-time system monitoring and data exchange are suggested.

### Lessons learned from the incident in Austria

1. The near blackout in Austria and the surrounding countries shows the strong interdependencies among the TSOs in the eastern part of the UCTE grid. Therefore, a close cooperation, pre-defined joint emergency procedures and an adequate information exchange during contingencies are crucial to assure operational security.
2. Unscheduled high burdens on transmission lines due to cross-border trading lead to a higher risk of wide-spreading disturbances.
3. Uncoordinated automatic line tripping for protection does not solve the problem of the overall system security but shifts the overload towards other elements of the network.

4. The public attitude against the building of new overhead transmission lines is a decisive factor delaying the reinforcement of the network which, in turn, has negative impacts on the operational security of the electric power system.

### A.1.4 Lessons Learned

Every single event followed its own pattern and happened due to a dynamic and complex interplay of multiple faults and contributing factors. Despite this uniqueness the studied incidents reveal a number of underlying common patterns and expose different technical, operational, institutional and legal deficiencies of today's European electric power system:

- The recent and still ongoing **liberalization process** within the European electricity market as well as the subsequent increase of international trading significantly changed the using patterns of the European electric power infrastructure, while the physical system and the organizational, institutional and legal framework were not sufficiently adapted to the new requirements.<sup>19</sup> The European TSOs, historically serving their national load, still have only limited real time system monitoring, data acquisition and communication capabilities beyond their control area. They also lack of adequate coordination and mandatory joint emergency procedures and can exert only little influence on the physical (parallel) transit flows as resulting from international trades, while being confronted more and more by unanticipated and uncontrolled high workload on the cross-border lines.

The Italian blackout and the Austrian near miss are both serious warning signals for the resulting risk of supranational, wide-spreading cascading grid failures, whereas already a minor single event may snowball into massive problems. The two events also question the adequacy of the N-1 security policy as determined by the UCTE Operation Handbook. The application of the N-1 rule seems to be inadequate in particular with respect to interferences between

<sup>19</sup> See Chapter 3 for more details.

different control areas, with respect to its real time monitoring, and with respect to the lack of a well defined allowable time delay to return the system to N-1 secure state after a contingency.

Insufficient regional short- and long-term reserve generation capacities is another crucial factor identified by the studies which can - at least partially - be attributed to market induced changes in the operational regime.

- Other **causal factors** associated with the incidents studied here include technical equipment failures and their coincidence in time the power systems simply are not designed to cope with, deficiencies related to defence plans (load shedding) and exceptional climatic conditions endangering the regional generation adequacy. Furthermore, protection systems are found to play a key role in a majority of catastrophic failures. Uncoordinated disconnection of transmission lines in order to avoid overloading of parts of the system shifts the overload towards other network elements and may cause cascading outages.

In the course of an incident aggravating factors are also human-related including a general lack of awareness of potentially far-reaching failures and short-term emergency preparedness, rather than purely technical.

All these factors seem to relativize the vulnerabilities induced by the liberalization and internationalization of the European electric power system. However, the long-term influence of these institutional and operational changes on the frequency and dimension of power outages remains to be seen in the coming years.

- None of the discussed blackouts or near misses was caused by a disturbance in the **Information and Communication Systems (ICS)** used in the electric power infrastructure. However, in the near future the growing dependencies are expected to result in an increased vulnerability of the ECEI to failures in the ICS (see Chapter 4 for more details). On the other way round, the study reveals that large-scale and long-lasting power failures can lead to a breakdown of the electricity dependent ICS which, in turn, has negative consequences for the restoration process.
- The **impacts** on our societies and on other electricity dependent infrastructures are significant. In 2003 more than 60 Million people have been directly affected by long-lasting power outages in Europe.

Being the most severe one, the Italian blackout affected 57 million people and restoration took up to 18 hours. Although there is no comprehensive study about the economic costs of this incident, losses of more than 100 million Euros mainly due to spoiled foodstuff and interruption of continuously working industries are reported.<sup>20</sup> In all the studied incidents the affected population did not panic and no severe accidents are reported.

<sup>20</sup> For comparison, the total costs of the power outage in the USA and Canada on August 14, 2003, are estimated at around 6 billion US Dollars (see Appendix 9).

## Appendix 2

# Critical Electricity Infrastructure: Current Experience in Europe

*Adrian Gheorghe, Dan Vamanu*

### A.2.1 Introduction

The results reported in this Appendix are based

- (i) on a selective and critical literature search; and
- (ii) on interviews with policy makers and managers in the electricity industry in several European countries.

Persons invited to take part in interviews agreed to review the minutes of the discussions. The texts as captured and edited reflect entirely the personal views of the persons consenting to be interviewed. The task of the authors was only to conduct the interviews on a similar list of issues with various experts in Europe, and later integrate the findings on record within the framework of this book - the critical electricity infrastructures<sup>1</sup> and risk governance currently experiencing the effects of liberalization, deregulation, privatization, internationalization and the ubiquity of digital systems.

*A caveat* is, therefore, in order: being an edited and summarized version of field records of testimonies of informed experts, opinion leaders and other stakeholders in the screened countries, the texts in the sequel may send various signals in a straightforward language. Acting, in this case, as *ad-hoc* ‘investigative reporters’, this section’s authors understand to keep themselves within a safe distance from such accents, while, however trying

<sup>1</sup> A number of *phone-conference meetings* took place, bringing together various stakeholders across Europe, by way of a common questionnaire, and framework discussions. This has led to the identification of current trends, and distinctive solutions adopted in various countries, relating to electricity market liberalization and deregulation in Europe, from the Iberian peninsula to the Balkans.

to faithfully carry the respective messages through. The true point is that the reader should not expect to find, under the title invoking a country or another, the official stand of the respective government, or even local ‘energy rulers’, but rather an informed opinion from a representative, if not necessarily dominant, local ‘think tank’<sup>2</sup>.

While the strength of this section is believed to stay with the variety of perspectives it endeavors to offer, one outstanding – if perhaps intricately emerging - conclusion of this, *sui generis*, pan-European debate is, however, that *a single European electricity market*, if properly designed and subject to the availability of sufficient interconnector capability in the critical infrastructure serving it, *will* increase chances for a sustainable – that is, technically efficient, economically sound, and environmentally forgiving – electricity business beyond what can ever be achieved in national markets acting in isolation.

## **A.2.2 Electric Power Systems in Europe: Critical Issues for Critical Infrastructure**

### **A.2.2.1 Issues for Europe**

For any company dealing with electricity generation, transmission, and distribution the basic design philosophy is that, at any time, one *should avoid a blackout and keep the lines under voltage*. The continuity in the supply of electricity services *must* be ensured irrespective of extraneous circumstances. Throughout the Old Continent as well as across the Ocean, the prime command is – ‘*the Power must flow*’.

For, indeed, *power* (electric) is essentially a *flowing* commodity, and this elementary finding draws almost immediately an enlighten parallel with another ‘commodity’ of the kind – *the air-transportation mobility*. A comparative look at the issues confronting the critical electricity infrastructure, and the continental air traffic management in Europe may reveal striking similarities, sharing similar origins. And the comparison is even more dramatized when a look to a similarly-scaled, yet differently-managed system is brought to the balance: the North-American air traffic

<sup>2</sup> The European Commission and Parliament are looking to strengthen the *Electricity Liberalization Directive* to try and move from many separate markets -- each one liberalized to a different degree and with notable differences in ‘philosophy’ -- to one unified market uniformly observing a single, consistent set of rules. This has eventually appeared a huge challenge, but the prevailing belief at the political level is that - it can be done.

management system. Without further expanding here on the ubiquously known *facts* featuring the cases in point, one may seize some key root-factors feeding operational efficacy, safety, efficiency and ultimately success in the trans-Atlantic case on the one hand, and operational hiccups, a questionable safety, an efficiency that, *regionally*, leaves to be desired, and a persistent frustration in our European Home, on the other hand. And the root-factors are:

- The establishment's manner of ruling; and
- The subjects' response, based on 'cultural' backgrounds – at large.

Pushing a bit the parallel in a metaphorical manner, one may note that what America *does have* whereas Europe *does not have* – both in the air traffic and the electric power management realms, and perhaps in so many other areas - is a true '*Federal Aviation Administration*', featuring (a) an uniform technical and managerial 'philosophy', or otherwise - policy; (b) an uniform set of standards and rules; and, not the least, (c) an uniform jurisdiction.

Which, for Europe, would presuppose (i) a shared and equitable interest in decently satisfying *all* end users, from the Arctic Ice Cap to the Mediterranean, and, indeed, 'from the Atlantic to the Urals'; (ii) an authentic comprehension of the 'cultural' differences between various European societies originating in the 'burden of History' and of the bearing these may have on *any* project of Continental ambition; (iii) having all parties subject to the respective Authority freely and authentically consenting to a shared discipline, and perhaps to shared sacrifices, which would unavoidably include giving away *some* fraction of national sovereignty.

Which apparently *is* the crux of the matter<sup>3</sup>.

Tempted, as we are, to further exploit this seminal analogy, we shall however leave it aside and focus, in the sequel, on a number of telling aspects on record with the stakeholders that offered to contribute their opinions. One issue that was frequently called to attention was – how a modernized and regionally-g geared European critical electricity infrastructure should handle its relationship with the IT & C technology.

The common-sense, unquestioned rule has been that all *ancillary* technology – and the IT & C is one of these – should do its part in serving the afore-said prime command: *let power flow*. To this effect no ways and means should be spared. In particular, even if the public communication systems are out of order, or are not accessible at the time of a contingency,

<sup>3</sup> A certain bias to the assessments in this section may owe to the time of drafting: the politically-cold European summer, 2005.



when a black-out is imminent, or just happened, the use of *any* communication and technological means - from battery phones to satellite communication phones - is deemed necessary, practical and acceptable<sup>4</sup>.

The policy of liberalization of electricity markets calling for transparency as a consubstantial requisite is perfectly consistent with an intensive use of information technology and open-access ICS for commercial transactions as well as for logistics-related purposes.

As it is now, in case of contingency the system relies on human operator's knowledge and experience, in order to avoid the loss of voltage in the power lines. In fact, most experts were of the opinion that, due to the complexity of the system and to the liabilities involved, one cannot expect, in the near future, that human operators be replaced by real-time intelligent expert systems. Noted was also the fact that it is only of little consequence whether protection and control systems (e.g. frequency control) are of the same technological generation ('age') - only the functional principle must fit into the system.

The security of electricity transmission was always a top priority issue and a main rule of governance for UCTE<sup>5</sup>. The current (N-1) safety design philosophy aims at ensuring the security of supply even under the terms of a higher grid complexity and new market regulations. Attempts – coming along with market liberalization - to operate the grid at higher loads will only increase the vulnerability of the whole system. UCTE is strengthening the need for an updated *Operation Handbook*, with rules bringing various countries and technological systems to comparable levels of operational safety performance - all based on the same fundamental technical principles, and sharing best practices.

In the current UCTE risk and vulnerability governance practice:

- there is no place for direct experimentation of new types and classes of models (e.g. evolutionary computation, etc.);

<sup>4</sup> For technology-related aspects on the continuity in service, the electricity transmission grids operate in an island mode, and are designed to use their own IT and specific communication resources, without need to interact with the public domain of ICS. However, for other management and marketing functions, a full interaction with, and use of the public ICS is encouraged and secured.

<sup>5</sup> In the UCTE area of responsibility, the practice of everyday operation requires that, in the dispatching control room at least two persons on duty should invariably be present. Special control procedures assure the security of the premises and the service continuity for transportation of electricity.

- it is, however, believed that the research in the field above should be encouraged, while results should be critically and carefully analyzed.

In investigating these aspects other findings were thought consequential:

- The new political trends, adopting the view of market deregulation, and the operability of technological systems based on fundamental technical laws will require the adoption and recognition of the needs for multi-criteria design and re-engineering in the power sector.
- The security of supply and the market opening criteria could constitute only the *de minimis* conditions to re-design and operate systems.
- The advent of renewable energy in the UCTE e.g. wind, solar, will not necessarily involve more use of external digitalized security assistance systems e.g. information technology since – in most cases – there are technical reasons, and also legal provisions that such security warranties be consubstantially built into the equipments.
- It is believed that the ICS technology will not have a significant advantage in the process of risk reduction, concerning the integration of classical and renewable energy sources.
- The compatibility of classical generating units with those based on the use of renewable sources is, on the other hand, an issue of high importance in Europe.

Liberalization may be implemented in many different, but not equally effective, ways. As testified by some models of liberalization adopted in Europe, the ineffectiveness – it was argued - may sometimes originate in ineffective ruling.

The first element brought to attention was that, *while one has no true single energy market, one does have a long-established financial market.* This means that, if the liberalization rules are not balanced among the various member countries, some companies may take advantage of premiums and privileges in their home market in order to more profitably shop in other markets. In practice, if European Directives make too many compromises, liberalization may generate damage and malfunctions and jeopardize the construction of a genuine single market. *The first commitment should be to establish the conditions for a fair competition between operators in Europe.*

The target of a European single market is not easy to attain, as shown by the difficulties that liberalization processes have encountered in Europe

for many years. In Barcelona, the European Summit has reached a virtuous agreement. It became apparent that a vigorous core of intents and beliefs are now shared by UK, Italy, Spain, other countries and the European Commission itself. However, policies and realities still have a way to go before meeting each other at a true Continental scale. From this finding on, a review of the current status in different European countries is almost a must.

#### **A.2.2.2 Nordel: Vulnerability of the Nordic Power System<sup>6</sup>**

A comprehensive vulnerability analysis of the Nordic electric power system identifies barriers to reduce vulnerabilities in the Nordic context. It also identifies a number of possible indications as to the rationale for analyzing vulnerabilities. Among these:

- The margin between installed generation capacity and peak demand has decreased after deregulation.
- Electricity consumption has increased, while there has been no corresponding increase in new generation capacity.
- Energy balance in the Nordel area of authority is strongly influenced by variations in inflow to the hydro plants.
- The blackouts in the year 2003 indicated that a number of unique, coinciding technical failures that are deemed to have low probability can have significant consequences.
- The vulnerability of society to power interruptions has increased.

It is believed that, in order to decrease the vulnerability of critical electricity infrastructures in the Nordic countries, the countermeasures to be adopted should be based on the following principles:

- Market prices shall balance demand and supply; this implies that prices reflect both capacity and the energy balance;
- High prices should not constitute a sufficient reason to intervene in the market;
- It is important, for maintaining the confidence of the market players, to balance demand and supply with respect to investment in new generation capacity;
- An enhanced co-operation between the various Nordic authorities and system operators is necessary in order to ensure

<sup>6</sup> The present text is based on literature survey and compilation of sources available on the Internet

the security of supply, including critical aspects such as the planning and expansion of the grid.

In order to achieve such goals, a systematic assessment should consider the following tasks:

- Identification of unwanted or critical situations;
- Description of the causes which might lead to critical situations;
- Evaluation of the probabilities for the occurrence of the critical situations;
- Classification of consequences;
- Risk matrix estimation, as a base for risk and vulnerability evaluation;
- Identification of barriers to handle and reduce vulnerability;
- Countermeasures to handle and reduce vulnerability.

The types of consequences which should be taken into consideration, when assessing the vulnerability of a critical electricity infrastructure, are: high price, curtailment, blackout, and the relationship among these.

Several existing laws and regulations are likely to constitute barriers in the effort of decreasing vulnerability in the Nordic electric power system, in a market-observant and efficient way. In this regard, the following aspects deserve special attention:

- Regulations of the TSOs organization and management are significantly different between the four Nordic countries. This will certainly lead to investments that are suboptimal from the Nordel prospective.
- Deficient, diverging and to some extent contradictory rules with respect to curtailment and price setting during curtailment, as well the absence of some key provisions fail to give clear signals to the market players with respect to their position, should curtailment become unavoidable.
- Differences in the procurement of fast reserves lead to sub-optimal solutions from a Nordic prospective.
- Differences in the congestion management constitute a factor of market inefficiency; this could lead to an increased vulnerability by reducing export capacity; also, in special cases the probability of blackouts may increase.
- Some of the physical connections within the electric power systems between Sweden and continental Europe are owned by power producers. Although this has not placed on the record any problem so far, the situation may give the respective

producers an increased market power with, potentially, negative effects during periods of energy shortage.

*The interactions among systems of power plants* in the Nordic countries, and the electricity pricing, is believed to be largely influenced by the power structure in Denmark (mainly coal) and the power structure in Norway (mainly hydro).

### **A.2.2.3 Finland: advanced integration of digital systems for risk management and risk governance**

The critical electricity infrastructures in the Nordic countries accept a *high level of cooperation*, and adopt the same rules towards achieving an accepted *high level of security*. A number of pivotal operational agreements are implemented as instruments for running safely the overall technical system of generation – transmission - distribution of electricity. In the Nordic countries similar planning criteria were adopted since early '70s, and were revised in the '90s. The so called, (N-1) reliability criteria, has been adopted as the basic design philosophy. In the '90s a *probabilistic approach to the overall grid safety* has been considered.

- The energy landscape reality in the Nordic countries (e.g. Sweden gives up the use of nuclear power, Norway through potential water shortages has also a limited access to hydro potential, Denmark has to manage its fossil energy park under severe constraints of sustainability and emission control imposed by the Kyoto protocol), makes every country and its electricity generation system to rely more on each other's *technical and market capabilities*.
- The combined electricity generation mix of the Nordic countries (i.e. Finland, Sweden, Norway, and Denmark) is an asset providing a total advantage at the *level of integration* of the four above mentioned systems.

The Finish electricity generation and transmission grid is embedded into the grid of the Nordic power system. The electricity generation structure (33% nuclear, 33% hydro, 33% fossil) in this country allows certain flexibility, and offers advantages into the partnership provided by the integration, under reliable and secure conditions. The peak power consumption reaches the level of *ca.* 12000 MW, while the production capabilities amount to only 9000 MW. There is an *active import–export trading of electricity*, mainly with Sweden and the Russian Federation, which is only natural given the geographical positioning of Finland.

Renewables are mainly present through the use of biomass. An estimated 500 MW of wind power is scheduled to be provided by 2010.

*New nuclear capacities are bound to using the old sites.* The TSO will have to build new 400 kV lines due to the operation of the new nuclear units.

The technical, methodological and operational concepts of gradual market liberalization have been smoothly assimilated in the Nordic countries over the past 30–40 years, in a determined and professional fashion; the market liberalization began in the beginning of the 1990's. Finland was part of this process.

*In Finland and Nordic Countries, on-line access to data and information is continuously provided, in a transparent and business-oriented fashion. Traders, as is the case in Finland, should have everywhere in Europe free access to information, and they should use this information in a responsible and fair manner.*

In Finland, like in all the Nordic countries, the long history of “*working together*”, among different – viz. *all* players - TSO, legislators, regulators, and plant operators, mutually understanding each other and also trained in how to deal and blend technical–societal–market requests has lead to the creation of defendable pieces of legislation. This is part of the *success story of electricity liberalization* and market approach in the Nordic countries in general, and in Finland in particular.

The current situation of electricity market deregulation in Finland and in the Nordic countries, as a compound market, is seen as an acknowledged success. This, one contends, is due to the *early preparations at all levels*: technical, regulatory, legal, innovation – v. the advent of information technology, and not the least to the final readiness of various categories of people acting within the electricity market.

*The basic principles on the security of the electric networks* are the same across all Nordic countries. The installed power structure, in various Nordic countries is complementary, and the different parties mutually integrate themselves into an, *unique operational market structure*.

In real terms, in Finland and in the Nordic countries at large, within the electricity grid business, *the production and investment decisions are left to the market rules and the competition environment*, while the grid itself is a monopoly and is regulated.

- Moving from a “*bilateral*” to a “*multilateral*” market approach allows, in practice, smoothing out the price differences among various electricity markets.
- A socio-economic *multi-criteria decision environment* made it possible to successfully run the process of electricity market liberalization.

- The objective operability conditions, on the one hand, and the need to provide reliable electricity services to a large variety of customers, on the other hand, made the technical system to be operational within a rather *flexible electricity market structure*.
- *Congestion management* is covered by a market-splitting strategy (or counter-trade strategy), where trading business activities are correlated with the technical and economic abilities built into the system.

*Pricing, policy and practice* are of high relevance in *prioritizing decisions* on the electricity system operation. The high stakes set to power quality and its associated indicators are part of the management process and the corresponding goals (e.g. prices, number of outages, potential harms due to power unavailability):

- There are, so called, *price areas* for electricity across all the Nordic countries. Prices in these areas differ if there are congestion situations.
- *The tariffs are different*, by region.
- *The implementation of the on-line pricing* is also considered, thereby allowing the fulfilment of adequacy issues in respect to electricity market liberalization.

There is a *legal and operational unbundling* within the system. The *stranded costs* issue has been mainly handled when consumption has increased and excess capacity has more intensely been utilised.

- There are, in general, *enough generation and transport capacities* in the Nordic grid in order to deliver electricity to the customers, in accordance with their preferred suppliers and also based on economic criteria. Finland takes advantage of this situation as a partner in Nordel.
- Qualitative and quantitative criteria are blended into a *multi-criteria approach* fashion in order to allow proper operation of the electricity system.

In order to make *efficient investments policies*, proper engineering-economic models were being applied over the years. Depreciation values are being taken into account, leading to the *“present value of the network”*, which, in turn, assists the investment mechanism into the electricity grid of Finland, in particular. A proper *cost-engineering analysis* is part of the instruments assisting the decision making process under uncertainty for the Nordic countries.

- An engineering/technical and economic integration framework is the basis for successfully and gradually integrating the electricity

market mechanisms in Finland and in the Nordic countries, overall. *All type of instruments* such as seminars, projects, opinion and expert elicitation methods are used (a bottom-up approach).

- The *new piece of legislation* adopted in December 2004 in Finland requires that the regulator be informed on decisions of planning future production capacities.

*Risks and vulnerabilities* of the electric system are considered fully within the overall system approach. In the context, it was found that loosing several large power plants or several high-voltage transmission substations may turn out as a problem for the stability of the entire Finnish grid.

- *The vulnerability of the power grid* to heavy snow, violent storms and other disruptive natural events requires a special assessment.
- Among the serious vulnerability issues to be addressed, deemed outstanding are:
  - a. A high *unavailability of hydro power* due to variability in capacity and water shortages. This could lead to shortages of up to 80 TWh in the Nordic market.
  - b. An *improper management* of congestion contingencies and an inadequate forecasting of power flow in the transmission networks.

There is an active work on *emergency planning and preparedness*; such work is done at the ministerial level and within NESA organization of Finland. A *high degree of awareness* is already established across the entire public–private partnership chain. The “obligation by legislation” concept together with a rational approach to the implementation of the regulatory framework is part of the adopted solution in Finland, within a comprehensive governance implementation scoping.

*Over the past two to three years, after some years of competition in liberalized markets, companies are starting to make profit also in energy sales, while a learning process related to e.g. the application of risk management instruments has been adopted, slowly yet efficiently.*

A *systematic learning process* has been pursued, in order to design and further develop management information systems to be used in the process of electricity market liberalization.

- *Providing correct / adequate / timely information* to all partners involved in the market operation does not create in Finland and in the Nordic countries any adverse competition problem.



*The overall objective is to keep the security of the network at the already established level (not to allow a deterioration of the situation from the level already accepted).*

- Blackouts in the Nordic countries have had mainly technical causes as initiating events.
- With respect to digital systems, the SCADA in Finland has to be totally separated from the open access system. There is still an open discussion whether the digital systems employed in the electricity sector at all levels should be treated separately, or otherwise integrated to some degree into the public systems.
- As a rule, the SCADA systems associated with the hydro power plants are of an elder generation, and have not yet been updated. It is evident that in the next 5 – 10 years something has to be done in order to bring the technology to the state of the art, which would essentially mean - digitalization.

According to the analysts consulted, there is a need for further prioritization of issues and tasks, in view of keeping under acceptable control all the driving forces of change involved, and ensure a good governance practice in the electricity markets.

#### **A.2.2.4 Sweden**

The *installed power capacity* in Sweden is *ca.* 32 GW. However, due to hydro variability the power being effectively used for electricity generation is at a much lesser level. Weather conditions and the export-import equation have a significant role in the manner the installed power in Sweden is used. The *installed capacity* in the Swedish power grid is comprised of *ca.* 50% hydro power and 50% nuclear power and combined heat and power (CHP) generation systems. Wind power has a marginal contribution. As indicated, the hydro potential is variable, this having an influence on the electricity balance sheet of the country.

Due to local conditions in Sweden in the year 2004, the amount of *electricity of nuclear origin* has reached the highest level ever, in this country. Because of the very structure of the electricity generation, and the hydro variability, the price is highly dependent on the characteristics of these two systems. Details on the *energy market in Sweden* can be found at [www.stem.se](http://www.stem.se).

In view of securing the operation of the Swedish electric power system, specialized *plans for emergency preparedness* do exist since several years. In order to extend new practical solutions for increasing the security of the

grid, the island solution for the transmission and distribution of electricity has been experimented and implemented when possible.

It is contended that the *deregulation process* made the communication among the various actors in the electricity system more difficult; allegedly, there are situations when the people running the grid do not communicate with the traders.

The coordination of the *use of river hydro potential* in Sweden is important, due to the fact that rivers are rather long, and hydro power plants are distributed over the Swedish territory, which makes the remote coordination techniques consequential.

*The electricity pricing* in Sweden is mainly dictated by the water regime variation, and there are also dynamic changes between day and night. Prior to the inception of the deregulation process in Sweden, the number of hydro companies was rather high. After the deregulation of the market, many small companies have merged, mainly into three big companies, though some other small players still exist. Under the *new organizational structure*, there is no monopoly established. A *monopoly pattern was detected more in relation to the pricing*. There were many *regional monopolies* related to regional grids, which allowed, under the conditions prevailing in Sweden, a direct access to the customers (300 independent electricity community markets).

- *The customers were captive to different electricity providers* via dedicated metering systems. After the reform in November 1999, customers are able to change or choose the suppliers without the need to have access to special meter systems.

Local network operators have a special role in *supplying information* and data to the system agents (e.g. traders), on forecast for the electricity demand, etc. A *System Operator* does exist in the Swedish electricity network and owns a big part of the grid. There is a *North-South problem in the Swedish system*, indicating that the hydro power plants are mainly located in the North and the consumption of electricity takes place mainly in the South of the country

There is a well-developed *national energy transmission grid*, but also a system of strong regional grid coverage of consumer needs. The general assessment is that the electricity grid in Sweden is adequately designed and managed to meet the current needs within the system.

- Related to the problem of congestion management, in the Swedish electricity grid there are four different transmission segments – the so-called “*cuts*” that become relevant where the system is becoming congestion-prone. The area is constantly surveyed by the TSO by computing the capacity to

be transported through these cuts transmission segments, and the export situation at particular instances in time.

- *The risk of congestion* is managed beginning with the planning phase approach. In real-time situations the risks of congestion is managed by *counter-trade actions*; this is done by balancing generation, transmission and distribution, which is, essentially, a market-based method.
- The country stands in the middle of the Scandinavian Peninsula, and this favours actions in relation to the *management of congestion*. The management of the congestion in electricity transmission is done by implementing a number of actions such as the adequate calculation of the electricity flow accepted by the network.
  - If congestion however occurs, the price is changing till the electricity flow becomes adequate.
- A process of *implicit auction* is involved in the management of risks in the Swedish electricity power system.

The Swedish electric power system represents one distinct area, *where always the same price is applicable*.

TSO is watching real-time-fashion the operation flows between Sweden and Norway. Counter-trade actions are performed by a “*re-dispatching*” activity, where the optimal solution is adopted in real-time under specific conditions of operation. This leads to the application of the concept of implicit auction, which is used consistently in the case of the Swedish electricity power system.

For the long term planning of electricity generation and the associated capacity, the market does not work by itself. The *financing of long-term investments is planned* by the Council of Ministers of the Nordic Countries. The market mechanism is left to the level of the current electricity trading activities.

The so called *green certificates* are offered in order to promote renewables and to complement the existing power structure offered to the consumers. There is no system of “*base load production*” of electricity which is entitled for the green certificates. There are new games among the actors involved in the secure operation of the electricity power grid. Examples refer to the *competition* among NPPs and natural gas units, but also with several types of renewables, to be considered for the future energy mix of Sweden.

The following observations are noteworthy: farmers in Sweden *fight against the use of the natural gas technologies*; rather, they want to sell to the electricity supply market the fuel generated in the farming activities.

At present, there is a new obstacle to the *process of market liberalization and deregulation* in relation to the optimal allocation of new investment funds. The old oil-fired plants, almost decommissioned, become operational in case of cold days (periods), in order to provide additional power.

- a. This practice of ad hoc *re-commissioning* disturbs the market and gives incorrect signals to the market on the medium and long-term horizon.
- b. The *decommissioning vs. re-commissioning* practice by use of the old plants using residual oil is a peculiar aspect in the overall process of managing critical electricity infrastructures under the rules of market deregulation. However, similar practices take place in the dilemma of old plants vs. new plants.

*Co-operation of System Operators* in the Nordic countries is strong and efficient. Some authors contend that *vulnerability* in the Swedish system is dominated today mainly by natural causes such as storms, tree falling, etc. In the context, the following findings were reported:

- There is strong interdependency between the telecommunication infrastructure and the electricity distribution infrastructure. When addressing the vulnerability assessment of such type of critical infrastructures, this feature has to be duly considered.
- NPPs presence in the national electricity grid induces specific vulnerabilities and finally requires *strong security standards* to be implemented.
- HPPs are controlled remotely, via digital and IT systems, vulnerable to possible attacks. Currently the operational centre for the HPP coordination and control is located in Germany.
  - This new situation requires adequate security standards, but leaves open the vulnerability of digital systems to outside threats. In this case, one contends, the real risk related to the operation of systems of power generation is induced by the degree of embedded digital and / or IT technology.

There is a need to keep the system frequency in the correct range of acceptance. The reason is two-fold, namely:

- to keep the system in *synchrony*; and
- to satisfy the *consumers who operate today digital systems that are sensitive* to frequency deviations in the power grid.

In general, it is considered by some Swedish experts, that there is *not enough “risk thinking”*, in order to understand the possible potential impacts due to so called “*failure of imagination*”.

- At present, Sweden observes a large *cooperation among the big national companies*, in order to help for coping with the new situation of deregulation and system’s increased complexity.
- There is a need for an overview related to the *new potential systemic risks*.
- The communication process is under threat when electricity can not be delivered.

As guiding principles for proper operational concepts adopted in Sweden, one can identify *the triad risk – vulnerability – security*.

When it comes to interdependencies and continuity in operation for *other vital systems* (e.g. hospitals) due to electricity shortages (blackouts) by use of back-up systems, this involves, in turn, the possible reorganization of hospital activities or the relocation of various services in the hospital. The need for electricity emergency systems for the surgery room in a hospital has to be coordinated with the need for the availability of electricity at some specific laboratories or services in the hospital.

- There is always *a trade-off between the installation of the back-up systems vs. the technical and organizational options* for securing the network.
- Another aspect to be addressed in this case is the *availability of the back-up systems* for providing electricity.

*The resilience concept* in the design and operation of critical electricity infrastructures does play an important part in improving the security of the system.

#### **A.2.2.5 Austria: issues with respect to risk governance<sup>7</sup>**

The installed power in Austria is *ca.* 17600 MW (including pump storage), while the peak load is 9200 MW. This allows high flexibility on the generation side. There is a surplus of generation capacity in the North of the country, due to generation capacities installed on the Danube river, yet the North–South electricity transmission capacity is deficient. The recently developed additional 720 MW wind power located in the North–East of the country could lead to security related aspects, mainly due to the

<sup>7</sup> The present text is based on an *ad-hoc* interview with a high-level Austrian expert and manager working with electricity related institutions in this country, and represents entirely the opinion of this expert.

topology of the existing transmission lines and the incompleteness, in the Graz area, of the North–South 380 kV transmission lines.

The level of security to be build-in into the Austrian grid is a matter of economic assessment. A valid issue to be address is “*How secure is secure enough*” vs. “*How secure is too secure*”? Costs associated with system security are becoming a problem of optimal allocation of resources.

In Austria, *meeting the peak demand for electricity does not constitute a problem*; demand could be fulfilled under normal weather conditions, which influence the availability of the hydro capacity (both run-of river and pump storage capacities in the Austrian Alps). According to the recent security of supply forecast ([www.e-control.at](http://www.e-control.at)) no generation shortage is projected for the next 5 – 7 years.

There is, in general, *one major problem* in the Austrian transmission grid: the deficiency in the North-South transmission capacity and the consequent congestion / overload. There is an urgent need to complete the 380 kV transmission line in the Styria region. Beyond that, the 380 kV Ring needs finally to be completed in the Salzburg area. For the spreading of *distributed generation* be successful and profitable in the overall performance of the electricity market and electric power system, a robust grid for balancing supply and demand is required.

The process of *market opening and liberalization* has been completed by October 2001, when the electricity market was 100% opened. The experience and lessons learned from the previous three-and-a-half years show many positive effects in terms of reduction of grid tariffs, higher transparency in the market, alternative suppliers and possibility of choice for all consumer groups, etc.

*In Austria, grid tariffs are thought of being relatively high.* Tariffs for the cross-border trading (“inter-TSO compensation”) and congestion management methods have been implemented according to the Regulation (EC) 1228/2003 with explicit auctions introduced at all Austrian borders with congestion. The only exceptions are the Italian border, where the auction would be organized only on the Austrian 50% of capacity, and the Slovenian border - where only 50% of capacity is auctioned since the 50% of capacity belonging to Slovenia is not subject to the above mentioned Regulation, by virtue of a Derogation dated July 2003.

*Unbundling of grid (monopoly) from the market* (e.g. generation, trading, etc.) *business* is indeed a key to a successful completion of the electricity market, and in the longer run - also to an adequate security and quality of supply that would ensure the tariff-based income from the grid really being used within the grid economy, for maintenance, investments, etc.

- Since the distribution grid is not fully unbundled / split from the generation and trading activities, there is a *danger that financial resources will be used to subsidize these activities*, via the tariff-associated mechanisms.
- It remains to be seen how the implementation of the EU Directive (EC) 56 / 2003 related to *legal unbundling* will affect the actual unbundling and the problems mentioned above.

*Sufficient transparency is a key to successful market evolution.* It is generally agreed that:

- There is a need for consistent behavior with *no political interventions* if the electricity prices are temporarily, or on medium term, increasing.
- The *market forces have to be left to act*, if a sustainable liberalized electricity market has to emerge, and to be robust to internal and external sectoral changes.
- Consumers should be encouraged to react, and adapt their consumption behavior in case of *price increases*.
- The *operational data* e.g. on generators, etc. need to be made available to the grid operators.
- There is a need for *total transparency, and trusted - share* and exchange of information and data. Only in this way there are chances for success in the process of electricity market unbundling and liberalization.
- Power generation units should give information to every actor in the electricity market and finally let the *market forces play their contribution to assure safe and efficient power system operability*.

A point was made, to the effect that going only “*halfway*” into the implementation of the market liberalization could be dangerous, and counter-productive.

- The vertically integrated utilities, as opposed to the organization in a liberally-oriented market, require *a different type of management approaches*.

Some *specific problems in the Austrian electricity grid* are related to:

- *Insufficient transmission grid capability* on the North – South direction, due to delayed construction of the missing parts of the 380 kV - grid (a major drawback and, therefore, an obviously recurrent remark).
- *A rapid increase in the wind power generation* in the North of the country, requiring an additional capability to balance power

loading and aggravating the North-South transmission deficiencies.

- There is a pervading feeling that *the liberalization should be done properly*, avoiding at all costs any “panic syndrome”, when market forces may act decisively. It is also believed that unwarranted corrective interventions from outside can only invalidate the initial positive results of the market-oriented performance.
- An *opposition from local communities* in Austria against building the necessary 380 kV line in the South of the country was notified to the interviewer.

On this line, several authors made the point that, in Europe in general, and in Austria in particular, the *opposition of the population and some political segments* to building new / additional transmission lines is becoming a risk in itself, in the overall process of allowing open market forces to fully perform. Other matters of opinion and good conduct that were emphasized include the following (all assertive language – on the account of the persons consulted):

- The unique features and technical demands of the electricity production, generation, transmission and storage have to be clearly conveyed to the politicians and the public; a warning must be issued, to the effect that the basic laws of Physics can not be circumvented by “*political will*” and the “*art of conversation*”, no matter how well-intended the first, or skillful the latter.
- The lead-time needed to obtain *permission of building* new generation and transmission capacities is too long, and this is a source of risk for the overall system operability.
- *Changing frequently the course and direction* in the liberalization process can make things worse. These might bring additional risks into the overall process (e.g. risk governance type inputs).
- Within the concepts of benchmarking and incentive regulation, a component of quality and quality regulation as such deserve special attention in any European electric power system. Generation capacity and investments are the key issues to *ensuring generation adequacy*.
- For a comprehensive and integrated approach to electricity market deregulation and liberalization, while taking into account *sustainability goals*, one has to get familiar and operate with new concepts such as:
  - a. management of congested markets in view of transmission of electricity in a safe and secure



- operational grid and taking into account the legal framework (EC) 1228/2003 and the market needs;
- b. new models and framework approach to demand forecasting (living approach and use of advanced technological opportunities e.g. information systems);
  - c. security of supply responsibilities and roles, by all market participants;
  - d. unbundling the current system should not go halfway, but be completed appropriately

*A threat to the system* is the one related to the opposition of various stakeholders to new assets to be build, with special regard to transmission lines. In the context, a peculiar situation is worth noting, when a group of people does not oppose the installing of wind generator towers, but show inflexible opposition to the construction of power transmission lines.

Due to market integration into the overall operability of electric power systems, the role of intelligent, *metering systems* will increase.

- “*Metering markets*” in the electric power sector of Europe have been considered in some countries, while in the U.S.A. this approach has been abandoned in some states.

The IT technology was believed, by those interviewed, to having a dominant role in the communication process related to energy management, being conducive to more *transparency in decisions* taken by various actors in the electricity markets. The new rules, implicitly required by the application of *risk governance principles* will allow and facilitate the rapid implementation of the digital technology, and information and communication infrastructures. This however may have mixed, i.e. positive yet also potentially negative, consequences.

- The market liberalization uncertainties as these are observed from the end-user perspective, particularly in relation to the electricity prices, indicate that *customers’ adaptation to the price fluctuations* may eventually facilitate the penetration and acceptance of intelligent meters, with positive effects, from the household level up to the major industrial consumers. This would amount to an intelligent management of the demand side, assisted by expert digital systems.

A particularly interesting remark was that similar *security rules and principles*, adopted in the air traffic field and promoted by IATA, should be considered and adopted in a liberalized, unbundled electricity market in Europe, if this movement is to be a technical, managerial, and an ideological success.

In relation to *SCADA systems*, more training to system operators must be offered and made compulsory.

- Isolated initiatives to certify qualification on SCADA operations are to be encouraged and extended.

*Interaction of the power sector as a critical infrastructure* with other infrastructures is a major issue in the programs relating to energy crises management. In Austria, the Energy Emergency Act (“*Energielenkungsgesetz*”) defines the responsibilities and tasks to be performed in terms of crisis management, prevention and planning. These activities are carried out by participants from the regulatory authority, from the ministries of the Economy and Defense, and by representatives of electricity market companies (grid operators, generators, etc.).

From the Austrian perspective, the belief was expressed that a *common security policy* of electric power critical infrastructures is needed across Europe, if the overall technical and economic results of the deregulated market processes is to be successful.

- With respect to the *Eastern European countries*, a statement was made to the effect that these do not pose stability risks and the operational security is within acceptable levels of technical performance, in relation to the Austrian power network.
- It was reminded that *UCTE* is in the process of recommending / implementing rules on operational security in the forthcoming *Operation Handbook* to be applicable in the UCTE synchronous area.

#### **A.2.2.6 Greece: looking for a risk governance strategy under local conditions**

As pointed out by the consulted experts, Greece has a series of particularities in relation to the energy sector (e.g. resources, ownership of production capacities, structure of the electricity consumption by type of consumers), and these affect in a specific manner the overall assessment process of the security level of the Greek Critical Electricity Infrastructure.

The large reserves of *low-grade lignite* in Greece will continue to be the main source for electricity generation. The use of natural gas is in relation to the high degree of reliance on the Russian pipeline (60 % Russia; 40 % Algeria). Other technical solutions foreseen to become available (Turkey and Italy pipelines) are currently considered in the energy strategy of the country. The *low price of electricity* generated by the use of lignite-fired power plants does not make yet competitive the use of natural gas-based generation units. This sends strange market signals to

the potential investors. *Lack of sufficient power generation capacity* asks for electricity imports up to 6-10%. There is still room for a growth in the electricity imports, would the capacity of the interconnected transmission system be higher.

*Renewable and cogeneration* have no substantive influence into the overall management system of the electricity generation in Greece. Their contribution does not significantly save energy, nor does it improve the load on the system at the national level. Privileged economic conditions served to these technologies, mainly owing to special offers within the European Union offer good business opportunities to the respective companies, but do not contribute, in real terms, to easing the overall problem of electricity generation and grid stability in the country. Under the climatic and resource conditions prevailing in Greece, the *photovoltaic technology* might show better promises. In this respect, however, the economic ingredients to promote the photovoltaics are lacking. Without the European or state incentives, renewables such as wind, photovoltaics, are for the moment not a profitable investment proposition to the shareholders.

The *Kyoto protocol*, signed by Greece, requires the adoption of additional solutions in order to implement, in parallel, the necessary provisions ensuring market liberalization and deregulation. And practical solutions are not obvious, yet. The Kyoto protocol strategy implementation in relation to Greece, established a 20% electricity generation from renewables by 2010, while currently only 12 % are secured, and this - including large hydro power plants. Given these, reaching the committed level within the prescribed time horizon is, indeed, a questionable goal.

There is an electricity *transmission congestion problem* in the North-South direction, since the generation of electricity takes place primarily in the North of Greece, while the main consumption area is in the South of the country. This has called for special measures in order to assure the stability of the system. *The Balkan electricity grid*, with Greece a part of it, and the special operational conditions generated also by the situation in former Yugoslavia have limited the ability of an open access to the information regarding grid's flow management.

There is no such thing as "*big consumers*" in Greece. Rather, any single consumption is limited in size. The structure of the tariff is not centred on the peak load. The companies that specialize in the production of cement or steel have their own power generation plants and cut-off switches, in order to reduce the electricity consumption from the grid and thereby save company money. They also apply relatively simple DSM strategies. They bring important economic savings to their respective

businesses, but do not help the overall economic and technical performance of the electric power system.

In contrast with other electricity markets in Europe (the Nordic Countries, Austria, Switzerland), the Greek market features *a single, vertically-integrated power generation company, holding 99% of the installed capacity*. HTSO (Hellenic TSO) is the operator of the System, but the owner of the transmission system is still the integrated company (PPC). Currently (spring, 2005) PPC is the sole owner of the 49% of HTSO. Almost all personnel of the HTSO consist of ex-PPC employees.

- All matters relating to the ongoing European process of *market deregulation and privatization* are being addressed within the major company. The single electric public company in the country is responsible for keeping the infrastructure working under reliable and safe conditions, according to a set of standards approved at national level.

*It appeared that in Greece, till now, there is no formal framework for a debate on the risks and vulnerabilities associated to critical infrastructures; a plan to the effect, has been outlined only in a draft format.*

- In the '70s the Greek decision makers and politicians have concentrated mainly on the electric sector development in the country, setting as primary concern to assure a balanced supply-demand relationship in the electricity economy. Under the dominance of this preoccupation, no comprehensive discussion on *risk*-relating issues could possible coalesce, although recently a nation-wide blackout has been experienced.
- After the *2004 Hellenic blackout*, as the occurrence came to be known, a Committee has been appointed by the Government, with the mission to look into the safe operation of the power grid, including generation and transmission.
  - a. In the summer of 2004, a brown-out took place primarily due to a system voltage collapse. A blackout would have subsequently occurred, if the voltage would not have been restored with considerable difficulty, due to the lack of power capacity within the electric power system.
- The recently established Governmental Committee is to be considered as an open discussion platform on risk related issues on *critical infrastructures*, with special focus on avoiding blackouts in the Greek electric power system. Nevertheless, the mandate given to the Committee is only centred on publishing a report expected to propose technical solutions to solve network problems

related to reactive power. A policy discussion at the national level has however taken place in order to contribute to the improvement of operability performance in the electric power system.

- The *security of the system* is becoming of a higher concern and tends to overtake in ranking other goals, such as securing system reliability or the economic efficiency, considering that these have already been put on track. Adequate rules of risk governance have to be adopted and implemented.

In the year 2001 the separation of the TSO from the independent system operators took place, as a concrete step towards electricity market liberalization. It was argued that the current policy in Greece, in relation to the electric power critical infrastructures takes, *de facto*, a short-view perspective, centred on a prompt solving of current problems, and applying *de minimis* additional regulations in order to meet the current EC requirements on privatization, deregulation, unbundling, and open access to the market of electricity generation and transmission.

- Several *anomalies* were noted, in comparison with other areas in Europe, in the way the open electricity market (liberalized), and its mechanisms are perceived and implemented in Greece:
  - a. According to the regulatory body, the expectations about the deregulation process seem to overshoot the promises of the current practice.
  - b. A *liberalized electricity market* is expected to bring new generation capacities under a different ownership than that of the existing company in Greece
  - c. An observation was ventured, that the *TSO operators and associated personnel* are former employees of the mother-, vertically-integrated company with whom they keep a close relationship, thus diminishing the potential for new chances of creative solutions, and for genuine market force interventions.
  - d. It was also argued that there is an *organizational struggle among various units and actors* currently operating in the Greek electricity market, where one cannot fully assert the value of interdependencies, and the potential of the market forces.
- The fact that *transparent information* related to the capacity flow within the Greek transmission network is not available was noted.
- The chances for *independent investors* to penetrate the market of electricity in Greece are thought to be hindered also by the

incomplete information on imports, and the limitations in the grid capability to handle additional generation, or imports.

- A need was identified, for a fair balance between the *rate of penetration of the new market rules*, on the one hand, and the new technologies required (including the full involvement of digital technology), on the other hand.

The legal provisions in Greece allow the HTSO and the DSO (which is PPC) to cut out the electricity supply to the consumers, without financial or legal consequences. For the *vital consumers* such as hospitals, one tries to keep electricity interruptions down to a feasible minimum; such consumers have already adequate sources of electricity generation for contingency situation.

There is an urgent need, it was argued, for a coherent and authoritative *risk governance* framework which would assist in the implementation of the new market rules in the Hellenic electricity sector. Such a framework should create conditions for a well-managed process of restructuring, that would bring the entire infrastructure from a vertically-integrated power system to a decentralized system, fully capable of providing electricity services at the prescribed standards of voltage, frequency, and reliability, and also compliant with the EU regulations and the rules of a safe and sane electricity market.

- The *regulatory body* in Greece holds the opinion that, currently, there are indeed considerable problems in the overall technical and economic performance of the system, mainly due to the present structure of the electricity market and to deficiencies in the overall approach of system's robustness.
- There are however opinions and corresponding pressure groups acting on the line that, under the current structure of the Greek power system, the TSO should go back to the *integrated vertical company*, as a separate body within a holding company. It was noted that, at present, neither a holding company; nor even proper separation of energy activities within PPC, have been achieved.
- Under the current situation, Greece *is* formally complying with the *de minimis* legislation requirements relating to deregulation. However, according to experts, the *modus operandi* currently prevailing does not actually work, and this situation could lead to further power system failures.
- The new laws in Greece encourage competition and *bidding for new investments* into the grid (900 MW of generation capacity that the HTSO might contract through an auction procedure).

- However, the actual business environment in Greece does not help in bringing new electricity suppliers into the electricity system.
- The *public opposition to the construction of new power lines* (the so called NIMBY – not in my backyard – principle) requires new and adequate governance solutions within the overall new framework of risk governance.
- The role of *local culture, business traditions, societal and human relationships* play a crucial role in the success strategy towards a horizontally integrated electricity market in any specific country, and in Europe as a whole. The case of Greece has to be dealt with caution.
- The concept of governance implementation, in principle, is important in the effort that Greece subscribes to the present requirements of an open electricity market. There is a *need for additional time*, and other type of resources (e.g. investments, willingness to open the markets) in order to make a successful transition to a fully market-oriented electricity economy, across Europe.
- As a contingency provision in the grid management, in order to save the system from prospects of local / national blackouts, a better arrangement should be contemplated and designed, to the effect of allowing the *selective and intelligent* shut down of consumers. Insurance and other, financial and logistic measures should accompany such a regulation, so that all parties experience minimal losses, and compensation schemes be eventually made available.
- Regulators should themselves send substantive *signals for change*, which, together with signals from the business realm, will probably trigger improvements in the current situation.

Other key issues relevant to the *vulnerabilities in the Greek electric power sector* were found to be:

- The so called *North – South problem* (generation in North and consumption in the South of Greece).
- The *air conditioning consumption* is rapidly increasing which, in turn, dramatize grid stability issues in the summer season.
- *Reactive power* (both generation and consumption) is a problem, which makes the grid vulnerable to collapse.
- The *public opposition* to the construction of additional, and badly needed, high voltage substations in the Athens area is a source of increased vulnerability and risks.

- The behaviour and *operational pattern of old coal generation units* using lignite is an increasingly significant risk factor; no consolidated opinions are available, on how this technology will behave during hot seasons, in the years to come.
- *Deficiencies in a systematic maintenance* activities or even the absence of these, over the lifetime of the power infrastructures have now become a significant source of risks and vulnerability to the overall grid.
- *Reliability related issues* of specialized generation agents into the Greek electricity grid e.g. boilers are a source of increased concern.
- The *variation in the quality of lignite* used to provide electricity, together with the aging of the current infrastructure is also a source of concern, in regard with risks and vulnerabilities.
- Many of the *old generating equipment* is stretched to the extremes of the availability figures during peak load periods; if shut down during such episodes, these could fail to restart properly.
- The *increased abuse of the current technology* without proper ingredients to implement new investments is considered as *highly risky*, and definitely induces a high vulnerability into the system.

Vulnerability due to *new threats* is not considered or taken into account into the existing operational and management environment. Current domestic reports addressing issues related to electricity generation or transmission do not highlight cases of exception, or of concern.

- The overall *degree of digitalization* of the Greek electricity grid is not particularly high. There is an expectation that the investments in this sector would increase.
- The TSO will monitor the units, without however having direct operational control on the system.
- Natural perils such as *earthquakes*, or the increased humidity in the air, might represent elements of concern for increased risks and vulnerability in the electricity grid.

The feeling of those interviewed was that the notion of profound changes in the electricity markets in Greece is, in essence, rather new, while other, more basic aspects / tasks have to be currently addressed. There is a need to *re-architecture and adopt re-engineering* tasks for the whole electricity infrastructure, including its economics, basic trading rules etc., in view of adopting, implementing and consolidating the new rules of risk governance under liberalized electricity markets all across the European space, with Greece a case in point.



As the perception in this country goes, building *new governance rules* involves, in the end, a completely new world of people, technology, business rules, sustainable education, and not the least an adequate governance culture (up to *e-governance* as an operational working platform).

#### **A.2.2.7 Italy: Towards an effective liberalization of the electricity sector<sup>8</sup>**

It was argued that the Italian case, the current unbundling of management and ownership of the Italian transmission grid revealed its limitations. Some would go as far as saying that there might be a need to re-aggregate the things. The company resulting from the re-aggregation would allegedly ensure a higher level of impartiality, security and efficiency in the operation, maintenance and development of the grid and in the management of its power flows (re-bundling). Proponents of this line of action would maintain that this activity might be run by a single company, capable of operating under a market approach, while also along the lines possibly indicated by the Government.

Beyond such speculations there is, however, a world of hard facts. After the power plant clearance regulations were brought to a standstill, the feeling is that one can not wait any longer. The risk of not being able to cover electricity demand owing to insufficient generating capacity - and thus of *facing brownouts or blackouts* - is deemed real, and the alliance of those who do not want to see Italy running such risks is widening.

It is believed that, in order to remove the obstacles that still hinder the full liberalization of the electricity industry and to enhance the security of the national power system one should revise the currently complicated procedures for the construction of power lines. This may eventually eliminate congestion in some areas of the country, which may impact the sitting of new power plants and of production settlements. The Italian Government has already taken some steps in this direction, by including power lines among the large strategic infrastructures that will follow the fast-track procedure for their implementation.

The allocation, configuration and functions of energy resources and the current energy infrastructures have a national character.

- the national electricity transmission grid, which connects the main power plants and the import lines, requires a coherent and uniform management in order to ensure the electricity supply to

<sup>8</sup> The present text is based on literature survey and compilation of numerous written sources available on the Internet.

all the regions, many of which are not self-sufficient for the coverage of their consumption; therefore, the regional management of the grid is technically impracticable.

The procedures governing the construction of power plants inside industrial sites are assessed as simpler than "green-field" endeavours. Such integrated plants, one contends, will be increasingly attractive to operators. Even if most of them are small-sized, their contribution is deemed particularly useful, as they will be distributed all over Italy and, located close to their presumable customers, will help relieve the congestion of the national transmission grid. The green certificates were introduced by Legislative Decree 79/89 with a view to promoting the use of renewable energy. These certificates represent the green power that is generated and are traded between the parties.

Authorized power plants include a non-negligible number of plants that are no longer active or are only partially active, owing to obsolescence. Taken 'as is'-fashion, these plants involve pollution problems and have prohibitively high generation costs. However, it is believed that part of them should be reactivated and retrofitted to generate cleaner and lower-cost electricity.

Energy development and environmental protection - these are the requirements that will have to be reconciled among the industrialized countries in Europe, if they want to secure the energy they need for supporting a sound economic development and meet the demands of the population, without causing an unsustainable impact on health and the environment. As seen by knowledgeable analysts, in Italy the situation might be even more difficult than in other industrialised countries. Integrating power plants into the townscape is an extremely complicated endeavour. Italy is a country with thousands of historical sites, and one of the major industrial nations in Europe and on the globe; new capacity *at competitive costs*, in order to be able to compete on international markets is needed, with due consideration to all parameters and constraints involved.

The domestic perception is that *electricity price is still very high*. Lower costs are seen as depending on many factors:

- creation of a competitive electricity supply side (i.e. consisting of producers) through the implementation of the power exchange;
- investments in new high-efficiency power plants, among which combined cycles are the most significant;
- investments in the retrofitting of existing low-efficiency plants; and, with regard to the general charges of the power system,

- reduction of the para-fiscal component of electricity tariffs and, where possible, measures concerning their fiscal component

A remark made by some analysts was that “Fortunately, the case of California cannot be transferred to Italy as such”. There are common difficulties, such as those relating to the authorizations for construction and operation of new power plants. On the one hand, in Italy one has a growing demand for connection to the grid, arising from new investment projects for a capacity of some tens of GW. On the other hand, the plants that are actually under construction are only a few. As a result, the available reserve capacity margin is being systematically eroded. The recently-passed law-decree, which simplified authorization procedures, is likely to be the most effective short-term solution for increasing supply and avoiding the risk of brownouts or blackouts. At the same time, on the demand side, it is felt that the domestic policy should be aimed at holding down national electricity requirements and enhancing efficiency in electricity end uses, which would have beneficial effects also on the environment. The diversification of the generating mix in order to avert the risks of an internationally-wide power crisis is held as a longer-term solution.

It was contended that, in a scenario of development of the national electricity-generating system, the issues should be viewed from the standpoint of both centralized and de-centralized power management. The latter form of generation is based on small plants using marginal hydro sources and isolated minor gas fields and combining heat and power production in a factory or in a small urban settlement. The Italians believe that *the liberalization experience of other countries confirms the need for developing both forms of generation.*

In Italy, the authorization for construction of large power plants falls under ministerial responsibility. The problem is to develop a reference framework for making increasingly adequate choices among the numerous plants for which the authorisation procedure has been initiated.

The siting of thermal power plants has always been a problem. These plants have a significant impact in terms of polluting emissions to the atmosphere, water consumption, space requirements and interference with land use. However, the situation has improved in comparison with the past, at least for new combined-cycle plants, natural gas-fired, and featuring a high efficiency along with a low environmental impact. The remaining problems are the large size and the unquestionable industrial imprint of a power plant, which may be an obstacle to other land uses. Usually, there are more opportunities for building power plants in sites where there are other industrial and energy settlements and where the

environment is already altered. These areas, usually close to large consumption centres, are deemed to make more suitable sites.

The established environmental impact assessment procedures (EIA) have the purpose of securing the compatibility of new plants with existing ones, thus alleviating to the extent possible additional burdens on the environment. Authorities are currently assessing the environmental impact of about 30 new plants, but many other operators expressed their intention to apply for the EIA. There is a total of over 150 plants, with a thermal capacity of over 300 MW. Some authors contend that, so far, the procedure has been very elaborate. Considering, taking into account the new situation, the recently passed law-decree has streamlined the assessment and authorisation procedures, without prejudice to the environmental impact assessment, and thus guaranteeing the citizens' entitlement to environmental health and quality.

The Kyoto Protocol may be regarded as an incentive to the Italian industrial system:

- to optimise energy generation cycles and thus curb emissions; and
- to manufacture high-energy-efficiency products (household appliances, heating systems, cars, etc.).

A case in point is electricity generation: the selection of new types of plant, such as gas-fired combined cycles, makes it possible to concurrently cut down unit investment costs and mitigate the environmental impact.

Thus, the electricity industry is playing, and will increasingly play its part in achieving greenhouse gas emission reduction targets, by introducing high-efficiency plants, deploying renewable power generation and pursuing policies of enhancement of energy efficiency in end uses.

In Italy too, the "*green certificates*" are a tool to promote the generation of electricity from renewables. Prices will be set by the market, i.e. by the demand-supply balance: the demand of those who must fulfil the obligation of injecting into the grid a proportion of renewable power equal to 2% of their generation; and the supply of independent producers who have the availability of such generation. Previously, the promotion of generation from renewables represented a component of the electricity tariffs and was thus directly charged to the end user. To ensure the functioning of this system, sanctions are deemed to be imposed on those who fail to meet their obligations. As part of a policy for further mitigating the environmental impact, the 2% renewable power obligation might progressively rise, so as to constantly balance demand and supply and to

achieve the ambitious targets of promotion of electricity generation from renewables that the European Directive 2001/77/EC has set for 2010.

### **A.2.2.8 Spain: Security Rules have to be Regulated<sup>9</sup>**

The total installed power in the Spanish grid is 65 GW (including hydropower), and the peak demand is 47-48 GW during the winter period. Most analysts' assessment is that Spain has a *good electricity mix* comprising hydro, coal, nuclear, and since 2002 - natural gas. The share of the *renewables is 20%*, which includes wind power generation and co-generation capacities. The Iberian Peninsula has a special situation related to the *limited interconnection capacities* for electricity transmission with the rest of Europe. Key aspects are:

- There are transmission interconnections between *Spain and Portugal*.
- There is *only 5% exchange peak demand* of electricity between Spain and France.

*Security* related aspects are at the core of the philosophy for running the Spanish power system, also under the new rules of market deregulation.

Since 1998, Spain has adopted the "*wholesale*" concept, and introduced the *System Operator* institution in order to manage the transition to liberalized electricity markets. Other significant aspect featuring the 1998 change was the *unbundling of the activities in the electricity sector*, with extended liberalization of the electricity generation and distribution sector. Spain created, according to the Spanish authorities, 'the first System Operator in the world'. The transmission grid and System Operator are jointly assisting the offer of reliable services to the consumers.

The *knowledge* needed to manage the transition and the operation of liberalized electricity markets in Spain developed gradually over the past seven years; according to domestic evaluations, one can say that today the endeavour is completely successful.

*There is an established and agreed mechanism in Spain, where everything related to the electricity system operation and rules on the market operability are regulated activities. All operational procedures adopt and include dedicated rules enjoying prior approval by the Government.*

<sup>9</sup> This text is based on the interviews with Spanish experts and represents entirely the opinion of these non-nominated experts.

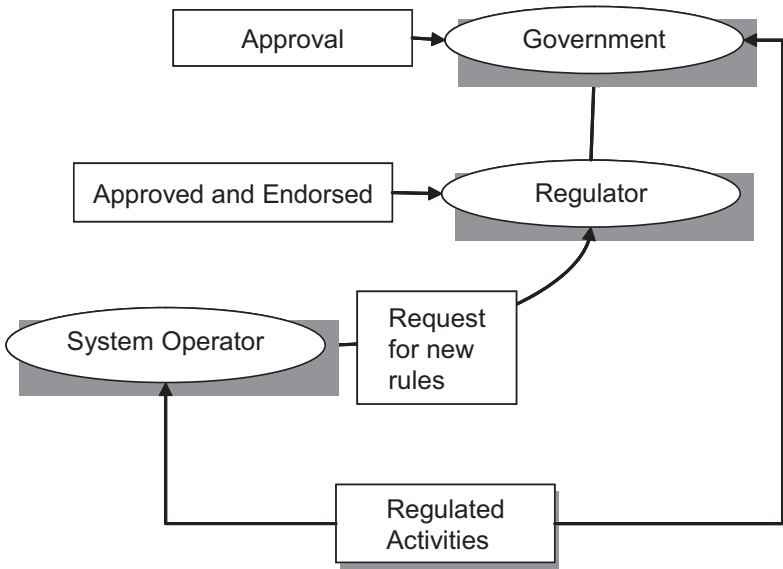


Figure A.2.1: The process of deregulation and its actors in Spain

In Figure A.2.1 one can identify the cycle of issuing regulated activities; the System Operator initiates requests for new rules to be adopted, the Regulator endorses or not the proposal, which finally goes to the government in order to be approved for further implementation in the decision making process.

In Spain, the Government has a fundamental role in the process of initiating and enforcing the observance of market rules. This allows maintaining control on the System Operator's most important activities for assuring a *high security level* of operability for the electric power system, in view of market realities.

The Spanish Government has an estimated 28% shares in the electric power industry. The System Operator together with the country's Regulatory body has *adequate knowledge and technical experience* and capabilities in order to assist the safe operation of the system. In normal operation conditions, the economic and security-related objectives are of comparable importance in the mechanism of the interaction with the electricity market.

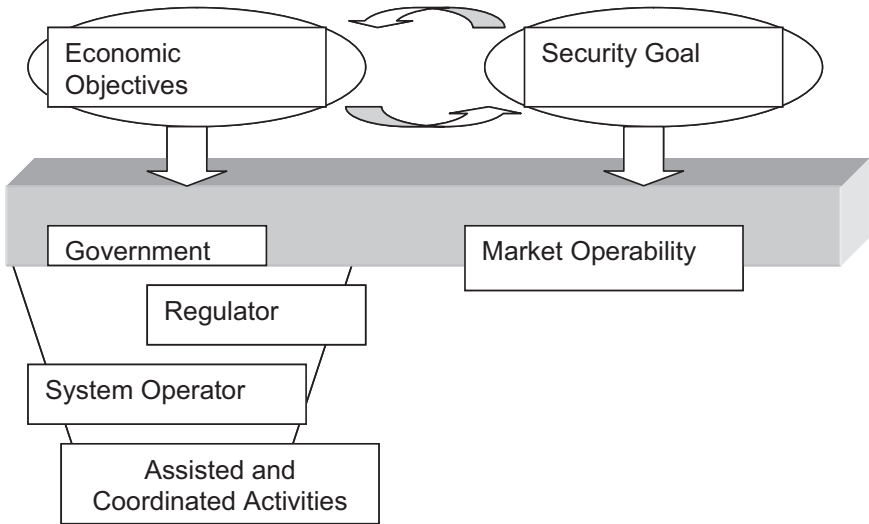


Figure A.2.2. Economic objectives and Security Goals in the Spanish Liberalization Mechanisms

In Figure A.2.2, a mechanism of prioritization of goals/objectives for the electricity market environment in Spain is presented.

After 1998, in relation to the unbundling in the electricity power a clear decision was taken, to go from, a vertically-integrated company architecture to a horizontal design with a reasonable number of generation and distribution utilities and only one transmission company which owns 98% of the transmission grid. The Spanish law gives, in principle, pseudo-administrative functions to be implemented by the System Operator. The mechanism for adapting the legislation to the new electricity markets is governed through the interaction between *System Operator and Regulator, and the Government*. New legal aspects are brought into action after sufficient information and knowledge are gathered from within the operational and regulatory environment.

Electricity consumers have permission to choose, on a commercial basis, their own electricity providers. Beginning with the year 2003, practically all consumers have the possibility to choose or change the electricity supplier. As already indicated, the relationship with the French electricity market is limited to the 5% electricity exchange capability, while with Portugal the situation is still evolving. There is an ongoing process to allow a deeper integration between the Spanish and the Portuguese electricity power systems. It has to be noted, however, that the

system in Portugal does not embrace the same market features as the one in Spain. New “actors” are now involved in Portugal in order to extend the market mechanisms for the electricity sector.

In Spain and Portugal, both the System Operator and the Regulator have plans to *increase the connection capability* between the two countries. The *access to and handling of the information* is of paramount importance in developing and implementing a proper market mechanism in the electricity critical infrastructure sector. Here are a few operational aspects:

- The information regarding the market operation is made available to all actors in the sector, providing what can be termed as *market information*.
- Information on *daily operability and bids* are made available to all the agents in the market with adequate regularity.
- Each and every agent in the market has *information on particular events* of significance, for the proper operability of the electricity market. Information is transparent and is designed to support current activities as well as medium term decisions for the electric power sector.
- Individual utilities have *daily access to information* on the production and consumption of electricity, and issues related to the System Operator activities.
- *The Government has the task to inform the public* on various aspects related to the operability of the grid, and how the legal requirements are met by all actors in the system, under the rules of market liberalization.

The liberalization of the electricity market in Spain is linked to the *regulatory legislation* for assuring a high degree of security of the electricity critical infrastructure.

- *Investment decisions in the energy sector* are correlated with the constraints following from the Kyoto protocol commitments regarding the greenhouse gas emissions, and in general with the European Commission policy on sustainable development.
- This requires a *deterministic approach* to the strategic and tactical options of electricity generation in Spain, under the rules of market liberalization and smooth penetration of renewables.

Regarding the management of the electricity transmission grid, Spain has no serious problems in relation to the *congestion aspects*. The



transmission grid architecture shows a high resilience to the inherent swings of the Spanish electricity market, and due to the low level import–export figures, and the limited interaction with the continental power grid, *there are no significant risks generated from the “foreign” grid*. Since 1985, Spain adopted market-based solutions in order to deal with congestion management in the transmission grid. This involves the adoption of technical and economic rules for a *joint co-operation of the System Operator and the mechanism of the market instruments*.

The following aspects were emphasized by the experts consulted:

- The digital systems integration into the overall operation and management of the Spanish electricity power critical infrastructures is considerable. The success of the implementation of electricity market liberalization and deregulation in the country is largely due to the systematic and consistent implementation of digital systems at *all levels of operation, management, logistics, and interaction* with the customers.
- *Ancillary services* operation and performance is assisted by ICS technology.
- Crucial aspects related to the risk of large-scale implementation of digital systems in the Spanish electricity critical infrastructures are related to the *cyber-threats*.
- All levels of management (i.e. system operator, regulators, government) in the electric power industry are fully alert about *possible risks and the vulnerability of the electric power sector* due to cyber-threats or other disruptions potentially induced by hardware and software failures of digital equipment.
- Of special concern for the regulatory body is *“what the operator can do when a digital failure occurs”*?
- A line of responsibilities in case of digital contingencies are designed and introduced at all procedural levels in the power sector.
- The System Operator is authorized to take action to secure the continuity of services in accordance to the market rules.
- *System Operator is given governmental abilities* in order to cope with emergency situations potentially generated by digital failures / threats within the system.
- As a way to reduce risks, it is accepted that *back-up systems are necessary and economically efficient*, in order to deal with unexpected, potentially disruptive events.

In addition to digital solutions for securing the operation of the electricity critical infrastructures, in Spain *the manual restoration plan* is also used and subject to drill when needed.

- *Special communication lines* are provided in case of emergency.
- Adequate *procedures and planning activities* are considered when full digital solutions are unavailable.

Cyber-threats are on the inventory list of threats which are of relevance and part of policy issues when dealing with new *emergency risks and associated vulnerabilities* in the electricity critical infrastructures.

- *Simulation runs* for assuring the system operability perform successfully.
- The *philosophy for securing the communications in the operation* of electricity critical infrastructures in Spain is: promote back-up lines, use computers and develop simulation procedures.
- In order to avoid large-scale failures within the power grid e.g. blackouts, the *interruption tariff concept* is used. This instrument proved to work well in order to facilitate keeping a secure operation of the grid. This procedure is used as a “last resort”, in situations when the power system could be prone to local or total technical failures.

The process of liberalization of the electricity markets has induced more *complexity into system operation*. New rules had to be developed, in order to achieve high security operational level; and these rules have to be regulated.

- A criterion for ranking priorities in the management of the electricity critical infrastructures through the mechanism of TSO is to *keep a high level of security of the grid* while maintaining all other functions related to the operability of the grid.
  - The liberalization of the electricity market is aiming at assisting the *provision of good services to consumers*, by assistance of the market rules and by an advanced use of digital systems at all the levels of the power system.
  - In all this process, the generation of rules of conduct and operation within the systems is associated with the System Operator and rules are finally approved by the Government bodies.

Within the mechanism of *implementing the market rules*, in the Spanish electricity sector a great deal of attention is given in parallel to the sustainable development policy in Europe. In the case of Spain this aspect is treated under the statement of “*special regime*”, which involves the use of economic instruments e.g. tariffs in order to reattribute sustainable solutions in the electricity generation.

- Political objectives on sustainable development of the Government are embedded into rules and regulations which, in turn, provide guidelines to the everyday activities within the network.
  - The Government has plans to *further promote renewable energy* and to integrate this into the market liberalization mechanism in Spain.
- Experts have assessed that there may be risks on achieving security goals, stemming from the use of renewables in the context of market liberalization, and the access to these sources by the consumers. New and adequate (advanced) models are currently implemented in order to deal with the uncertainty of supply generated by renewables.

There are a number of aspects considered to be relevant when analyzing the current situation in Spain. The following are outstanding:

- *Regulations* supervised by the appropriate government bodies have to be approved in order to promote the so-called “special regime” technologies, to finally observe the market rules (e.g. a complementary vision to let the market decide)
- There is a constant interest, and adequate practical action is taken in order to *develop planning procedures* for achieving higher political goals in the field of electricity generation, such as sustainable development. The goal is to install 13 GW power of renewable origin in the Spanish electric power system.
- Methodologies are developed and continuously updated to the evolving situation in order to fix incentives and /or premiums to achieve stable operation of the electricity power system. This involves proper and targeted actions, in order to transfer to the consumers the costs associated with the achievement of high-level political goals e.g. sustainable development. This work takes into account short, and long - term perspectives, in view of securing the stability of the power system. *Uncertainties and risks* are included in the overall strategy for power generation.

The policy of initially subsidizing the generation of electricity from renewables is based on the fact that a fair *cost-benefit balance* has to be considered. In Spain the approach is that costs should be reconsidered via tariffs paid by consumers, in connection with mainly the renewables.

- This approach allows, in theory, a fair manner to gradually integrate those special technologies into the electricity market environment in Spain.

As the electricity transmission system might become a bottleneck into the overall ongoing process of market liberalization under high level of security performance, solutions are sought by adopting adequate and timely planning processes. Thus, the *political decision* to build / extend additional transmission lines is being assisted by a corresponding planning effort.

In Spain also, one recognizes that critical electricity infrastructures are in *close interdependency* with other critical infrastructures. In case of potential accidents or technical failures, contingency plans are in place. Procedures to deal with such situations do exist, and specially-approved rules and regulations are enacted. Many economic actors and stakeholders are involved in the spectrum of actions to be taken in case of contingency.

- When dealing with *malicious threats/attacks*, these kinds of events are considered to some extent foreseeable, into the risk and vulnerability scenarios development and action prioritization.
- To *overcome uncertainty evaluation* and minimize risks due to electricity generation by renewables, a series of models were developed and are currently in use, in order to forecast the real share of renewables in the power generation within the Spanish grid.
  - Recently (2005) important advancements in the realm of forecasting the short term contribution of renewables to the grid were obtained. Four-hour forecasts have demonstrated less than 10% error.

*System Operator management* and the random contribution of the wind power to the load management is in the uncertainty range of using thermal power units.

When dealing with new type of threats, such as malicious attacks, with respect to the electricity critical infrastructures, Spain does not feature too many cases to report.

- There was recently *an attack on a transmission line* in Spain, without notable consequences to the overall grid performance. In this respect, the Spanish electricity grid

exhibits a rather high degree of resilience; this is a design characteristic, mainly due to the relatively high physical isolation of Spain from the rest of the European grid.

- *Nuclear units* enjoy a special security protection and, according to some expert opinion, there is a relatively small risk that these units are facing.
- In contrast, *the electricity transmission grid* is highly vulnerable to malicious threats and attacks. The local perception is that the options to truly alleviate this vulnerability are rather limited. However, one admits that precautionary principles should be employed in designing contingency plans in the power transmission sector and *counter-trading* in case such situations occur.

The pervasive feeling conveyed by the interviews was that *Risk Governance* should include aspects specifically targeting risk and vulnerability of critical electricity infrastructures. In this respect the following remarks are noteworthy:

- The security concept has to systematically associate the new element of *security culture*.
- Transmission and system operations should indeed be mutually integrated, while however one has to keep in mind that they are, in essence, different activities when it comes to providing electricity services.
- The physical structure of the transmission networks allow the delivery of telecommunication and electricity services, while the System Operator preserves security in the triad *production, transmission, and distribution*.

Under the new evolution and associated trends in relation to the generation of electricity one has, in principle, to observe the following:

- *Maintain the operational functions* offered by vertical integration companies, while implementing and running electricity market operations under a horizontal integration of technologies and functions, and pursue a coherent set of security objectives for a highly interconnected technical system and a diverse organizational management.
- The new functions, in the case of the Spanish electricity power system, are considered to be manageable via a strong cooperation of the System Operator and Regulators, while the regulated activities should pursue the goal of *achieving high security standards in the grid operation*.

The new risks have engulfed the formal, so called “old risks”, known as health and environmental risks (see Figure A2.3).

- There is a need for *change of paradigm in terms of risks*; from comparative risk assessment to *emerging systemic risks* and the integration of the latter within the Risk Governance concept, by taking into account the participation of various stakeholders.
- There is a need that *certain risks be internalized by the system*; companies and the society at large have distinct responsibilities in handling new risks.

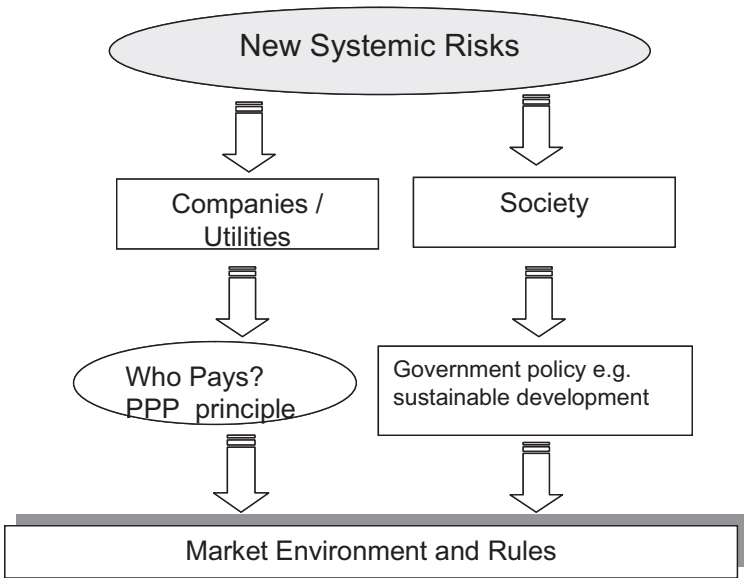


Figure A.2.3. Market environment rules, integration of public-private partnerships – the case of Spain

#### A.2.2.9 Switzerland: a transit country for the European Critical Electricity Infrastructure<sup>10</sup> exchanges

To position Switzerland within the European electricity generation, transmission and transiting landscape, one has the following key figures<sup>11</sup>:

<sup>10</sup> The content of this section is based on the conclusions of an expert meeting which took place in Switzerland, 2003

<sup>11</sup> For additional information and details, useful sources are [www.ucte.org](http://www.ucte.org), and [www.etrans.ch](http://www.etrans.ch)

- Swiss installed power, of 14000 MW, of which 3200 MW are of nuclear origin;
- Swiss electricity production (average value), of 70 TWh; and
- Domestic Swiss electricity consumption (average value), of 53.7 TWh.

*Electricity and Computer Security Issues:* The investigation has prompted the following findings:

- The design-base principle for the electricity transmission system in Switzerland is of the type (N-1), which indicates that, in order to assure continuity of services in delivering electricity, only one component is allowed to fail while the system still provides its services. However,
  - a. There are areas of operation of the electricity transmission system where the (N-2), (N-3) principles are accepted and enforced.
  - b. In Switzerland there are various layers of the grid co-ordination at tactical- (e.g. Laufenburg), or operational (e.g. Olten, etc.) levels.
- The Swiss electricity transmission technology, from basic infrastructures to computerized control elements, goes across a spectrum of over 50 years of technological developments. Some components of the grid were designed and executed with the engineering-economic background of the early 50's, while others enjoy the technological advances of the 21st century. This variety of engineering-economic design philosophies, sophisticated interactions among mechanical, electrical, computer hardware and software, fibre-optic information transmission technologies implementation etc. influences the overall safety and security performance of the Swiss electricity transmission grid.
  - The topology of the Swiss energy system (production capacities, and electricity transmission capabilities) is design to safely cover the domestic Swiss electricity consumption, while also seeking to be competitive on the European market in the flexible and efficient transfer of power from, and to neighbouring countries.
  - There are continuing technical improvements of the architecture of the Swiss electricity transmission system in order to meet the present market requests under the rules of deregulation and high competition profiles in Europe and in the UCTE region at large.

- External or internal hazards might induce vulnerabilities in the Swiss power grid, and these cannot be fully avoided. The recent case of the Swiss impact on the Italian blackout is highly mediated (see Appendix 1 for technical details). This, in turn, recommends future assessments of the Swiss electrical transmission network vulnerability and its capability to be resilient to internal or external hazards and threats (e.g. falling trees, landslides, malicious human action).

- In Switzerland, the control and management, as well as ordinary operational activities related to electricity generation, transmission and distribution are fully assisted and implemented by the ubiquity of the ICT. The Swiss example could be considered as representative for many developed countries.

- Expert judgment opinions has recommended that the Swiss electricity generation and transmission system be isolated from the ICT – public domain, allowing full use of the internal communication technology e.g. fibre-optic, “red line” capabilities etc. In the view of experts, there is a small likelihood that external hackers or other types of cyber-attack procedures could be successful from a long range distance. However, it is admitted that cyber-attacks could be effective at close range, within the transmission and transformation stations of numerous sites in the Swiss system.

- The Internet type connections between ICT and Swiss electricity industry takes place at the financial transaction and marketing levels. Related to generation and transmission of electricity, this poses small risks to the technical system.

- The reliance on human factors, of the system, both in relation with human error and malicious acts, is an issue of some increasing concern which, however, has not been fully addressed yet from a vulnerability perspective. It is deemed that the aspect of one person acting, at a given time, as a sole control operator and supervisor of the entire grid management should be further re-considered in the newly emerging context, and discussed as an additional vulnerability factor to the power supply, both during normal operation and abnormal occurrences.

- In case of total system failure / outage (see the Italian case), the emergency electricity generation and transmission systems start up, and the restoration of the demand-supply balance becomes an operational issue of the highest significance. The role of the ICT, and the relative bearing of features like its capacity, speed of reaction, and manoeuvrability under these operational conditions is yet *fuzzy* and far from the ability of providing valid and definitive guidelines. These notwithstanding, it is



believed that the Swiss electricity grid technological ‘environment’ could be considered as a good representative example for the UCTE region.

- The current feeling is that the integration of “old technologies” with “new generation” technologies, including computer-based process assistance and monitoring systems, may potentially have impacts only at the local level, in a limited domain, and without overall system safety significance.

- A fair overall comparison between the USA electrical transmission system and its management, and the European / Swiss corresponding system, would evidence fundamental differences in the security culture awareness and implementation. The American concept accepts, at all levels (engineering, management, policy) the risks and vulnerability at a higher level of system design. By contrast, the Europeans adopted a more *risk-averse attitude*. This has, in turn, specific computer system echoes and management consequences related to the overall performance.

- The standards for the electricity – computers design performance interactions in Switzerland are, by and large, those adopted within the UCTE region network.

- A list of questions expected to be addressed in the near future includes:

- (i) how one can cause operational harm to an electricity generation and transmission system, by using means of external attack; and

- (ii) to what degree the protection system and the need for a continued energy supply could co-exist on a safe, reasonable and acceptable basis, with the system stability and synchrony preservation in mind.

*Features for the Swiss case:* In relation to the digital systems for electricity critical infrastructure assistance some observations are worth noting:

- The electricity system architecture is isolated from the open-access information and communication systems. It believed by the Swiss experts and agreed among practitioners, that this very fact results in a higher security for the electricity generation and transportation, improves the reliability and availability of associated systems, and provides a higher service continuity performance.

- Evidence in the Swiss case indicates a conservative approach in dealing with the use of computers in the electric power grids, and a policy of limiting the “invasion” of the open-access information and communication systems into the Swiss energy generation and transmission domain continues to be highly regarded.

- The open-access information and communication systems and the internal information and communication technology and its associated systems are isolated, but due to market pressures they have common hardware and software components. This, in turn, could generate a high degree of vulnerability to the overall generation and transmission system.
- ICS – Critical Electricity Infrastructures nexus architecture is customized in order to ensure exclusive service continuity and the quality of services in delivering electricity to the public, industry, and business.
- According to current views of leading TSO companies in Switzerland, the open access ICS applications should be limited mainly to the financial and commercial transactions, not being allowed to penetrate the process control and system load management facilities.

#### **A.2.2.10 United Kingdom: An independent transmission as a backbone of a successful competitive market<sup>12</sup>**

The British system was characterized by one monopolist (*Central Electricity Generating Board*) and by over 600 distribution companies. Under the criteria outlined in the Government's White Paper "*Privatizing Electricity*", the system was divided into 4 trenches. In 1990, generation was divested into *National Power* (52%), *Powergen* (33%) and *Nuclear Electric* (now *British Electric*, 15%).

The electricity industry in the UK was restructured and privatized in 1990, following the privatization of other state-owned industries (e.g. telecommunications, gas)<sup>13</sup>. The shifts from public to private ownership reduced overall state ownership in industry by about 60%, and raised more than £65 billion for the government through the sale of shares in the newly privatized companies. The main challenge in restructuring the electricity sector was how to transform a vertically integrated system into a competitive system that would bring enhanced business and customer

<sup>12</sup> The present text is based on literature survey and compilation of numerous written sources available in the Internet.

<sup>13</sup> A first opening of the market took place in April 1990 for customers with over 1 MW. Since end 1998, liberalization has been applied to all customers. Another key element of the British system is the electricity pool, a power exchange based on a mandatory pool, now transformed into NETA (*New Electricity Trading Arrangements*). The oversight of the whole system is ensured by the *Office of Electricity Regulation (Offer)* and namely by the Director General of Electricity Supply (Dges), who has very ample powers: some of his decisions are immediately binding and he may submit his findings to the *Monopolies and Mergers Commission*, thus triggering a formal investigation.

benefits, but that had to be introduced in a seamless manner without any possibility of the lights going out. The UK experience has proven that the challenge can be successfully responded. One initial issue was how to structure the generation sector. Government was concerned that nuclear generation ownership would make the generating companies less attractive to market investors, so it decided to create one company to accommodate the liability. This resulted in only two generating companies being created at first, although the nuclear generators were also privatized in due course.

The ownership structure in generation has changed significantly over the years through divestments of plant by the major generators and the entry of new actors. Effective regulation and independent transmission was instrumental in this process, which today results in lower market prices. This leads onto the national grid system and infrastructure, where it was important to provide the right, long term, incentives to perform. Over the last decade, the British authorities argue that the benefits of unbundling vertically integrated utilities have been demonstrated<sup>14</sup>.

After a number of steps in the process of privatization, high-voltage transmission was transferred to national grid, a company listed on the Stock Exchange of which the Government holds the golden share. Low-voltage distribution was spun off - under monopoly-based geographic criteria - into 12 independent regional electricity companies (*RECs*), also listed on the Stock Exchange. Electricity sales, initially transferred to the *RECs*, were progressively opened up to competition.

*Pros and cons for the British privatization, about 15 years after its inception.* Deregulation brought about a profound restructuring of the industry, the revamping of the generating mix (decommissioning of 20 GW and connection to the grid of an equivalent new capacity), the cutting of personnel (from 38,000 to 19,000 members) and strong decreases in the costs of new plants and fuels, while the profits of the generating companies have more than doubled.

The electricity market in UK (specifically England & Wales) is fully liberalized due to: foreign investments, consolidation through merger and acquisition, and diversification of utilities. All these become commonplace in the privatized utilities.

<sup>14</sup> A 22% real reduction in UK electricity bills has come about between 1993-4 and 1998-9, with *National Grid* being responsible for a 41% reduction in the transmission element of the bill which now represents just 3.9% of the final total. The initial privatization concerns regarding investment have also been answered. Since 1990 *National Grid* has invested more than £5 billion on capital expenditure. Improvements include increasing capacity on main constraint lines by over 60%; this combined with technological advances have enabled a reduction in the congestion costs by 65% since 1994.

- The generation market has changed, from a highly concentrated market with a few portfolio players, to a market with many diverse generating companies. With major expansion of gas-fired capacity, *National Grid* has facilitated the connection of more than 22 GW of new generation to the system.
- Another major change has been with distribution companies; initially they were allowed to keep their monopoly over supplies to customers with demand of less than one megawatt. Today, any company holding with an electricity supply licence can sell electricity to consumers. Companies that don't own local networks can pay to use the distribution companies' networks to supply their customers.

Suppliers no longer need to own assets; this is helping produce liquidity in the electricity markets and forcing prices downward. Regulations adopted in the British system were conducive to making electricity as similar to other commodity markets as possible, including the issue of bilateral contracts, firm commitments and self-dispatching of generation. It effectively removed the ability of generators to rely on the pool mechanisms for revenues, with plant margins now driven solely by market forces. *National Grid*, as a transmission operator, played a key role in developing the governance, market rules and system design for the new market liberalized environment. Private ownership in relation to the national grid, has given clarity of purpose, which in turn has led to a strong management focus on running reliably and efficiently the transmission networks. Engineering excellence, innovation and use of technology all have contributed to benefits for customers through lower prices and increased reliability<sup>15</sup>.

The creation of incentive-based regulation has resulted in new standards for congestion management and cost-efficiency. Private ownership allowed making long-term decisions without fear of government policy changes or funding limitations interfering with those long-range plans. The shareholders have benefited<sup>16</sup>.

<sup>15</sup> For example, rapid development and deployment of new types of conductor has vastly increased circuit capacities, and better asset management systems allowed targeting investment in the right place.

<sup>16</sup> In the past few years, *National Grid* has begun to transfer its UK experience to new markets including the U.S., which now accounts for more than half of the operating profit. *National Grid* is widely considered one of the most successful companies to emerge from UK privatization. That experience is being used to support the deregulation of other transmission markets (i.e. Europe and the U.S.)

Making the transmission operator subject to the disciplines of the equity and debt markets, management is encouraged to make the right financial and operational decisions. It is essential to ensuring there is a robust business case for every major development, or investment decision. In reference to dispatching decisions on the balancing market, the public status of the company is not an issue. The Stock Market though does act as a method for companies to raise capital for new build projects and acquisitions. This could be seen as a driver to help new generation capacity and the possible creation of new players in the generation and supply markets, with an effect on the system final price. If one company is not performing, the market mechanism allows other, more efficient and innovative, companies to offer to do a better job.

It is argued that an electricity market, with competition in electricity production and supply is likely to be the most economic, efficient and robust framework for satisfying electricity demands and providing good services to the consumers. The decentralized decision making on capital investments and risk management can stimulate innovation and provide a diversity and transparency of approach which is often lacking in centrally planned systems. According to experts in UK, there is gathering experience that, over time, markets can reduce costs while improving service levels and security of supply.

### **A.2.3 Integrated Views: Risks for Critical Electricity Infrastructures**

As already indicated in the main body of this book, critical infrastructures are *large scale-dynamic systems*, potentially showing *non-linear behaviour* and, thereby, being prone to multiple threats and posing risks themselves. As *meta-systems*, critical infrastructures are characterized by a high degree of connectivity, complexity and relevance to society. Critical electricity infrastructures have recently been given a high priority, with specific aspects relating to systemic risks induced by e.g. the *ubiquity of digitalization*. An *Ad hoc Meeting* addressed, and agreed on a number of challenging issues<sup>17</sup>. It was thought appropriate to summarize, in the sequel, several findings of relevance to the issues analyzed in this work.

<sup>17</sup> IRGC Challenge Meeting, Switzerland, 2003

### A.2.3.1 General Awareness

Critical infrastructures are subject to a new kind of risks. Also, they are essentially vulnerable, and expose nations to serious security hazards at both the individual and societal level. *Awareness* on the new safety aspects related to the operability of critical infrastructures has still to be enhanced at various levels within the society and in the business realm, although the first steps to this effect have already been taken and specific solutions were made available.

An outstanding issue is *the evolving role of computer power* in relation with the security of critical infrastructures in general, and the electric power system in particular. One of the most striking developments was thought to relate to the fact that the ‘computer’, in a symbolic sense, has lost its originally central position in the critical infrastructure safety management: the ‘computability’ feature is actually on the course to being dispersed, and dissolving into ubiquity.

One view contends that the evolution of digitalization, including its patterns of distribution in time and space, is today comparable with the evolution of living systems. Co-operative and competition behaviours are indeed identifiable, as well as conservatism, resistance, and (counter) adaptive insularization. Beyond these, however, the *ubiquity of digitalization* in respect to all critical electricity infrastructures is to be considered as a new and revolutionary paradigm, in general, in spite of questionable exceptions coming from highly sensitive sectors (NPPs, TSO, other critical infrastructures, such as hospitals) where caution was always a traditional rule, and a consolidated discipline.

The current state of urgency related to the assessment of risks and vulnerabilities of a large variety of critical infrastructures leads to the conclusion that one cannot wait for a “new science” to fully address issues of critical infrastructure security. It is argued that *employing existing tools in advanced modes* may better assist in searching for new and innovative approaches to the new intellectual and practical challenges posed by the vulnerability of critical infrastructures.

Whether or not such a conservative attitude would eventually spring up a ‘new science’ is debatable, though arguably immaterial, and perhaps only a matter of language convenience. What in fact *is* required, are determined and intellectually-bold *approaches to address the issues beyond the rhetorical level*, so that the new phenomenology involved be captured in *models* showing sufficient explanatory and predictive power to persuade, and assist, stakeholders. Such a ‘new science’ could indeed help in handling the dynamic developments in technology and the corresponding changes within the society.

Other findings are:

- The nature of the interdependence among critical infrastructures does qualify them as *open and unbounded systems*; methods are needed to properly describe these.
- *The security culture for critical infrastructure* design, operation, and management is emerging as a topic which has to be professionally handled. Entities such as the *International Risk Governance Council (IRGC)*<sup>18</sup> could be instrumental in issuing appropriate recommendations in view of triggering actions at various levels of governance, concerning the multitude of aspects to be considered in defining a framework for the security culture of critical infrastructures.
- At some point in the evolution of infrastructure relationship, there is a *tendency of embedding one system into another* (e.g. computers are integrated into the production, transportation, and distribution of electricity, while electricity is running computers and communication systems). Such developments may dramatically change the terms of the debate, and the overall name of the game.
- Critical infrastructure security has to be approached from a variety of angles of comparable relevance. *Technical, business, and political issues* have to be jointly considered in assisting the decision making process towards increasing security.
- There is no real ‘owner’, or ‘supreme controller’, of critical infrastructures, or of their interdependencies. A smooth, ‘as per design’ functioning of an infrastructure can never be taken for granted on the account of a ‘good management’ only, because, as systems of a high degree of complexity, highly interactive with other systems, and essentially open, critical infrastructure do not only ‘function’: they *behave*. The connotation is to a certain degree of *apparent autonomy* resulting from never-completely-accounted-for influences, in conjunction with the propensity for non-linear responses that such systems evidence.

### ***A Novel, Systematic Approach***

Whether or not a ‘new science’ of the *system of systems* will eventually be called to deal with the interdependencies between critical infrastructures, new approaches to grasping the behaviour of these and keep their security under sound control are certainly in order. This will

<sup>18</sup> see [www.irgc.org](http://www.irgc.org)

undoubtedly have consequences on the ways one understands models, and decides on, the security, risk and vulnerability of individual critical infrastructure technologies and combinations of these. Critical infrastructures absorb technologies of a large variety, of different ages, with distinct life cycles and life expectations (from a decade to almost a century), all caught into an intricate interplay of *dynamic interactions and interdependencies*. Currently a consensus is emerging, that concepts like *interdependency and interconnection* are not equivalent when dealing with security aspects of critical infrastructures.

- *Interconnection* implies mutual influences among distinct components, up to the system level.
- *Interdependency* affects services provided by distinct infrastructures e.g. banking, hospitals, in their performance, quality, coverage, and indicates the built-in resilience of various distinct systems up to their interface interactions.

It is perhaps important to keep in mind that *different critical infrastructures were not initially designed for the present-day imperatives of the market environment and behaviour, including, and especially, the liberalization and deregulation requirements*. The lead-time issue - to see infrastructures adapting themselves to the new realities is with us all, to one degree or another. Some technological infusions may be more helpful in the process than others, with the IT a case in point. IT systems, through their tendency of being organically assimilated into e.g. electricity and transportation systems, and carrying the fascination of fast and automatic response were, for a long time, *a priori* considered to be of meaningful assistance to *all* new societal changes, and invariably conducive to *maximum security and minimal costs*. However, as time and again argued throughout this book, this *cliché* is far from enjoying an uniform acceptance, and the reactive trend towards a more careful examination of the additional vulnerabilities the IT might induce is gaining momentum.

- New concerns are in sight, and call for response. For instance, the insurance industry, as a virtual – if indirect - controller of critical infrastructures and technological developments is at unrest about the occurrence of “surprises” that may entail large losses, sometimes generated by the *incubating time of undesired events* - that could have been originated some time-back (even down to several years), and emerge suddenly, apparently without warning.
- The pressure to strengthen the security of critical infrastructures may occasionally entail proportional pressures on *people privacy*



and some argue that this could stain the democratic fabric of our society at large.

- In spite of the overwhelming complexity of the technical aspects of infrastructure security, *the human factor* plays a decisive part. It goes from the proper information management and decision making, down to a renewed dimension of risk/vulnerability aversion behaviour that may get heavy of political connotations. In a purely technical sense, it is proved by the Italian and American black-out examples that *misinterpretation and wrong/inadequate decisions* by system operators are prominent aggravating factors sizing the losses in case of crises.
- According to the findings on record, in the ongoing debate on ‘*how much digitalization is enough digitalization*’ the recent blackouts seem to evidence [- as argued in Appendix 1] that the current levels and *modi operandi* of the integrated digitalization may well be still insufficient for properly facing sophisticated crises, where unpredictability is the rule, rather than the exception.

### A.2.3.2 Lessons for Critical Infrastructures Interaction<sup>19</sup>

Lately, an observation is often made to the effect that “*common mode technology*” leads to “*common mode failure*”. This complicates the task of ‘designing for security’ the critical infrastructures. In the case of systems embedding state-of-the-art technology, experts have stated that the ubiquity of digitalization should be managed by pursuing the concept of “common mode failure”, adequately linked to the overall risk and vulnerability assessment of critical infrastructures – which, while understandable, may prove to be easier said than done.

In a more general sense, an honest appraisal of the abundance of expert opinions formulated on how best one should approach the need for more security in critical infrastructures cannot escape the feeling that one is still in a phase of epistemological inquiry, where the ‘good to haves’ prevail over the ‘must haves’, simply because no consensus can decently be expected, on the ‘must haves’, at this point in time. Here are some more ‘guidelines’ of this nature:

- The ubiquity of digitalization and its influence on vital systems gives new dimensions to how treat, individually or collectively,

<sup>19</sup> This summarizes discussions which took place at the IRGC Challenge Meeting, Switzerland, 2003

events such as *sabotage, human negligence, or the lack of security culture.*

- There is a need for a *balanced approach* between market intervention and risk governance management, and the more for *innovative manners to reconcile the imperatives and 'styles' of action* of those. An indiscriminate use of the traditional methods of both market *and* governance can only emphasize the inherent antagonisms present, and result in chaotic developments that may jeopardize what was gained so far with the 'new order' in the electric power infrastructures. If it ever comes to that, the nations that are less advanced in the matter will make the first victims.
- *Early warnings* coming from experienced experts in the assessment of critical infrastructures show that the respective systems were long downgraded, by a patent disregard of precisely their 'critical infrastructure' dimension, and a brutal reduction to 'wheels, coils and wires'. Pools of opinion have considered this a graphical expression of an obsolete – if still authoritarian - pattern of the interface between science and practice of risk / vulnerability / security analysis on one hand, and the decision making process and, ultimately, the governance, on the other hand. This may be another way of saying that, while the (proudly autonomous) critical infrastructures had so far 'the nerve' of ignoring the need for an informed and good governance, a good and informed governance may still not be always there for them, either...
- *Precautionary principles* have to be more strongly emphasized, and ultimately enforced, as both operational imperatives and key ingredients of a security culture.
- *Information and knowledge assets* within corporations have to be properly evaluated in order to further induce new mechanisms for risk management and decision making. In respect with the ubiquity of digitalization vs. the influence on other vital systems, it may be interesting to note that the corporate management of infrastructural systems (e.g. energy, ICS) seems more inhibited by changes in the regulatory framework and associated market influences, than by prospects of aggressive technological change.
- *Testing* in practice the safe operability of critical infrastructures may, at present, be a too far-fetched ambition. However, one has to extensively and confidently engage in the intellectual game of *modelling and simulation*, seen as valid, and decent, substitutes for

‘playing God’. One submits that this is *not* a pathetic state of mind: for indeed, when it comes to securing lifelines, *foreseeing* – one way or another - is a must. And the least one can do is – keep trying!

- Unlike the air traffic, and even the power traffic, the *information* flow has no easily discernible direction. It is an almost self-sufficient universe, where every output almost invariably generates a new input, and this – at near-light-speed. This remark should be carefully considered in designing for an on-line operability of critical infrastructures, because it is key to future vulnerabilities, many of which yet un-comprehended.
- There is a need for an updated and ‘liberated’ vision of using *multidimensional indicators* for modelling and monitoring the dynamical behaviour of critical infrastructures. If a ‘new science’ is not necessarily in order, a *new thinking* is.
- *Complexity* turned out to be a mixed blessing. Without it, life would now be unbearably dull and uncomfortable. With it, one is ‘living dangerously’. Insurance companies had the experience that corporate managements have difficulties to foresee potential hazards associated with critical infrastructures. In their turn, governments got in the habit to display an astounding leaning towards instinctual reactions and inconsistent behaviour on the world arena, which *may be* picturesque, but *is* definitely risky. *Governance training in the rigors of informed security building of sophisticated critical infrastructures, on one hand, and corporate training on sound governance principles going beyond the vested interests, on the other hand* are issues that have to be fully considered by both parties - governments *and* private corporations, that should form renewed alliances in order to fully assess the merits and risks generated by the new processes and problems at hand.

And, on a more technical chord:

- *Epidemic models* inspired by biological systems might have a methodological impact and could be of practical use for the ongoing modelling efforts of the evolution of ICS and their interactions with other vital systems for achieving “safe” living behaviours.
- *Insularization* of some vital, sensitive systems e.g. NPP’s, is believed to be a feasible strategy, in principle. In fact, the close-system philosophy (e.g. the “oyster” design concept) for ICS-vital systems is increasingly catching ground in relation to some

vital technologies, such as the nuclear, while for others (e.g. communication systems) this design concept has been fully abandoned.

- *The externalization of security* for critical infrastructures is another concept that is recently vehiculated, especially in relation with the risk-benefit analysis of the matter. On the other hand, an **‘internalization of externalities’** (similar to the approach on environmental and technological risks due to pollution or accidents) may test society’s willingness to pay for a higher security performance of critical infrastructures (see e.g. the “*cash and carry security*” concept).
- Methodologies that have proved effective in the security assessment, as well as current, proven practices should be transferred and incorporated into sets of rules and guidelines for managing the technology and market competition in a liberalized economic environment, whereby *security gets an economic value* for trading intangibles.
- ‘Storage’ vs. ‘just-in-time’ concepts have to be integrated into a secure/safety design of the ICS and other vital systems, thus enhancing compatibility and co-operation of interacting systems and reducing the ICS aversion.
- The ‘alternative energies’ and technology including the renewables like solar, wind, biogas, the co-generation, fuel cells among others, that are now in train to be integrated into power grids as a matter of incentive-driven EU policy, will inevitably (by design) increase the use of ICS. This may offer a ‘soft and sweetened’ opportunity for a mutual accommodation of the two infrastructures – energy and information, that are fatally bound to a marital status, whether consented or not.
- “*Near-miss*” events on the brink of blackouts would have to be more analytically considered in view of a better understanding of the security needs of critical infrastructures, and the ways the ICS may be of effective assistance.

A long-sighted view on the security of the electricity infrastructure in Europe cannot dispense with keeping an open view on:

- future technological breakthroughs (e.g. quantum computers, superconductivity);
- changes in the political and societal values, including the current landmarks of the managerial code of good conduct (v. privatization, deregulation, liberalization);

- the continental demographical developments, and the intra-generation abilities to address multi-faceted changes.

A long-established by now, and certainly well-intended – if not always reasonable and well-mannered – ecological movement has spoiled consumers with the notion that they may rightfully oppose all ways and means that science, industry and business may offer, ‘to protect and serve’ them. While the *right* in itself should never be questioned, the *abuse* of the right should. This is to be taken in the sense that, after 9/11 2001; the tsunami Christmas, 2005; the Asian earthquakes; the explosive July in UK and Egypt, 2005 and so many other cascading occurrences that have patently evidenced not only educational, technical, managerial, logistic, strategic, and governance flaws, but also *a general lack of preparedness in the face of disasters*, it is high time that *Society, the People (capitals emphasized) should at last share in a fully responsible manner in the endeavour of an informed management of risks and vulnerabilities.*

#### **A.2.4 Managing Critical Electricity Infrastructures in Europe**

*Security culture* for critical infrastructure design, operation, and management is emerging as a topic that has to be professionally handled. In addressing the overall assessment of risk and vulnerability of interdependent critical infrastructures, one should create a technically-informed awareness on how systems could fail; this could be useful and relevant as input knowledge within the design, operation, and re-engineering processes. By adopting individual “*ISO*” *type recommendations* for individual critical infrastructures, one may end up with the need to adopt ISO type recommendations for *handling mainly their interfaces*, while digitalization is becoming a common denominator.

Risks and vulnerability in relation to electricity critical infrastructures become evident especially when facing the public opposition to either build up additional capacities for generation or transportation of electricity, or finalize projects that have been started some time ago. Delays in committing to the grid such capacities, due to changing public attitudes, introduce serious risks to the stability of the European power grid, especially under the new rules of the market liberalization, deregulation and privatization.

Success stories in making the European electricity market competitive and fully operational show that there is a need for adequate timing and management adaptation to the new conditions. The processing of information and access to accurate and open information on the market

behavior are highly consequential. An initial analysis on how various European countries and regions allow access to the information on the electricity markets, from generation to transmission to trading, may discriminate between the following attitudes and beliefs:

*Version A:* 'Unlimited access to the real time, technical and economic information for electricity generation, facilitates the proper functionality of the market.'

*Version B:* 'Use of adequate information systems, including the open systems such as the Internet, brings transparency and stakeholder participation in the process of electricity markets liberalization; the use of advanced and adequate management information systems becomes paramount in the process of successful market liberalization.'

*Version C:* 'One has to consider in cautious manners the degree of integration of open access information systems, in accordance with the specific conditions within the given system.'

*Version D (elusive):* 'There is no conceivable single solution for all countries in Europe, on how to achieve a successful implementation of the electricity market liberalization, deregulation and privatization.'

The issues indicated above, and tracked back to the cases of the different countries in Europe, lead to a first categorization:

- *The Nordic countries*, which have adopted, and have fully implemented over a span of a decade, adequate management information systems, including Internet, and the open access of a large variety of stakeholders to the real time market situation. The integration of the information technology with the rules of the open market with relevance to the electricity generation and transmission is seen as part of the solution for a safe operation of electricity critical infrastructures. The Nordic countries display full confidence in the validity and feasibility of the triad privatization, deregulation, and liberalization.
- Much in the same league, the *United Kingdom*, where the early and independently-initiated start of the liberalization of the electricity market generated effective solutions for both the system and market work in harmony and perform at a high level of success, with no foreseeable new risks and vulnerabilities posed to the associated infrastructure. Like the Nordic countries, the UK stands for a confirmed success of the reformatory projects.

- *The traditionally market-oriented Central European countries*, which are facing a variety of demands and constraints, such as Italy's new capacity sitting and retrofitting problems; the power transit pressure on Switzerland; Austria's gaps in critical transmission lines, and where, generally, the partial inadequacy of the transmission capabilities nullifies the advantage of the excess in generation capabilities, in several regions of concern.
- There is evidence in the Iberian peninsula for a determined and well-managed course towards a successful implementation of liberalization and deregulation, with solutions that fit the local conditions and were carefully integrated into the socio-economic fabric. A notable feature is government's being fully involved in observing the overall regulatory process needed to sustain market liberalization, with involvement of other national actors too.
- Special conditions in Greece, as *the* traditionally market-oriented Balkan Country, seem to delay the process of unbundling in the electric power sector. The lack of domestic incentives, and the imperatives of 'bare necessities', both technical and economical are pointed at, when it comes to explain several considerable problems, the ultimate expression of which is the perceived threat that the already started process on market liberalization and deregulation be stalled, or even reversed.
- *Finally, there come the Central- and Eastern European countries recently emerging from centrally-planned, non-market economies*, and posing radically-different problems. In the absence of truly relevant statements or comments on liberalization, deregulation and privatization commitments from authorized domestic analysts, let it be only said that these countries are, to an extent or another, faced with the need to adapt their infrastructures and, particularly, management to the new conditions of operability including being now part of the UCTE system, with its new rules and requirements. In several countries under this category, the true amplitude and consequences of the structural and managerial transition required is only marginally perceived at domestic levels and, more often than not, is approached at only a rhetorical, or 'political correctness', level. Money and

a determined 'ideological' and managerial guidance from the West will be of essence.

On a technical chord, a pattern has somehow emerged, in understanding the current situation in Europe with respect to the penetration of Risk Governance attributes and features. Thus, the main success criteria in implementing privatization, deregulation and liberalization at regional and domestic levels may well be:

- The share of the adopted *e-governance platform* within a given region or country.
- The society's perceived capability to change, in relation to the adoption of the full set of rules and directives regarding the new electricity market across Europe.
- The degree to which various instruments of risk governance have been deployed, and employed.

And yet, the true issues are definitely beyond the realm of the technical ingredients. If one is to condense the imperatives of the times in a single word only, then, in all senses conceivable, that word is the one that the Europeans had always a hard time to utter: ***Sharing...***



## Appendix 3

### Security Conceptual Frameworks

*Marcelo Masera, Alberto Stefanini, Giovanna Dondossola*

The issue of power system reliability and security, and its relationship with system stability, is debated since the 1920s. There have been repeated attempts to establish a systematic approach to the matter, by for instance CIGRE and IEEE Task Forces, starting from the 1950s until the recent deliberation issued by a Joint Task Force (JTF) of the two bodies (IEEE/CIGRE, 2003; IEEE/CIGRE 2004). In the fifth section of both these reports, the relationship between the concepts of power system reliability, security and stability is summarised as such:

*“**Reliability** of a power system refers to the probability of its satisfactory operation over the long run. It denotes the ability to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period.*

***Security** of a power system refers to the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service. It relates to robustness of the system to imminent disturbances and, hence, depends on the system operating condition as well as the contingent probability of disturbances.*

***Stability** of a power system refers to the continuance of intact operation following a disturbance. It depends on the operating condition and the nature of the physical disturbance.”*

According to the JTF, “*Reliability is the overall objective in power system design and operation. To be reliable the power system must be secure most of the time. To be secure the system must be stable but must also be secure against other contingencies that would not be classified as stability problems, e.g., damage to equipment such as an explosive failure of a cable, fall of transmission towers due to ice loading or sabotage. As well, a system may be stable following a contingency, yet insecure due to post-fault system conditions resulting in equipment overloads or voltage violations*”. UCTE, in the OpHB Glossary (UCTE, 2004), summarizes a well accepted definition: “*Reliability describes the degree of performance of the elements*

of the bulk electric system that results in electricity being delivered to customers within accepted standards and in the amount desired”.

A further distinction is made between two basic and functional aspects of reliability:

*“Adequacy: the ability to supply the aggregate electric power and energy requirements of the customer at all times, taking into account scheduled and unscheduled outages of system elements.*

*Security: the ability to withstand sudden disturbances such as electric short circuits or non-anticipated loss of system elements.” (IEEE/CIGRE, 2003)*

Dependability of computer and communication systems had been a concern since the foundations of these technologies (Avizienis, 2001). Computer Science and systems engineering view *dependability* as a global concept, encompassing such properties as:

- *availability*: readiness for correct service
- *reliability*: continuity of correct service
- *safety*: absence of catastrophic consequences on the user(s) and the environment
- *confidentiality*: absence of unauthorized disclosure of information
- *integrity*: absence of improper system state alterations
- *maintainability*: ability to undergo repairs and modifications

Several other dependability attributes have been defined that are either combinations or specializations. For instance, security is defined as the concurrent existence of *availability* for authorized users only, *confidentiality*, and *integrity*.

The widespread use of information and communication technologies made the above terminology accepted in many sectors of industry in Europe, starting from the safety critical ones: automotive, aerospace, railways, ships etc., so that it may be considered as a mature conceptual framework nowadays. Dependability requirements are therefore defined as the “*required goals of the application system in terms of the acceptable frequency and severity of the failure modes, and of the corresponding acceptable outage durations (when relevant), for a stated set of faults, in a stated environment*” (*ibidem*). Based on these notions, various ICS specification and design methodologies have been introduced to either prevent the introduction of (mainly software) design faults, or avoid failures by tolerating those faults – for instance:

- Structured methodologies based on languages such as UML;

- Methodologies based on the Automata Theory like Superimposed Automata (Ciapessoni, 2001);
- Formal specification and verification & validation methods based on logical languages (Heitmeyer, 1996).

The methods and tools for state space analysis based non Petri Nets and Timed Automata are applied for the quantitative analysis of identified dependability properties (Schneider, 2004). The specification and analysis of dependability requirements have been also addressed by structured methodologies integrating standard object-oriented notations such as UML (Bernardi 2004) with (logical and operational) formal languages.

As a matter of fact, the dependability framework from Computer Science was never fully taken up by the power sector, where the previously described “power security” perspective emerged long before the introduction of digital computer systems. This is especially confusing due to the digitalization of the power sector: the same problem (let’s say, a blackout caused by a failure in a control system) has to be described with different, unrelated notions, very often using the same terms, namely:

- *Reliability*: continuity of correct service. The divergence (perhaps subtle depending on the context) is that the power definition states reliability as the goal “*to supply adequate electric service on a nearly continuous basis, with few interruptions over an extended time period*”. This corresponds to availability in the computer systems domain, as reliability refers to the continuity of correct service and is incompatible with the occurrence of any service failure.
- *Security*: there is a substantially dissimilar, uncorrelated meaning of this term between the two disciplines. In Computer Science (Laprie, 1992) security refers to “*dependability with respect to the prevention of unauthorized access and/or handling of information*”, while Power System security, as discussed before, is “*the ability to withstand sudden disturbances such as electric short circuits or non-anticipated loss of system components*” (IEEE/CIGRE, 2004).
- *Dependability*: formally defined in Computer Science, while it has no formal meaning in Power Systems Engineering, although sometimes in this latter discipline dependability is used as synonymous of reliability.

The practical consequence of these different conceptions of reliability in Power Systems and Computer Science is that there exist no comprehensive approaches to risk assessment, which can be applied for concurrently evaluating the failures of electro-mechanical and digital components.

The latent harmful consequences deriving from ICS vulnerabilities are known: “*Devices used to protect individual equipment may respond to variations in system variables and cause tripping of the equipment, thereby weakening the system and possibly leading to system instability*”, (IEEE/CIGRE, 2004). For that reason, if it is accepted that the failure of ICS (monitoring and supervisory equipment, control equipment, communication networks) was one background cause of some of the recent power system outages, and will be a potential key source of power systems disservice, such wide-ranging assessment methodologies have to be considered an urgent challenge.

In the Critical Infrastructures Protection (CIP) arena there have been recent attempts to reconcile the power system view to the Computer Science one. Holmgren et al. (Holmgren, 2001) from the Swedish Defence Research Agency Research propose the following definitions:

- *Vulnerability*: the property of an infrastructure system that limits its ability to endure threats and survive accidental events that originates both within and outside the system’s boundaries
- *Robustness*: a system’s ability to endure threats and survive accidental events that originate both within and outside the system’s boundaries, and if disturbed, return to a state where the operating characteristics correspond to the assigned function
- *Reliability*: the ability of an item to perform a required function, under given environmental and operational conditions and for a given period of time
- *Risk*: a combination of the likelihood for an accident to occur and the resulting negative consequences if the accident occurs.

In the main, this approach is seemingly closer to the global approach to dependability, but it needs to be complemented as it does neither pretend to integrate the classical Power System approach, nor consider the specific elements that characterize intentional acts..

A unifying view might be based on the recently proposed SQRA concept to define properties of a power system as a service infrastructure (Samotyi, 2003). This approach defines four concepts that have to be simultaneously fulfilled by electric power systems, corresponding to four types of vulnerabilities:

- *Security* of power delivery and market systems as a measure of system exposure to natural events, human errors, and intentional attacks;
- *Quality* of power supplied as a measure of electric supply characteristics that can impact the performance of digital systems;

- *Reliability* of power supplied as the number of failure events and the amount of time the system is accepted to be unavailable in a given year;
- *Availability* of affordable energy services as the average time per year the system is in service and is satisfactorily performing its intended function.

Yet, these are only first attempts to develop a common overall security framework of reference, shared by all actors involved in the power infrastructure engineering life-cycle: from the planning to the design, and from the operation to the maintenance of systems.

## Appendix 4

### ICS Security Standards

*Marcelo Masera, Alberto Stefanini, Giovanna Dondossola*

#### A.4.1 Introduction

Standards are a key driver in the development of engineering systems in general, and of the electric power sector in particular. Standards, which can impose a certification scheme, constrain the technical choices, or harmonize by promoting their voluntary adoption. With reference to ICS and specifically to security, standards will be fundamental for the creation of a market and for supporting the procurement process. As a consequence, the design and implementation of security countermeasures will be facilitated, best available practice can be applied in a consistent way, and the risks across the infrastructure can be reduced in an uniform way.

But, what is the current status of ICS security related standards? Reality is that the production of standards is at its early stages. Acknowledgement of their importance is rather new – less that a decade old; and awareness of their urgent need if more recent.

The situation is challenging, and by all accounts will continue to be so for the next decade – if not more. Industry is already waiting for standards that will not be ready in the next coming years. In the meantime ICS technologies are being deployed with an ad-hoc approach to security, based on the restricted knowledge of each company.

There is therefore the risk that standards will arrive too late: when some important accidents will have happened, and when non-standard and incompatible solutions will be in use. As ICS are at the core of the interconnections among the different actors of the electric power sector, the delay in the availability of effective standards is, by itself, other vulnerability; the near future will see a great window of opportunity for ICS security-based incidents.

This deficiency has to be dealt with immediately, as any further postponement of clear positions by industry and regulators can aggravate the security conditions. The answer to this situation can take the form of an intermediate set of guidelines and best-practices to be applied in the transitional period until appropriate standards will be complete. This is the approach in North America, with the leadership of institutions such as the North America Electric Reliability Council (NERC) and the USA's National Institute of Standards and Technology (NIST). Similar initiatives would be greatly desirable in Europe.

A further factor that will have to be taken into account is the convergence with telecommunications and particularly the work on Internet. Although the electric applications run on top of the communication layers provided, the evolution of the latter will significantly affect the functionality and security of the others. Not the least, some other vendors and communities might come from the telecommunications and computing networks sector, offering their security solutions and constraining the electric power sector choices.

#### **A.4.2 Power Sector Standards and Recommended Practices**

The necessity for the consideration of information and network security in the electric power sector standards was only acknowledged in the late 90's. The proprietary and isolated nature of the ICS equipment up to those years seemed to require no special provision.

The International Electrotechnical Commission (IEC) is the leading international body for electrical, electronic and related technologies. Its Technical Committee 57 "Power Systems Management and Associated Information Exchange" issued the Technical Report TR62210 in May 2003 discussing the security aspects related to the computerised supervision, control, metering and protection in electrical utilities. TC57 recognizes in its Strategic Policy Statement (IEC, 2003) that "The fast development of information technology (IT) and communication technology has impact on the work of TC57". A key point of the strategy is to open proprietary structures by standardization of data exchange interfaces among IT systems and software applications".

The committee collaborates with other organisations making important developments with respect to SCADA security, such as the American Gas Association (AGA), the Instrumentation, Systems and Automation Society (ISA) and NIST. It is composed of a relevant set of working groups, among them: telecontrol protocols, distribution automation, substation

communication, application program interface for Energy Management Systems, communications for deregulated energy markets, interfaces for distribution management systems, interoperability, and especially the Working Group 15 data and communication security, launched in October 1999. The dates show that the intervention was arriving late with respect to the actual use of insecure remote access equipment in the field installations.

TR 62210 illustrates the risks associated with the typical IEC communication protocols, examining some threats, vulnerabilities and potential consequences of electronic intrusions. The document also considers some actions and countermeasures that can be applied, and presents a first attempt to analyze the risks with a cause-consequence diagram.

A first lecture of the IEC's Technical Report (Dondossola, 2004) puts on view some unusual elements for Technical Committees dealing with "computerised supervision, control, metering, and protection systems in electrical utilities":

- It is recognised that ICS security involves the "corporate security policy", which should be the departure point of the so called "Normal corporate security process". But that security policy is not part of the customary practice of electric power companies. How many European companies do have an explicit information security policy? And if yes, which are the references for the industrial control and communications sections?
- It is recognised the importance to create common vocabulary, as shared notions are the basis for standards. Threats, vulnerabilities, information security etc. are not yet stabilised notions.
- It is recognised that vulnerabilities and threats have to be analysed with reference to the consequences that might be produced. Some of the consequences suggested point to the broad set of elements that need to be examined: loss of revenue due to increased competition or contractual disputes, reduced profitability due to cash flow disturbances, manipulation of production and consumption data that leads to erroneous forecasts, artificial change in stock value, asset destruction or degradation, etc. In addition it is evident that most of these topics fall outside the typical analytic space of engineers, indicating that assessing these consequences will not be easy, and will demand suitable methodologies and the participation of a considerable staff.
- It is recognised that the network topology interconnects all actors of the electric power system, technical and market-related. The



suggested list of stakeholders is ample: obviously generation, transmission and distribution companies, but also data aggregators (business entities that for instance process and combine metering data), meter service providers, electricity suppliers without installations (that operate in the electricity wholesale market), risk management market participants (that sell, trade, broker or operate with derivatives in the market), and finally the end customers (who expect not just the supply of energy, but also information services related to the technical operations, the commercial relations and the market). This broad set of actors also point to the potential difficulty of the security assessment.

- The report suggest the employment of a methodology for the assessment (i.e. consequence diagrams), that requires the identification of all relevant stakeholders, the business processes that concern them, the consequences that can adversely affect those processes, and the events that might provoke those consequences. This will serve for ascertaining the threats and the vulnerabilities that are of primary importance. If such assessments are to be accepted as necessary, it is apparent that much more research in the field and training of personnel will be required.
- The Report finally links the identified relevant threats to the specification of the protocols developed by the Technical Committee 57, and especially the Telecontrol Application Service Element No. 2 (known as TASE.2), and the IEC 61850 and IEC 61334 series (respectively devoted to communication networks and systems in substations, and distribution automation using distribution line carrier systems). It is proposed to apply the standard ISO 15408 (known as Common Criteria, discussed later in this chapter), for the generation of Targets of Evaluation (TOE) and Protection Profiles (PP) for the protocols. A vast work can be foreseen in the interplay between the specificity of each installation (and consequently their own security risk) and the genericity of TOE and PP. The needed standards will not be available in a short period.

The International Council on Large Electric Systems (CIGRE') convened in 2003 the Joint Working Group D2/B3/C3-01, with participation of the Study Committees D2 (Information Systems and Telecommunication), B3 (Substations) and C3 (System Environmental Performance). Its objective is explicitly the security of the ICS of the electric power systems. The working group is producing a series of papers that will undoubtedly serve for raising awareness in the sector. The first

two papers have been published in the journal *Electra* (CIGRE, 2005a; CIGRE, 2005b). The intention is to present a series of reflections and suggestions of immediate actions that could help in bettering the level of ICS security and the development of proper security policies.

In North America, NERC (North American Electric Reliability Council) has organised a Cyber Security Urgent Action, resulting in some guidelines, compliance audits, and activities such as workshops for raising awareness. In 1998 the USA's Department of Energy assigned to NERC the role of co-ordinator of critical infrastructure protection activities reference point for the electric power sector, including cyber security. It was created the CIPC (Critical Infrastructure Protection Committee) that develops and maintains capabilities to respond to security threats and incidents, and supports the production of standards and guidelines. In June 2002, NERC issued the "Security Guidelines for the Electricity Sector" that cover physical and cyber security, along with emergency plans and business continuity. The approaches and practices recommended are generic, and no indications of particular methodologies are given. In any case, the guidelines are useful for disseminating common requirements and could act as a basis for further developments.

NERC's Cyber Security Urgent Action was set with the purpose to reduce the risks from any compromise of critical cyber assets. A first standard (known as Urgent Action Cyber Security Standard 1200) was issued in August 2003. It is applicable to control centres only and aimed at self-certification. The Draft 2 of the last Cyber Security Standards proposed by the NERC Action (CIP-002-1 through CIP-009-1, formerly known as Urgent Action Cyber Security Standard 1300) was issued in August 2003 and is currently under review by the drafting team. It is expected to be finished by mid 2005 and applies to control centres, power plants – except nuclear– and substations and lists several tasks that are deemed essential for cybersecurity, ranging from security management controls, to the identification and definition of critical assets, controls, personnel, and functions such as training, systems security management, incident response and recovery plans. But it doesn't consider control system protocols.

The standard presents detailed metrics. Its importance resides more in its specification of basic requirements and measures, and the definition of compliance monitoring processes, levels on on-compliance and sanctions. This is a language easily understandable by industry and demonstrates a significant commitment. This type of approach, although its results will always be far from comprehensive, gives an important indication to all players in industry and regulatory bodies: the recommendation we can

derive is that the problem is serious, basic solutions are urgently needed, compliance and enforcement are a must.

In parallel NERC manages the ES-ISAC (Electricity Sector Information Sharing and Analysis Center), for the exchange of information on critical risks in the electric power sector. In particular two indexes have been developed for indicating the threat levels for indicating the possibilities of physical and cyber attacks. These instruments are very helpful for creating alertness on the situation, but also a general awareness on the risks.

### **A.4.3 Other Industrial Control Initiatives**

In parallel, IEEE has been producing some standards, such 1547 for “Interconnecting distributed resources with Electric Power Systems”, 1525 for substation automation, and 1379 for substation IED communication. The IEEE Substations Committee has the task force C0 TF1 that deals with Substation Data Security. An open question remains on the multiplicity of efforts for a sector that needs promptly answers.

There are related activities in other industrial sectors that are germane for electric power. In the Instrumentation, Systems and Automation Society (ISA), the committee SP99 looks after control system security. CIGRE takes part in this initiative. ISA has a standard under development that will be issued in the coming years, with a multi-industry focus. Part 1 that aims at the consolidation of models, definitions and terminology will be ready by the end of 2005. Part 2, dealing with security programs and the analysis of risks and vulnerability will be presented in draft forms in the following months. Part 3 (on Security Programs) and 4 (on Security requirements and controls) will only begin their development in the future. There is of course no guarantee that the adopted terminology and methodology by ISA, although coherent and efficacious in their context, will not enter into conflict with other initiatives.

The American Petroleum Institute has been working on cyber security guidelines documents and API 1164 is the first (published in 2004) dealing with SCADA security best practice. Its goal is to provide an easy to follow and rapid guide to industrial companies mainly in the pipeline sector – but their applicability is broader. There are no plans for third party certification or requirements on self-certification. Although incomplete and not very sophisticated from the security viewpoint (for instance in the consideration of authentication and access control, links to security policies, etc.), it provides ready applicable and sound recommendations. It is therefore a straightforward, practical and undemanding effort that, if applied by industry, can have immediate effects. As a provisional action while waiting

for more thorough measures, it is a lesson to learn by the European electric power sector.

The American Gas Association (AGA) initiated quite early some initiatives in the context of infrastructure security. Already in 1988 they had the first discussion in the use of encryption protocols to protect the gas sector communications and the SCADA systems. The first technical proposals by the Gas Technology Institute (GTI) received scarce attention, due to the lack of awareness on the risks. Only after the September 11<sup>th</sup> 2001 events there was some consciousness that specific safeguards were required. The work is conducted by a dedicated working group that has delivered the standard report AGA 12 “Cryptographic Protection of SCADA Communications” (Draft 4), issued in November 2004. Although the work is limited to the encryption of communications, the working group pointed to the beginning to generic results targeting several industries: gas, electric, water, wastewater and pipeline real-time control systems. It should be considered that encryption is a valuable solution, but it is first needed to understand the problem: the security risks.

NIST has released in April 2004 a System Protection Profile for Industrial Control. This has been developed in the context of the Process Control Security Requirements Forum (PCSRF). The specification follows the Common Criteria, as a starting point for the specification of security requirements. The document extends the typical elements of a Protection Profile (PP) to broaden security controls to non-technical procedures and management functions. The PP is generic to all kinds of industrial control, focusing in the subset of elements that are applicable to all implementations. Very importantly, NIST highlights that security functions should respond to risk analyses and dedicated assessments, and that these assessments should be applied to new designs, but also for retrofits and upgrades.

#### **A.4.4 General-Purpose Standards**

There are two general standards that set the reference framework for all initiatives in information security: ISO 17799, the Code of practice for information security management, and the already mentioned ISO 15408, the Common Criteria. Both standards provide guidance to security management and the specification of security requirements for products, respectively. But they don't demand the application of specific methodologies or technical architectures.

ISO 17799, derived from the British Standard 7799 and produced by the ISO/IEC Joint Technical Committee 1, Subcommittee SC 27, in December 2000, presents a starting point for developing organization specific guidance arrangements. It is a “comprehensive set of controls comprising best practices in information security”, and comprises a code of practice and a specification for an information security management system.

A corporation applying it will have to perform a risk assessment, prepare its security resources, and prepare the needed elements for certification and compliance. These will include the corporate security policy, and the functional and assurance requirements that have to be implemented. The standard provides a generic list of these requirements at a high level, independently from specific technologies. A fundamental point is the provision of appropriate security policies. A policy should set the direction for action and the commitment of the company to information security. Remaining at the management level, the application of this standard to industrial installations, mainly one with potential critical consequences, seem to merit a review, or at least a complement with particular considerations on, for instance, timing issues related to control applications.

As a single reference point, ISO 17799 is important for providing a common view on administrative and industrial information and communication systems. If companies across an industrial sector would apply it, the creation of a trusted environment will be fostered.

The Common Criteria are the result of long developments in the USA, Canada and European countries (the Netherlands, France, Germany, United Kingdom), and aimed at supporting the specification of products with security requirements. First published in 1996, its second version was adopted by ISO as standard 15408 in 1998. The requirements to be defined are functional requirements, those related to desired security behaviours, and assurance requirements, which are the basis for gaining confidence that the claimed security measures are effective and implemented correctly. The standard gives the possibility to select among seven evaluation assurance levels, which can be used for grouping components, or provide retrofit compatibility with existing products (first 4 levels), or develop specialised components.

This standard supports purchasers of products in the definition and formulation of the requirements they necessitate; vendors or developers in the specification of their products, and third party evaluators in the verification and validation of products. In this way, the whole procurement process is assisted with common terminology and procedures.

It is understandable that several approaches to the security of industrial control have taken the Common Criteria as reference. However it should be considered that this standard, although technically important, hasn't been heavily applied in the real world. Verifying technical products against a standard that comprises functional and assurance procedures is very costly. Some significant criticisms are that the evaluations don't seem to add value while entail notable costs, that it doesn't have a noteworthy impact on the reduction of vulnerabilities, that the engineering efforts could be better employed in other technical tasks related to security.

As a consequence, we can say that the Common Criteria might mature into a useful framework for the development and procurements of security devices. Nevertheless, it will take time and will be dependent on the evolution of the standard in other fields. In addition, the more immediate needs of the electric power sector seem to lie in the system evaluation area – and this is not currently supported by the Common Criteria. These will have to evolve, incorporating new assurance requirements.

## Appendix 5

# Critical Information Infrastructures (CII) and Risk Analysis Framework

*Myriam Dunn, Isabelle Wigert, Adrian Gheorghe*

### A.5.1 Innovation strategies for reduced vulnerability

Innovation is an important part of the answer to the challenge for security and reliability under the new infrastructure governance paradigm. Current innovation efforts directed towards enhanced reliability of critical infrastructures are grouped under three themes:

- Smarter infrastructures
- Alternative infrastructures
- Résilient infrastructures

In addition to these three innovation strategies, we briefly detail a number of ICT-innovations that enable smarter capacity management in infrastructures for transportation of people and goods. The challenge of bringing about the required investments for innovation and the possible role of government regarding this challenge is addressed here. Where current market designs fail to ensure public values on the long term, change is urgently needed, as the overall demand for infrastructure related services is still growing at a fast pace, and the quality demands imposed on the services will be increasing likewise with the increasing dependency of society and the economy on those services.

#### A.5.1.1 Smarter infrastructures

One of the most consistent trends of the past decades has been the steady growth of electricity consumption, telecommunication services and air, road and rail traffic. Where this growth has been faster than the development of infrastructure capacity, we have seen congestion, overload,

shortages and similar threats to reliability. Traditionally, the increasing demand for services is met by building new infrastructure – more roads, expanded airports, new electricity generators, more transmission capacity, increased bandwidth in data networks, et cetera. Building new infrastructure will remain an important activity. However, in the current economic and regulatory climate, building costly new infrastructures is proving to be more and more difficult for policy makers in the EU member states. The constraints vary from more stringent spatial and environmental constraints to limitations on the funds available in the public and private sector.

These constraints have pushed for innovations that make infrastructure ‘smarter’ instead of larger. ‘Smarter’ typically means that capacity is allocated more efficiently. Much of this relies on innovative technologies, such as ICT, to control and manage infrastructure at the network level (see table 2 on different levels). This way, reliability is strengthened – not only by keeping up with increasing demand, but also because of the enhanced control and management of the infrastructure itself.

### **A.5.1.2 Alternative infrastructures**

Under the traditional paradigm, each infrastructure delivered a fairly stable and distinct set of services. However, infrastructures have innovatively crossed over into each other’s markets. For consumers, this means they can get the same or a similar service through different infrastructures. A typical example is internet access. In addition to phone line connections, we now also see access through cable networks originally used for transmitting TV-signals and through wireless networks (WiFi, satellite, GPRS/UMTS).

Some alternatives are being delivered through existing networks. Others require new networks, such as the MagLev trains. Some innovation go even further, such as the scenario of the “energy internet,” where the centralized system of power generation, transmission and distribution is largely replaced by a distributed system of local generation units and power sharing.

The availability of substitutes is an important contribution to the reliability of these services – as well as a main driver of competition, raising quality levels and lowering prices. Infrastructures are more and more interconnected and overlapping in terms of the services they provide. How can the use of alternative infrastructures contribute to increasing reliability?



### **A.5.1.3 Robust and resilient infrastructures**

Innovations are emerging that aim to make infrastructures more robust and more resilient. More robust means that infrastructures are better able to predict and prevent incidents. More resilient means, infrastructures are more able to ‘bounce back’ from incidents that do occur.

In recent years, attention has shifted toward resilience of infrastructures. Under the new paradigm, it has become more difficult to predict and prevent incidents – with the extreme example of terrorist attacks. Therefore, it becomes more important to cope more effectively with these incidents before they lead to large-scale disruptions or system failure.

Innovations in this direction include specific technological and organizational solutions, but also changing approaches to infrastructure design in general, such as the concept of ‘self-healing infrastructures.’ These new approaches seek to better cope with incidents through distributed intelligence in the system itself, rather than in centralized control centres.

### **A.5.1.4 Capacity Management in Transport**

In the field of transportation, three promising innovations have emerged that rely on advanced ICT to make the infrastructure smarter:

- ATM (Air Traffic Management)<sup>1</sup>.
- EVI (Electronic Vehicle identification)<sup>2</sup>.
- TIS (Traffic Information Systems)<sup>3</sup>.

These innovations potentially create breakthroughs in infrastructure management, but this potential can only be realized when a number of policy issues is addressed first.

<sup>1</sup> Recent Single European Sky legislation is an important step to more effectively deal with the issues of safety, capacity and efficiency in European airspace. It has already stimulated the involvement of the ATM industry in developing new technology for air traffic management. The proposal of the industry, known as ‘SESAM’, is a further step in making joint progress that can bring about a structural solution to existing and, on the short term expected, capacity bottlenecks.

<sup>2</sup> EVI enables a series of applications serving different public goals wherein the identity of the vehicle and/or owner is rather essential. Capacity management is one of them

<sup>3</sup> TIS enables travellers, transporters and enterprises to base their transport planning on more reliable and real-time information of the actual available capacity of infrastructure (for instance of the road).

### **A.5.1.5 Investments in new infrastructures**

An important means of increasing the reliability of infrastructures is building new and innovative infrastructures. New alternative infrastructures generally increase overall capacity and incorporate state-of-the-art technologies that match higher reliability standards. What is more, new infrastructures that compete with existing infrastructures constitute a redundancy that enhances overall reliability.

In the current economic climate public money for constructing alternative infrastructures is often scarce. Moreover, both policy makers and economists largely agree that public financing of such investments should no longer be a default, as it might have been some decades ago. On the other hand, investments in infrastructures are generally high, face political risks, and often have uncertain returns and long payback times, which imply that private parties might also be reluctant to invest. Taking these drawbacks for private initiatives into account, the central policy question of this Appendix is: How can policy makers improve the climate for private investment in new and innovative infrastructures, in the fields of energy supply, telecom and transport?

### **A.5.1.6 Framing the risk governance question**

There is a sense of urgency from an economic perspective to place the reliability of infrastructure-bound services high on the political agenda. Adding the complex system perspective, there is also abundant reason to place the reliability of infrastructures high on the agenda for research and innovation. The need for knowledge to ensure a better understanding, the need for innovation and the need for policy action to safeguard the reliability of infrastructure, becomes evident when we see that the annual societal damage caused by infrastructure malfunctioning runs in the billions of euros. Although reliable aggregate cost figures are missing, even a conservative estimate of known damages incurred by routine failures already amounts to over 5% of the EU-25 GDP. Consequently we identified the following urgent policy questions:

- Have Member States made the reliability of vital infrastructures the priority it needs to be?
- How can Member States ensure the reliability of such vital services as electricity, internet, telephony, air traffic, and road transport?

- Are the current – European, national and sectoral – market designs and regulatory frameworks capable of dealing with the new complexities of infrastructures?
- What technological and institutional innovations are needed to make infrastructures more intelligent, more flexible and more robust and resilient?
- How can Member States stimulate private investment in innovative infrastructure development?
- What initiatives are needed at the European level?

### **A.5.1.7 Conclusion**

Innovating for reliable vital infrastructures is a challenge that needs to be addressed not only within each infrastructure on its own. These issues require intensified cooperation among the transport, telecom and energy sectors at the European level for three reasons:

- The sectors face the same fundamental challenge to their governance of reliability and a coordinated response is needed to be effective – much like the liberalisation policy was inter-sectoral and coordinated;
- Innovations in one sector provide lessons for the other sectors;
- The interdependencies among infrastructures in the three sectors are intensifying, which implies that the interconnections among transport, telecommunication, information and energy infrastructures require immediate attention.

## **A.5.2 Risk Analysis**

### **A.5.2.1 Introduction**

In the context of CIP/CIIP (Critical Infrastructures Protection / Critical Information Infrastructures Protection), risk analysis could theoretically address any degree of complexity or size of system. However, when the boundaries of the evaluated system are set too wide, the lack of available data makes accurate assessment difficult or even impossible. The risk estimate is produced mainly from the combination of threat and vulnerability assessments. It analyzes the probability of destruction or

incapacitation resulting from a threat's exploitation of the vulnerabilities in a critical infrastructure. In the least, risk analysis encompasses risk identification, risk quantification, and risk measurement, according to the three classic questions:

- a) What can go wrong?
- b) What is the likelihood of it going wrong?
- c) What consequences would arise?

Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:

- a) What can be done?
- b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
- c) What impact do current management decisions have on future options?

Even though risk analysis is extremely well established and used in different communities, it has many shortcomings. These include especially the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decision-making processes. There are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events – and this is what we are dealing with in the context of CIP.

### **A.5.2.2 Examples of Risk Analysis Processes for CI/CII<sup>4</sup>**

Below, the following seven examples are described:

- 1 Australia and New Zealand – Risk Management Standard (NSW)
- 2 Canada – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)
- 3 European Union – The CORAS Project (CORAS)
- 4 Norway – Protection of Society Project (BAS)
- 5 Switzerland – Swiss Roundtables Risk Analysis Methodology (Roundtables)
- 6 United Kingdom – NISCC Building Blocks (NISCC)
- 7 United States – OCTAVE Methodology (OCTAVE)

#### ***1 Australia and New Zealand – Risk Management Standard (NSW)***

The *Australian and New Zealand Standard for Risk Management* (AS/NZS 4360:1999) is the standard by which all critical infrastructures

<sup>4</sup> This is an abbreviation for Critical Infrastructures / Critical Information Infrastructures

are assessed to assist with the review of risk management plans for prevention (including security), preparedness, response, and recovery<sup>5</sup>. The Australian *Defence Signal Directorate* (DSD) has also released a new version of the *ACSI33 Government IT Security Manual* in an attempt to consolidate and restructure a number of existing Australian IT security policy documents into a single, cohesive manual. The *New South Wales Office of Information and Communications Technology's* (OICT) website additionally features a long list of guidelines for information management and information security. The *Information Security Guidelines Part 1* is concerned with risk management<sup>6</sup>. Its objective is to assist government agencies in the identification and management of information security risks. Its components are: assets, asset values, threats, vulnerabilities, security risk, security requirements, and security controls (Figure A.5.1).

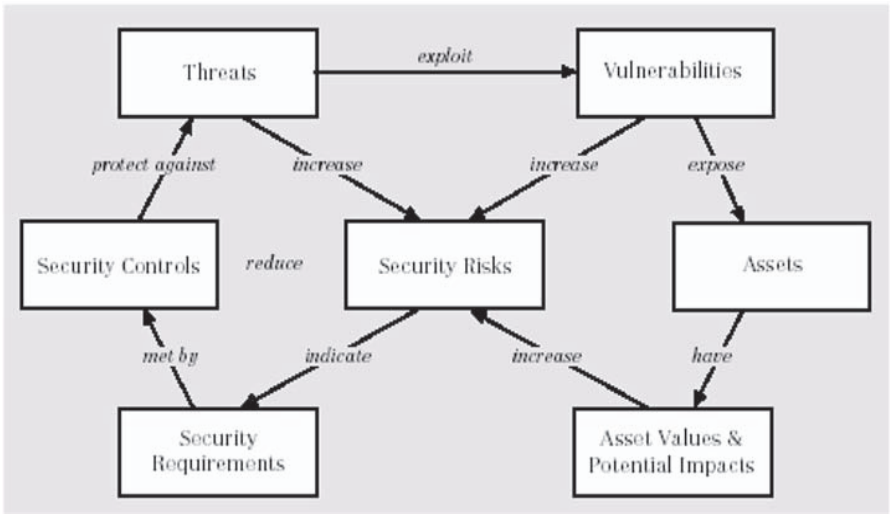


Figure A.5.1. Risk Concept Relationship

<sup>5</sup> The AS/NZS 4360:1999 standard provides a generic guide for the establishment and implementation of the risk management process involving identification, analysis, evaluation, treatment, and ongoing monitoring of risks. In accordance with AS/NZS 4360, it is necessary to establish the strategic context. In the current security environment, security risk assessments should also consider terrorism in all its forms.

<sup>6</sup> This guideline is based on the *Australian/New Zealand Handbook on Information Security Risk Management* (HB 231:2000). It should also be read in conjunction with the *Information Security Guidelines Part 2 - Examples of Threats and Vulnerabilities* and the *Information Security Guidelines Part 3 - Information Security Baseline Controls*.

## 2 Canada – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)

In the spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive review process for critical infrastructures in Canada. One of the goals was to better understand risks (Figure A.5.2).

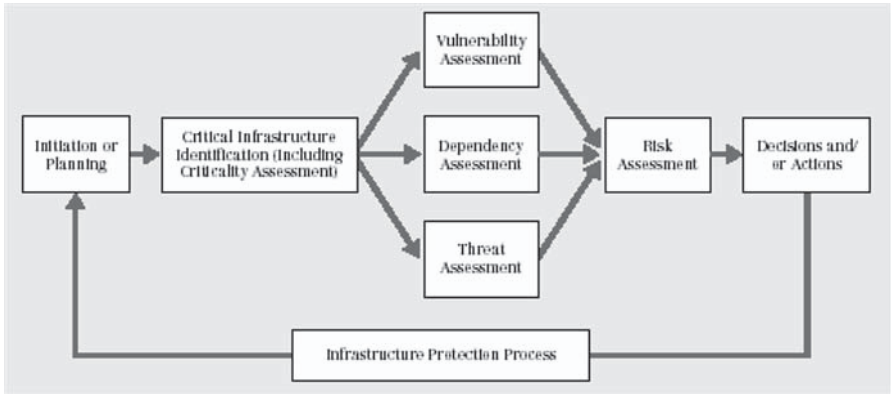


Figure A.5.2. Canadian Infrastructure Protection Process

Risks were determined by using a *Risk Rating Matrix* that multiplies threat values with vulnerability values. This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructure elements, which are called specific risks. It was taken into account that risks accumulate when the risks of dependencies are propagated (*Cascading Effect*). Therefore, the Canadian process conducts a *Cumulative Risk Assessment* through dependencies. The assessment of impacts can be done with a *Risk/Impact Scatter gram*.

## 3 European Union – The CORAS Project (CORAS)

The EU-funded *CORAS* project (IST-2000-25031) developed a tool-supported methodology for model-based risk analysis of security-critical systems.<sup>7</sup> The *CORAS* methodology for model-based risk assessment

<sup>7</sup> The project was initiated in January 2001 and completed in September 2003. The *CORAS* framework consists of terminology, languages for system modelling, processes for system development and risk management, and methodologies for security risk analysis as well as computerized tools.

(MBRA) applies a standardized modelling technique to form input models to risk analysis methods that are used in a risk management process. This process is based on the *AS/NZS 4360:1999 Risk Management* standard.

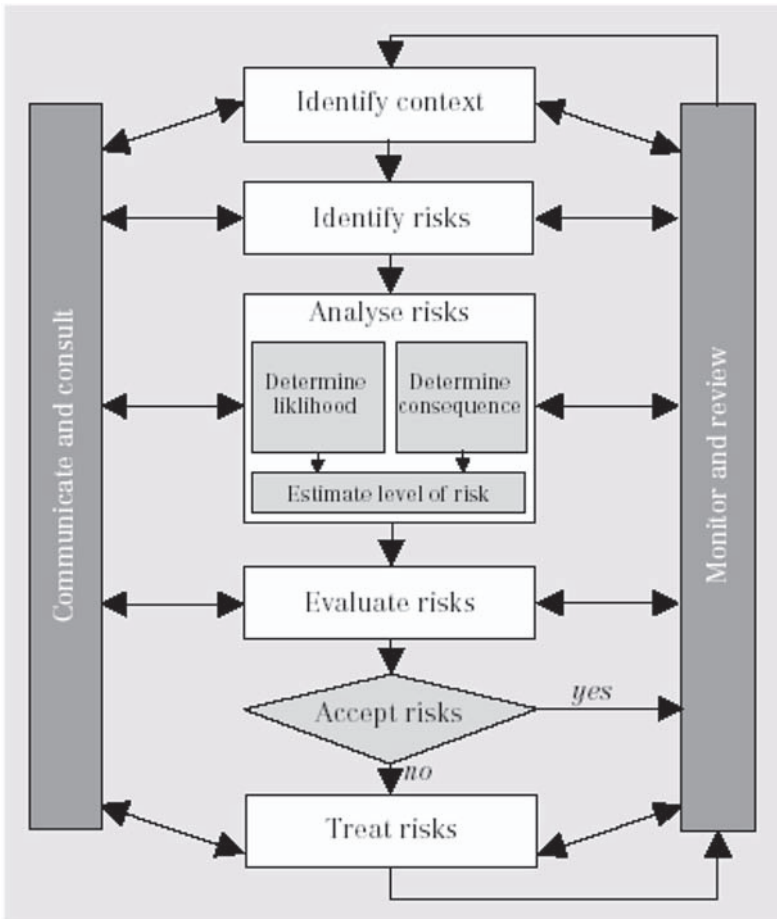


Figure A5.3. The CORAS Risk Management Process

Figure A5.3 indicates that the AS/NZS 4360 standard provides a sequencing of the risk management process into sub-processes for context identification, risk identification, risk assessment, risk evaluation, and risk treatment. In addition, there are two implicit sub-processes targeting “communication and consultation” as well as “monitoring and review” running in parallel with the first five steps.

#### 4 Norway – The Protection of Society Project (BAS)

“Protection of Society” (BAS) is a joint project between the Directorate for Civil Defence and Emergency Planning (DSB) and the Norwegian Defence Research Establishment (FFI). The project uses a methodology for cost-benefit/cost-effectiveness analysis to design and evaluate civil emergency measures. The same methodology was applied in the project “Protection of Society 2” (BAS2). The purpose of the BAS2 project was to study vulnerabilities in the telecommunication system and to suggest cost-effective measures to reduce these vulnerabilities. The analysis was conducted in four interlinked steps (Figure A.5.4):

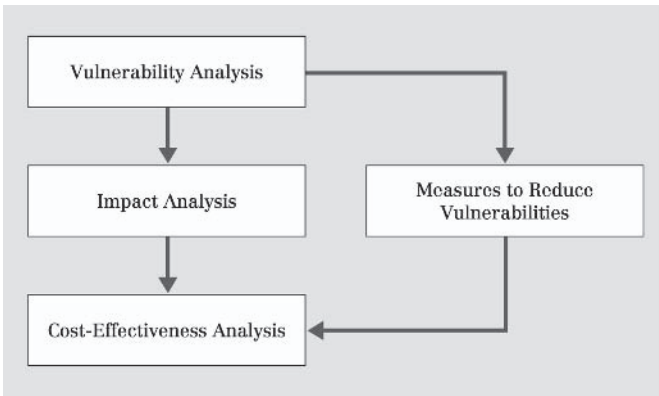


Figure A5.4. Steps of the Norwegian Vulnerability Analysis

In a first step, a *Vulnerability Analysis* was conducted. By using *Seminar Games*, BAS2 mapped the dependency of modern society upon telecommunication services in crisis and conflict situations. After this, an impact analysis was conducted. In a next step, measures that might reduce the vulnerabilities were evaluated. Eventually, the actual cost-effectiveness analysis was undertaken. Because no single method was able to handle all the problems, BAS2 had to use a combination of several techniques and methods to calculate the most cost-effective protection strategy for the telecommunication system<sup>8</sup>.

<sup>8</sup> The additional approaches used were seminar games; use of Scenarios, Causal Mapping, Fault Tree Analysis, Probabilistic Cost Estimation, and a Multi-Criteria Model. The Multi-Criteria Decision Approach systematically maps out subjective expert evaluations and combines them into a quantitative measure of effectiveness.



The *Multi-Criteria Decision Approach* involves structuring the problem in a multi-criteria hierarchy, where measures are linked to a top-level goal through several levels of decision criteria. The top-level goal is the overall objective of the system of analysis. In this process, the complex dynamic system to be analyzed is represented by a simplified linear, easily understandable model. Lower-level technical criteria are aggregated to wider, more general criteria in a rigid linear model<sup>9</sup>. The multi-criteria model used in BAS2 is a hierarchy with two interlinked parts. The top part of the hierarchy describes the “societal sub-system” of the analysis, while the lower part of the hierarchy describes the “technical sub-system”. The two sub-systems are connected, so that the top criteria in the technical sub-system are identical to the bottom criteria in the societal sub-system (Figure A.5.5). Maximizing the protection of society was defined as the top goal. The top goal was further distilled into three sub-criteria, which were: minimizing loss of life, minimizing economic losses, and minimizing the danger of a loss of sovereignty. These three sub-criteria were divided into more specialized sub-criteria (Figure A.5.6).

Creating a *Multi-Criteria Model* is an iterative process. One of the main problems in the design process was to determine, to the greatest extent possible, exclusive criteria that were independent of the other criteria on the same level in the hierarchy. Still, the design process was extremely useful for establishing a thorough understanding of the problems that were analyzed.

<sup>9</sup> The relationships between criteria at different levels can be quantified by experts expressing their subjective preferences of criteria, i.e. identifying the criteria they consider to be important for the success of the criterion on the level above. In other words, the experts *weigh* the different criteria in the model against each other, and the experts’ preferences serve as a measure of the *effectiveness* of one criterion compared to the others on the same level. The top goal of the hierarchy expresses the total effectiveness of the measures involved.

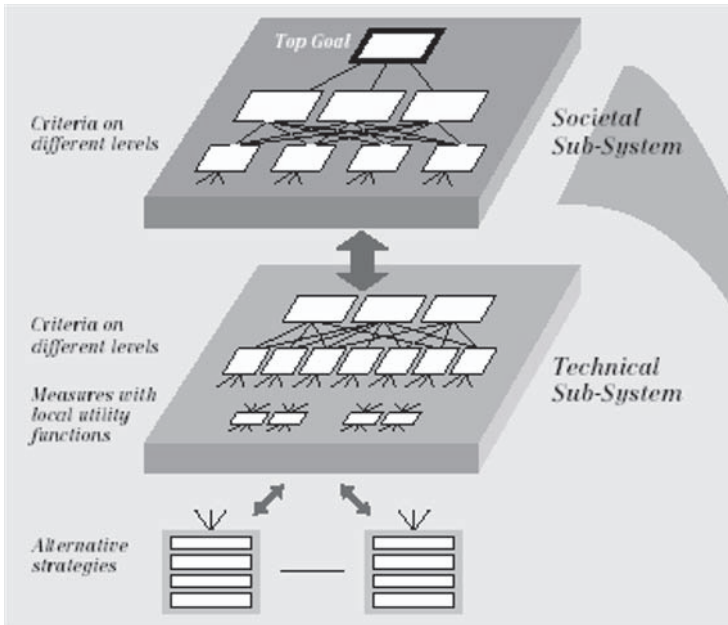


Figure A.5.5. Multi-Criteria Hierarchy

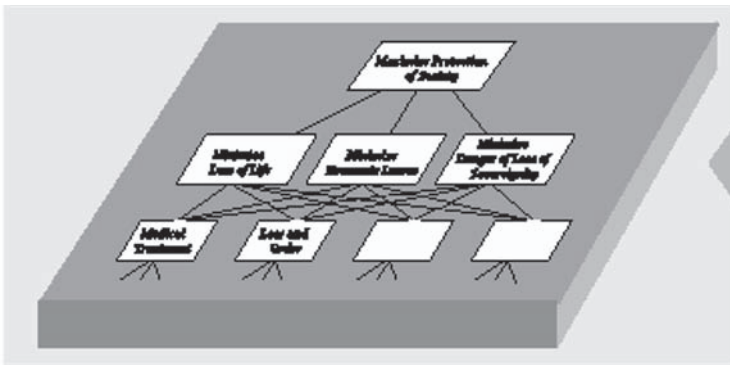


Figure A.5.6. Parts of the Social Hierarchy for the Multi-Criteria Analysis

**5 Switzerland – Swiss Roundtables Risk Analysis Methodology (Roundtables)**

Under the auspices of the *Swiss InfoSurance Foundation*, sector specific risk analysis round tables are conducted for ten sectors identified as critical. The methodology used for each of the sectors is a ten-step risk analysis approach as shown in Figure A.5.7.

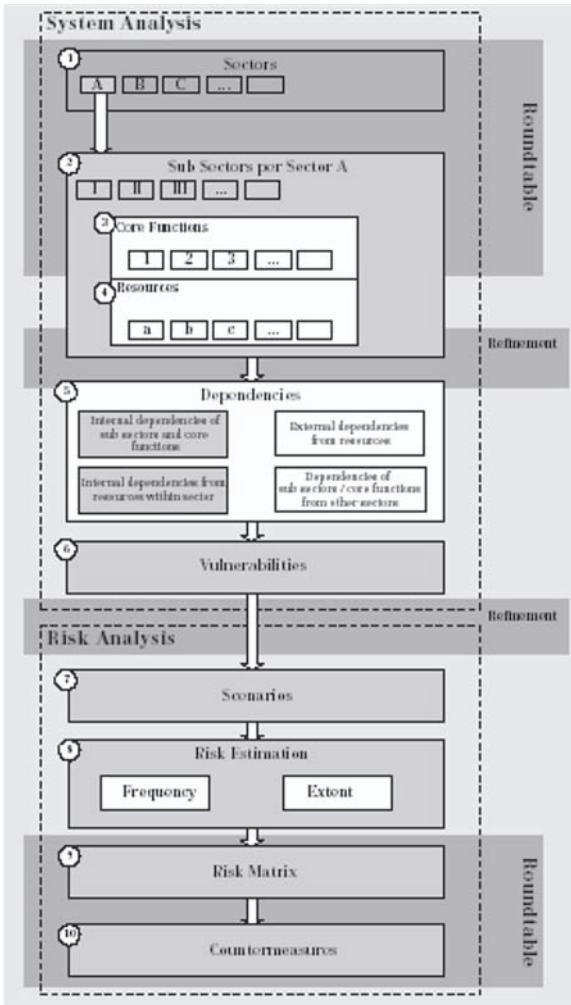


Figure A.5.7. Swiss Critical Sector Risk Analysis Approach

Four *Roundtables* that can be amended by working groups are planned for each sector. The processes can be divided into a system analysis and a risk analysis:

- The system analysis aims to gain an overview over structures, elements, and the dependencies in the respective sector (Steps 1-6).
- The risk analysis uses scenarios for identified weak points and focuses on them (Steps 7-10).

### **6 United Kingdom – NISCC Building Blocks (NISCC)**

The UK government's CIIP centre, the NISCC (*National Infrastructure Security Coordination Centre*), has developed a set of "building blocks" by asking a series of key questions in order to provide protective security advice efficiently. It is an ongoing process already initiated in the UK.

The information gained from these questions gives the NISCC a detailed insight into the protective measures and consequences of failure of these organizations and companies. In order to provide the interview partners with advice, recommendations, and information sharing opportunities, the NISCC assesses the following three points:

- What is the threat?
- How can the respective company improve its resilience?
- How can the sector improve its resilience?

Answers to these building block questions generate a 'map' of CII (networks and services), key organizations, and interdependencies. The information allows the NISCC to give the organizations feedback, including a set of recommendations to improve safety and security; vulnerability analyses on components or networks used by the organization; and a threat assessment based on intelligence and investigatory findings. These inputs allow the organization to manage more effectively their risk management for electronic attack protection.

#### **A.5.2.3 Threat Assessment**

As critical infrastructures deliver a range of services that individuals, and society as a whole, depend on, critical infrastructures are a favoured target for malicious attacks. Any damage to or interruption of critical infrastructures causes ripples across the technical and the societal systems—this principle held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure, therefore, has a "force multiplier" effect, allowing even a relatively small attack to achieve a

much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors<sup>10</sup>. On the side of the government, the ability to gauge threats to critical infrastructure has traditionally depended on the ability to evaluate the intent of an actor, coupled with the motivation and the capability to carry out the action. Threat assessment in the risk analysis sense includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, it should be kept in mind that terrorism is an actor-based threat that is intrinsically non-quantifiable.

#### A.5.2.4 Vulnerability Assessment

Vulnerability can be defined as susceptibility to injury or attack. It can be defined in the context of CIP/CIIP as “a characteristic of a critical infrastructure’s design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat”.

However, it may well be that vulnerabilities and infrastructure disruptions will not be traceable in any useful way to single technical subsystems – this could be due to a consequence of a overwhelming system complexity. The analysis of vulnerability should therefore be based instead on *functional units*, whose interactions with each other and with their environment can best be described by way of their societal manifestations as a whole, with less emphasis placed on technical issues. Additionally, threats and vulnerabilities must be seen as two sides of the same coin: As a threat-source does not present a risk when there is no vulnerability that can be exercised, as vulnerability on its own also does not represent a risk when there is no threat. Besides, especially when considering human threats, for example terrorism, a sole focus on vulnerabilities, sensible though it may be with respect to cost-benefit

<sup>10</sup> The US *Presidential Commission on Critical Infrastructure Protection* (PCCIP), for example, defines “threat” as a “foreign or domestic entity possessing both the capability to exploit a critical infrastructure’s vulnerabilities and the malicious intent of debilitating defence or economic security. A threat may be an individual, an organization, or a nation.” In publications on security of IT systems, threats are seen as the potential for a particular threat-source to successfully exploit a particular vulnerability, which means that a threat-source does not present a risk when there is no vulnerability that can be exercised. Threats do not necessarily need to originate from human sources, but can be natural, human, or environmental.

arguments, often implicitly assumes that terrorist actors will also recognize and identify the same infrastructures as priority targets – an assumption which might backfire.

### **A.5.2.5 Impact Assessment**

An isolated vulnerability and an isolated threat are not enough to cause harm or damage to CI/CII. Rather, the convergence of a threat with a specific vulnerability, combined with the possibility of a *harmful impact*, produces the risk. Such impacts are disruptive challenges of different types, durations, and levels of severity, and can be measured using different parameters such as economic loss or social and political damage. The term “impact” is also used interchangeably with the terms “harm”, “effect”, or “consequence”. Impact assessment is one step in the overall risk analysis process. The grade of possible harm to an asset must be determined by a number of experts familiar with the assets, be they executives (such as experts within the administration), asset owners, or asset managers. The adverse impact of a security event on IT-systems can be described in terms of loss or degradation of any, or several, of the *IT-Security Objectives*: integrity, availability, and confidentiality. Other impacts (e.g., loss of public confidence, loss of credibility, or damage to an organization’s interest) cannot be measured in specific units.

### **A.5.2.6 Analysis and Conclusion: Analysis of Methods and Models for Critical (Information) Infrastructure Assessment**

The need for assessment of CI is indisputable, and new vulnerabilities due to society’s dependence on CI are acknowledged. In order to plan adequate and cost-effective protection measures, the working of these systems and their role for society should be sufficiently understood. But such an understanding is not at all given today, mainly because the complex behaviour of infrastructure networks presents numerous theoretical and practical challenges for various stakeholders<sup>11</sup>. Generally

<sup>11</sup> Each of the methods and models used for the assessment of CI can only be applied to certain limited aspects of the problem, meaning that no single one is sufficient to address the whole range of issues. This requires a combination of different methodological elements, as shown in the patchwork application and multi-step approaches used in certain countries. Additionally, only few approaches have been developed for the purpose of analyzing CI specifically.

speaking, current methodologies for analyzing CI are insufficient in a number of ways: One of the major shortcomings is that the majority of them do not pass the “interdependency test”. In other words, they fail to address, let alone understand, the issue of interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic, security-related, and economic importance of CI. Furthermore, one of the main difficulties facing risk analysis involves the theoretical and practical difficulties of estimating the probabilities and consequences of low-probability high-impact events – since no useful statistics for possible damage and failure probabilities exist. It also appears that there is no way of cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way. Additionally, risk analysis clearly does not pass the “interdependency test”. CIP efforts currently face one major problem: Protection is aimed at the present status of existing CI – and thus always lags one step behind. This is problematic as a lot of the challenges and problems are only just emerging, so that the system characteristics of future information infrastructures will differ fundamentally from traditional structures. Understanding them will require new analytical techniques and methodologies that are not yet available. Their development will, in turn, require great efforts in unconventional and forward thinking.

### **A.5.3 Assessing Critical Infrastructures**

An assessment of approaches for analyzing various aspects of critical infrastructures is very enlightening. For fourteen countries, such approaches have been compiled in a recent publication<sup>12</sup>. In effect, the methodological toolbox can serve as an indicator of the current understanding of key issues. However, the huge variation in the granularity of methods and models used to analyze and evaluate aspects of the CI in the surveyed countries makes a meaningful comparison rather difficult. This means that most of the approaches can only be applied to certain limited aspects of the problem. Examples of such patchwork applications include sector analysis; interdependency analysis; risk analysis; threat assessment; vulnerability assessment; or impact assessment.

<sup>12</sup> Dunn, I. Wigert –“ Critical Information Infrastructure Protection. – Handbook 2004”, ETH Zürich, Switzerland, 2004

### **A.5.3.1 Sector Analysis**

There are many aspects that might be analyzed in connection with individual sectors, such as how and why they are critical, or what parts of it are particularly vulnerable, etc. In general, sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects such as underlying processes, stakeholders, or resources needed for crucial functions. Sector analysis is a basis for better understanding the larger, complex infrastructure systems. However, sector analysis on its own remains insufficient for a holistic understanding of the larger infrastructures system at hand. Even more, the division of the whole system into sectors is rather artificial and serves a more practical purpose. It is a need stemming from the fact that infrastructures are mainly owned and operated by private actors, so that the only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. It is therefore necessary for a meaningful analysis to evolve beyond the conventional 'sector'-based focus, since, for example, in the case of terrorist attack the key elements within an infrastructure are more likely targets than entire sectors. It makes more sense to categorize targets in terms of their inherent function – e.g., the supply of raw material, distribution nodes, or command and control centres.

### **A.5.3.2 How to Specify Characteristics of Critical Sectors**

The determination of how critical sectors function, what the influencing parameters are in particular sectors, how important specific sectors are to the economy, and who the major players are, including the identification of core functions, value chains, and dependency on information and communication technology in each critical sector, is a prerequisite for subsequent interdependency analysis. Most critical sectors have different structures and requirements, so that the appropriate level of detail might vary considerably from sector to sector. They can, for example, be subdivided into industries, into services, into products, or combinations of the various subdivisions. Different industries require different approaches to consulting experts. In some industries, workshops can produce rapid and valuable results, while in other, personal interviews might be necessary.



### A.5.3.3 Interdependency Analysis

Critical infrastructures are frequently connected at multiple points through a wide variety of mechanisms, so that bi-directional relationships exist between the states of any given pair of infrastructures. This means that CI are highly interdependent, both physically and in their greater reliance on the information infrastructure, resulting in a dramatic increase of the overall complexity and posing significant challenges to the modelling, prediction, simulation, and analysis of CI. The information infrastructure plays a crucial role, as most of the critical infrastructures are either built upon or monitored and controlled by ICT systems, a trend that has been accelerating in recent years with the explosive growth of information technology.

An *Interdependency* can be understood as a “bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.” A *Dependency*, on the other hand, is a unidirectional relationship<sup>13</sup>. The study of systems interdependency, and possible cascading effects in case of failures have become the focal point of research, due to the explosive growth of information technology. Interdependency analysis looks to gain a better understanding of the complex (bi-) directional relationships between infrastructure components, subsystems, systems, and/or sectors.

### A.5.4 Digitalization

In today’s digital world, technology failures are matters of public interest, not something that can be ignored in the hope that nobody will notice, care or understand. Today’s computer networks and digital systems are large, complex and occasionally fragile. The interconnectedness that let

<sup>13</sup> A comprehensive analysis of interdependencies is a daunting challenge, though, mainly because the science of infrastructure interdependencies is relatively immature. There are many models and computer simulations for aspects of individual infrastructures, but simulation frameworks that allow the coupling of multiple interdependent infrastructures to address infrastructure protection, mitigation, response, and recovery issues are only beginning to emerge. The operational, R&D, and policy communities have accepted the importance of infrastructure interdependencies and the need to better understand their influence on infrastructure operations and behaviour.

us transfer energy and information over large distances, also gives us a degree of instability and unpredictability that we cannot design out of the systems. By dealing with such networks of generators and transmission lines this is in fact the network equivalent of the well known Gödel's Theorem which indicate that *any system sufficiently complex to be useful is also able to collapse catastrophically*. In practical terms, following blackouts or network failures, we need a full report on what went wrong and what was done to fix it, as well as a planning action term to be followed. It would be unacceptable for any of the parties involved to hide behind commercial confidentiality or even parliamentary privilege. When a major system collapses, we need to know what went wrong and what is being done differently. According to modern rules of governance, anything less is a betrayal of public trust.

#### **A.5.4.1 Critical infrastructure complexity and management of vulnerability**

It is evident that the insurance of high service reliability has become much more challenging. Rather than being a product of individual organizations, highly reliable services are more and more the outcome of networks of organizations, many with competing goals and interests. This creates new challenges for effective market and network regulation and new needs for communication and information sharing. The California crisis could have been a lot worse than it was if the operators of the various subsystems had communicated less intensively.

Overall demand for infrastructure services is increasing. At the same time, society demands ever higher reliability of service as we grow more dependent on infrastructure bound services. By lack of options to directly interfere in the development of the physical system, we can only ensure that the collective actions of players are steered towards the public interests through adequate innovative market design, adequate network regulation (if the network retains its monopoly character) and additional legislation and regulation for safety, health, environment, etc. A specific challenge is to ensure that the design of markets and regulatory frameworks generate sufficient investment signals to stimulate private actors to timely invest in infrastructure development and innovation.

#### A.5.4.2 Varying Policy Responses to Critical Information Infrastructure Protection (CIIP) in European Countries<sup>14</sup>

The critical infrastructures of modern society rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. These software-based control systems underpin many elements of the CI, as many information and communication technologies have become all-embracing, connect other infrastructure systems, and make them interrelated and interdependent. These infrastructures are the so-called **critical information infrastructure (CII)**<sup>15</sup>. However, CIP and CIIP cannot and should not be discussed as completely separate concepts, as CIIP is an essential part of CIP. An exclusive focus on cyber-threats that ignores important, traditional physical threats is just as dangerous as the neglect of the virtual dimension – what is needed is a sensible handling of both interrelated concepts.

While information systems offer many opportunities, they are at the same time exposed to failure and susceptible to cascading effects as well as potential targets for malicious attacks. As a result, within the last few years, many developed countries have taken steps to better understand the vulnerabilities of and threats to their CII and have drafted possible

<sup>14</sup> For a detailed presentation of selected European countries see the monograph by Dunn, I. Wigert –“Critical Information Infrastructure Protection. – Handbook 2004”, ETH Zürich, Switzerland, 2004

<sup>15</sup> A clear and stringent distinction between the two key terms “CIP” and “CIIP” has not yet been achieved. In government papers and official publications, both terms are used inconsistently, with the term CIP frequently used even if the document is only referring to CIIP. This is not due to a lack of accuracy or random use of the two concepts. Rather, the parallel use of terms reflects the stage of political discussion in different countries and points to the deficiencies in understanding conceptual differences between the concepts. What is the relation between CIP and CIIP? While CIP comprises all critical sectors of a nation’s infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on the critical *information* infrastructure. The definition of exactly what should be subsumed under CI, and what under CII, is another question: Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country’s critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with the information and telecommunications sector, and includes components such as telecommunications, computers/ software, the Internet, satellites, fibre-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

solutions for the protection of these critical assets. It became clear that effective measures, policies and organizational arrangements are needed inside and across countries to face these new risks and threats.

Looking at European selected countries it becomes clear that there are various ways to approach these new challenges. CIIP can be seen as mainly a

- The *system-level, technical perspective*:<sup>16</sup>
- The *business perspective*:<sup>17</sup>
- The *law-enforcement perspective*:<sup>18</sup>
- The *national-security perspective*:<sup>19</sup>

For a comprehensive approach to CIIP, all these various perspectives and issues should be considered. Therefore interdisciplinary approaches, also taking into account the politically motivated actor's perspective (which is often neglected in risk analysis) are promising.

#### **A.5.4.3 Addressing the issue of CIIP at the government level: a challenging task**

The development of the Internet, a global network that is often perceived to be inherently insecure, into the main pillar for the

<sup>16</sup> CIIP is approached as an IT-security or information assurance issue, with a strong focus on Internet security. In this view, threats to the information infrastructure are to be confronted by technical means such as firewalls, anti-virus software, or intrusion detection software. The establishment of so-called Computer Emergency Response Teams (CERTs) and similar early-warning approaches in various countries is an example of this perspective.

<sup>17</sup> CIIP is seen as an issue of "business continuity", especially in the context of e-Business. This requires not only permanent access to IT infrastructures, but also permanently available business processes to ensure satisfactory business performance. The means of achieving this coincide, by and large, with the ideas of the technical community outlined above; however, the focus is not solely on the system level, but includes organizational and human factors. This perspective is also reflected in some countries' protection approaches that mainly aim to support the Information Society.

<sup>18</sup> CIIP is seen as an issue of protecting society against (cyber-) crime. Cyber crime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and including issues such as infringements of copyright, computer fraud, child pornography, and violations of network security.

<sup>19</sup> Usually, the whole of society is perceived as endangered, so that action is taken at a variety of levels (e.g., at the technical, legislative, organizational, or international levels), and the actors involved in protection efforts include government officials from different agencies, as well as representatives of the private sector and of the general public.

advancement of the information society, including e-Government, e-Commerce and so on, was in many cases a catalyst for governments for national protection efforts, sometimes under the heading of CIIP, sometimes under the more general banner of information security.

While the need to protect the CII is recognized, there are a wide variety of different CIIP approaches that make cooperation between governments and private industry or across countries sometimes difficult. This variety reflects the different threat perceptions as well the country-specific peculiarities and traditions, which lead to different CIIP policies. In most countries CIIP is seen as a subset of CIP, including protection, detection, response, and recovery activities at both the physical and the cyber level.

### A.5.5 Conclusion

Today's critical information infrastructures are getting increasingly complex at several levels. Their *physical networks* consist of a growing number of components that are becoming more and more sophisticated. The complexity of the *social networks* is growing because of, e.g., liberalization and internationalization, which both lead to a larger number of players in the field with an increasing number of dependencies. These developments lead to a far more complex *socio-technical* network. Additionally, infrastructures get more and more *interconnected* because of, for instance, mutual dependence (as in the case of the energy and communication sectors), or market substitution. The increasing complexity and interdependence at these four levels may result in higher risk levels, as failures in one sector can easily affect other sectors. An overview of *risk analysis processes* in various countries shows the diversity of approaches that are used. In the special case of the information infrastructure, which is used in all other infrastructures for operation and control, there is no uniformity either. An analysis shows that the approach to *critical information infrastructure protection* varies widely among countries.

## Appendix 6

# Critical Information Infrastructure Protection – Organizational and Legal Aspects

*Myriam Dunn, Isabelle Wigert, Adrian Gheorghe*

### A.6.1 Critical Information Infrastructure Protection (CIIP)

#### A.6.1.2 Approaches in Selected European Countries

While the need to protect the CII is recognized in most countries, the various stakeholders at government level are organized differently.<sup>1</sup> In a few countries such as Canada (with the Public Safety and Emergency Preparedness Canada<sup>2</sup>), Germany (with the Federal Office for Information Security, BSI<sup>3</sup>), New Zealand (with the Centre for Critical Infrastructure Protection, CCIP<sup>4</sup>), Sweden (with the Swedish Emergency Management Agency, SEMA<sup>5</sup>), the United Kingdom (with the National Infrastructure Security Co-ordination Centre, NISCC<sup>6</sup>) or the United States (with the Department of Homeland Security, DHS<sup>7</sup>) central governmental organizations have been created to deal with CIIP, specifically. Yet in most other countries the trend to an interagency approach can be identified,

<sup>1</sup> A comprehensive overview can be found in: Dunn, Myriam/ Wigert, Isabelle. *The International Critical Information Infrastructure Protection (CIIP) Handbook*. Zürich: Forschungsstelle für Sicherheitspolitik, 2004.

<sup>2</sup> <http://www.ocipep.gc.ca>.

<sup>3</sup> <http://www.bsi.de/english/index.htm>.

<sup>4</sup> <http://www.ccip.govt.nz>.

<sup>5</sup> <http://www.krisberedskapsmyndigheten.se/english/index.jsp>.

<sup>6</sup> <http://www.niscc.gov.uk>.

<sup>7</sup> [http://www.dhs.gov/dhspublic/theme\\_home1.jsp](http://www.dhs.gov/dhspublic/theme_home1.jsp).

as the responsibility for CIIP rests with more than one authority and with organizations in different governmental departments. And in most developed countries public-private partnerships (PPP) are becoming a strong pillar of CIIP policy. The following is a short overview of country-specific findings with regard to the organizational structure of CIIP in selected European countries on the government level.<sup>8</sup> For instance in France, Germany, Sweden and the United Kingdom central agencies with overall responsibility in the field of CIIP have been established:

- In **France**, CIIP is seen both as a high-tech crime issue and as a matter of developing the information society. Overall responsibility for CIP and CIIP lies with the General Secretary of National Defense (SGDN), a service attached to the Prime Minister's Office. The SGDN promotes and co-ordinates the activities between ministries involved in CIIP. Furthermore, within the Ministry of Defense, the Direction for Security of Information Systems, (DCSSI), Inter-Ministerial Commission for the Security of Information Systems (CISSI), and the Advisory Office are the key organizations responsible for CIP/CIIP, whereas in the Ministry of Interior, the Central Office for the Fight Against Hi-Tech Crime plays a comparative lead role.<sup>9</sup> The DCSSI administers the Security of Information Systems (SSI) website and co-ordinates its activities. The SSI website comprises information on the Computer Emergency Response Team (CERTA),<sup>10</sup> information on regulation, certification, authorization, electronic signature, and cryptography, and provides technical advice.<sup>11</sup>
- In **Germany** the Federal Office of Information Security (BSI), which is part of the Ministry of the Interior, is the lead authority for CIIP matters within the organizational structure. The BSI deal with all areas related to security in cyberspace and takes preventive action in the form of analyzing IT weaknesses and developing protective measures. As the government agency responsible for ensuring Germany's internal security, the Federal

<sup>8</sup> A comprehensive overview can be found in: Dunn, Myriam/ Wigert, Isabelle. *The International Critical Information Infrastructure Protection (CIIP) Handbook*. Zürich: Forschungsstelle für Sicherheitspolitik, 2004.

<sup>8</sup> <http://www.ssi.gouv.fr/fr/index.html>

<sup>9</sup> <http://www.bsi.bund.de/english/index.htm>

<sup>10</sup> Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques: <http://www.ssi.gouv.fr/fr/index.html>.

<sup>11</sup> <http://www.ssi.gouv.fr/fr/index.html>.

Ministry of the Interior (BMI) is closely involved with CIP/CIIP.<sup>12</sup> This is where the relevant topics are dealt with and coordinated, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. Other key players in the field of CIP and CIIP in Germany include the Federal Office for Civil Protection and Disaster Response (BBK), responsible for developing measures to improve physical protection<sup>13</sup>, the Federal Bureau of Criminal Investigation (BKA)<sup>14</sup> and the Federal Ministry of Economics and Labor (BMWA)<sup>15</sup>, playing a role with regard to the energy sector and developing the framework for securing the energy supply.

- **In Sweden**, a number of organizations are involved in CIP/CIIP. The Swedish Emergency Management Agency (SEMA) at the Ministry of Defense has a key role and coordinates work on the preparedness of society for major crises and war. SEMA analyzes the development of society, and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors. The agency also coordinates and initiates research and development in the emergency management area and has overall governmental responsibility for information assurance in Sweden. Within SEMA, the Information Assurance Department mainly manages the latter task, while the Research and Analysis Department handles the former task.<sup>16</sup>
- In the **United Kingdom**, the main responsibility for CIIP lies with the Home Secretary.<sup>17</sup> However, a number of other departments play a role in the protection of the various critical sectors and contribute resource and expertise to the British CIIP effort. These contributions are coordinated by an interdepartmental center that reports to the Home Office – the National Infrastructure Security Co-ordination Centre (NISCC). Policy is formulated and

<sup>12</sup> [http://www.bmi.bund.de/dokumente/Artikel/ix\\_93830.htm](http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm)

<sup>13</sup> [http://www.bmi.bund.de/Annex/de\\_25112/Gesetzentwurf\\_fuer\\_die\\_Einrichtung\\_des\\_Bundesamtes\\_fuer\\_Bevoelkerungsschutz\\_und\\_Katastrophenhilfe.pdf](http://www.bmi.bund.de/Annex/de_25112/Gesetzentwurf_fuer_die_Einrichtung_des_Bundesamtes_fuer_Bevoelkerungsschutz_und_Katastrophenhilfe.pdf).

<sup>14</sup> <http://www.bka.de>.

<sup>15</sup> <http://www.bmwa.bund.de>.

<sup>16</sup> [http://www.krisberedskapsmyndigheten.se/defaultEN\\_\\_\\_224.aspx](http://www.krisberedskapsmyndigheten.se/defaultEN___224.aspx)

<sup>17</sup> <http://www.homeoffice.gov.uk/terrorism/govprotect/infrastructure/index.html>.



developed at a working level through a dialog between several government departments and bodies: the NISCC; the Central Sponsor for Information Assurance (CSIA); the Civil Contingencies Secretariat (CCS); the Cabinet Office Security Policy Division; and the Home Office itself. NISCC coordinates and develops existing work within government departments and agencies as well as CI organizations in the private sector and has strong ties with the private sector and the intelligence community.

In other European countries there is no main governmental central organisation dealing with CIP and CIIP, but rather a number of different organizational units. Here are some examples:

- In **Austria**, there is no single authority responsible for CIP/CIIP – all ministries have their own specific security measures to defend against outside attack and to prevent the unauthorized usage of data. CIIP is mainly perceived as an *issue of data protection*, the Austrian E-Government Program, the Official Austrian Data Security Website, or the Pilot Project Citizen Card indicates.
- In **Finland**, CIIP is seen as a data security issue and as a matter of economic importance, closely related to the development of the Finnish information society. Several organizations deal with CIIP, including the Finnish Communications Regulatory Authority (FICORA), the Emergency Supply Agency (NESA), the Board of Economic Defense, and the Committee for Data Security. NESA is the cross-administrative operative authority for the security of supply in Finland. NESA serves to develop co-operation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply. NESA has a growing role in assuring the critical national infrastructure by developing and financing the technical backup system. FICORA's mission is to promote the development of the information society in Finland, which includes issuing technical regulations and the co-ordination of standardization work at the national level. Another task of FICORA is to ensure that the telecommunications operators are prepared for emergencies. The operators must report to FICORA significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services.<sup>18</sup>

<sup>18</sup> FICORA. *Annual Report 2001*, p. 74: [http://www.ficora.fi/2001/VV\\_vsk2001.pdf](http://www.ficora.fi/2001/VV_vsk2001.pdf).

- In **Italy**, CIIP is part of the advancement of the information society. There is no single authority dealing with CIIP. A Working Group on CIIP was set up at the Ministry for Innovation and Technologies that includes representatives of all ministries involved in the management of critical infrastructures and many Italian infrastructure operators and owners as well as some research institutes. The Ministry for Innovation and Technologies<sup>19</sup> is charged with promoting specific action plans and programs for the deployment of information technologies in order to improve governmental online services for citizens and business.
- In the **Netherlands**, responsibility for CII lies with a number of authorities, but the Ministry for Interior and Kingdom Relations coordinates CIP/CIIP policy across all sectors and responsible ministries. The Ministry of Economic Affairs/Telecom and Post Directorate is responsible for the protection policy for telecommunications and the Internet. Other parts of the same ministry are responsible for CIP/CIIP policies regarding the energy sector and private industry, including SMEs. The Ministry of the Interior is responsible (in terms of policy) for the protection of government information infrastructures and coordinates CIP policy across all sectors and responsible ministries.
- In **Norway**, the national key player in Civil Emergency Planning, the Directorate for Civil Defense and Emergency Planning (DSB), subordinated to the Ministry of Justice and Police, is also a key player for CIP/CIIP-related issues. The coordinating authority on the civilian side is the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Trade and Industry, while the Ministry of Defense is responsible on the military side. The Ministry of Transport and Communications has responsibility for the communication sector in Norway, including all related security issues. Directorates and authorities that are responsible for handling the different sides of CIIP on behalf of the ministries are subject to the respective ministries.<sup>20</sup> A Unit on Telecom Infrastructure Security has been established at the Post and Telecommunications Authority.

<sup>19</sup> <http://www.innovazione.gov.it/eng/index.shtml>.

<sup>20</sup> Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

- In **Switzerland**, there are a number of different governmental departments and organizational units dealing with CIP/CIIP. One of the main bodies is the Federal Strategy Unit for Information Technology (ISB)<sup>21</sup>, subordinated to the Swiss Federal Department of Finance (EFD). A key authority of the Swiss CIIP early warning system will be the Reporting and Analysis Center for Information Assurance (MELANI), set up by ISB, as well as the Special Task Force on Information Assurance (SONIA), as a central crisis management organization. Public-private partnerships are among the central pillars of Switzerland's CIIP policy. The most prominent example of a body promoting cooperation between industry and public administration is the InfoSurance Foundation.<sup>22</sup>

*Early warning* is perceived as one of the key CIIP issues in most countries. Computer Emergency Response Teams (CERTs) as well as Information Sharing and Analysis Centres (ISACs) play an increasingly important role. In some countries, *permanent analysis and intelligence centers* have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sector. Many countries reviewed their CIIP policies and legislation as a result of September 11, 2001 event. The development of effective regulations, laws, and criminal justice mechanisms are seen as essential in deterring cyber-abuse and other offences against information infrastructures.

Like many political leaders, business leaders tend to view cyber-attacks on infrastructures as a tolerable risk. Additionally, public-private partnerships are mainly based on trust, so that information-sharing is arguably one of the most significant issues in CIIP.

One of the future challenges in many countries will be to achieve a *balance between security requirements and business efficiency imperatives*. *Satisfying shareholders by maximizing company profits has often led to minimal security measures*.

<sup>21</sup> <http://www.isb.admin.ch/internet>.

<sup>22</sup> The Foundation for the Security of Information Infrastructure in Switzerland. See <http://www.infosurance.ch>.

### A.6.1.2 The European Union and CIIP

CIIP, the Information Society, and Information Security are key issues for the European Union (EU). The EU is supporting these issues and investigating them by:

- Considering its various aspects and impacts on citizenship, education, business, health, and communications
- Supporting relevant programs and initiatives, such as the eEurope Action Plan, Information Society Technologies Research, eContent, eSafety, the Internet Action Plan, etc.<sup>23</sup>

The action plan “eEurope 2005: An Information Society for all” was adopted in June 2002. It is an extension of the successful “eEurope 2002” initiative.<sup>24</sup> With the “eEurope 2005” initiative, the EU clearly recognizes information security to be more than a purely technological challenge. The EU states that information security is mainly dependent on human behaviour, on the knowledge of threats, and on the management of these threats. Hence, the social and political aspect of information security is stressed. Since information security embraces a number of policy fields such as privacy, civil rights, law enforcement, international trade, and defence, the EU promotes a “holistic approach” concerning CIIP.<sup>25</sup> This means that an effective CIIP approach depends on the cooperation of all actors involved (public, private, individual) and on a multi-dimensional approach to establishing protective measures (including technical aspects, social and political aspects, and legal aspects).

The European Network and Information Security Agency, ENISA, came into being on 15 March 2004. This key agency in the field of CIIP has advisory and coordinating functions concerning data-gathering and data analysis on information security. Furthermore, the agency serves as a centre of expertise and excellence for the EU member states and EU institutions. The agency helps to establish broader cooperation between the key players and to ensure the interoperability of networks and information systems by promoting security standards.<sup>26</sup> On 20 October 2004 the Commission of the European Communities released a Communication on

<sup>23</sup> [http://europa.eu.int/information\\_society/index\\_en.htm](http://europa.eu.int/information_society/index_en.htm).

<sup>24</sup> <http://www.e-europestandards.org>.

<sup>25</sup> [http://europa.eu.int/information\\_society/europe/2005/all\\_about/security/print\\_en.htm](http://europa.eu.int/information_society/europe/2005/all_about/security/print_en.htm).

<sup>26</sup> [http://www.enisa.eu.int/index\\_en.htm](http://www.enisa.eu.int/index_en.htm).

“Critical Infrastructure Protection in the fight against terrorism”.<sup>27</sup> In there a European Programme for Critical Infrastructure Protection (EPCIP) is announced, that should seek to assist industry and Member States Governments at all levels in the EU, while respecting individual mandates and accountabilities. Moreover, as soon as possible in 2005 a Critical Infrastructure Warning Information Network (CIWIN) should be set up in order to stimulate an exchange of information on shared threats and vulnerabilities as well as appropriate measures and strategies to mitigate risk in support of CIP.

<sup>27</sup> Commission of the European Communities. Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the fight against terrorism. Brussels, 20. 10. 2004. COM(2004)702final.

## Appendix 7

### Profiling the Risk Governance Gap

*Caroline Künzi*

#### A.7.1.1 Risk Profiling

Based both on the previous discussion of the socio-economic context of the European electric power system as well as on the outline of risk governance as a way of achieving solutions (i.e. a heuristic tool), it is possible to set up a ‘risk governance profile’ indicating where and to what extent the governance of the risks affecting the European electric power system has gaps. While such a profile visualises the features of a particular risk or problem area, it equally allows for the identification of the governance problems associated with it and, eventually, for an easy comparison of the major differences between risks.

To establish the profile, a risk needs to be investigated in the context of a range of criteria which influence the governance of a risk to such an extent that they can serve as indicators of its status and quality<sup>1</sup>. These

<sup>1</sup> A separate IRGC project investigates ‘basic concepts of risk characterisation and risk governance’ and aims to consolidate this knowledge into an ‘analytic framework’ – a set of guidelines for improving the governance of risks across a variety of risk areas and socio-political cultures. A prototype of this framework is outlined in an IRGC White Paper which will be published in the second half of 2005 (principle author and project leader: Ortwin Renn). The criteria used to develop the risk governance profile described here are part of that analytic framework, which, in the following, is briefly explained.

The framework’s component parts include, on the one hand, the classical means of framing, assessing, evaluating and managing risk which, if combined in a logically compelling sequence, comprise a model risk process. This process is iterative and has risk communication as a companion to all other steps of the process cycle. A crucial element of the guidance in this respect proposes a set of criteria incorporating key risk characteristics and, based on which characteristic is dominant, derives different risk management strategies.

criteria can be bundled around four main issues: how a risk is framed, how it can be described, how the defence or control and co-ordination mechanisms are shaped, and how it can be rated in terms of wider implications.

During the profiling one establishes for each of the criteria how the risk scores on a scale of five discrete parameter values. For some criteria, the scale offers the traditional range of low, low to medium, medium, medium to high, high; for others the scale uses different descriptors while retaining the main idea of having five gradually changing values – or ‘intensities’ – along a spectrum with two clear poles. All of these different scales are threaded by a unifying concept or, in fact, an assumption: the more towards the right pole a risk scores, the higher is the presumable gap in risk governance assumed to be and, consequently, the bigger is the need for corresponding remedial study as well as specific risk governance measures. Vice versa, the closer a risk is to the left pole, the better risk governance seems actually handled. Under an alternative interpretation and

---

Equal importance is, on the other hand, given to contextual aspects which, as they are the basic conditions of any risk-related decision-making, bear strongly on the outcome of any effort to address and deal with risk. Contextual aspects include:

- the structure and interplay of the different actors dealing with risks as well as the institutional and legal background within which they operate (governance structure);
- the different ways in which actors may view risk (risk perceptions);
- the policy-making or regulatory style prevalent within the entities and institutions having a role in the risk process (political culture);
- the organisational assets and capacity needed for effective risk governance.

Beyond the classic component parts of a risk process as well as the contextual or cultural aspects of risk, the framework contains a number of value-based or normative premises. These premises obviously also have their part in shaping the recommendations and strategies resulting from the framework’s application. They include:

- the conviction that a balance needs to be achieved between considering both the physical and the social characteristics of a risk;
- the need to ensure early and meaningful involvement of all stakeholders and, in particular, civil society;
- an acknowledgement of the important role of risk-benefit evaluation and the existence of risk-risk trade-offs;
- a commitment to explore the possibilities and limits of the self-regulatory power of ‘market forces’ and to engage in the search of innovative ways of risk coverage (including insurability and supranational liability regimes);
- the need for the framework to implement the principles of ‘good governance’;
- the understanding that, while it is necessary to know and properly accommodate the risks related to emerging technologies, innovation and progress must not be stifled.

depending on the risk's features, this case could also indicate that the risk under question is not an issue of risk governance, meaning that it can be dealt with by adopting single measures, the design and implementation of which does not require significant interaction beyond the boundaries of the organisation or institution in charge.

The below template (see Figure A.7.1.) gives an overview of the criteria to be investigated and their corresponding scales and illustrates the 'mechanism' of such risk governance profiling, which, eventually, concludes with 'linking the dots'. Both the criteria and the scales are briefly explained in the following.

### **Risk Framing**

The criteria in this category take into account the fact that risk, by and large, is a mental construct which per se can have different meanings to different people. These criteria, in summary, look at how a particular problem or circumstance comes to be seen as a risk by a majority of stakeholders:

- Risk scope: What is a risk's 'catchment area': Does the risk affect a local community solely or does it affect us on such a scale that an adequate response has to be organised on a national or regional level? Is the risk international in that it affects a wide range of countries or is it even globally relevant?
- Risk perception: What do stakeholders and society select and interpret as risk? Are their views and perceptions about what constitutes a risk convergent, tending to converge, mixed, tending to diverge or divergent?
- Public awareness: Is the general public conscious of a particular risk or problem area? Is their awareness high, high to medium, medium, medium to low, low?



## Risk Governance Profiling Template

Characteristics		Scale of Governance Gap					
		low	←————→			high	
Framings	Risk scope	local	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	global
	Risk perception	convergent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	divergent
	Public awareness	high	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	low
Risk Characterisation	Probability	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Damage potential	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Ubiquity of damage	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Persistence of damage	short	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	long
	Reversibility of damage	high	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	low
	Delay effects of damage	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Level of complexity	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Level of uncertainty	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Level of ambiguity	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Impact on equity	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Public concern	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Coordination & Control	Responsibilities pattern	clear	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regulatory basis		sub-national	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	international
Binding rules		binding for system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none
Level of compliance		high	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	low
Regulation adequacy		high	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	low
International co-operation		fully functional	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	not existing
Stakeholder participation		full engagement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no engagement
Further Implications	Impact on global free trade	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Impact on business	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Impact on actors' power	low	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	high
	Insurability	fully given	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none
	Technology change	incremental	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	break-through

Figure A.7.1. Risk profiling template

### Risk Characterisation

This category comprises of a number of criteria by which risk can be characterised. In doing so, risk is considered in two dimensions – a ‘factual’ dimension which comprises physically measurable characteristics or outcomes (i.e. risk as a combination of potential damage and probability of occurrence) and a ‘socio-cultural’ dimension, which includes how a particular risk is viewed when values and emotions come into play:

- Probability of occurrence: Is the relative frequency of the risk occurring estimated to be low, low to medium, medium, medium to high, high?
- Damage potential: Is the potential for adverse effects (measured in natural units such as death, injury, production loss, service loss, environmental degradation, destruction with regard to the built environment) low, low to medium, medium, medium to high, high?
- Ubiquity of damage: Is the geographical dispersion of the damage considered to be low, low to medium, medium, medium to high, high?
- Persistence of damage: Is the damage going to last for a short time, short to medium time, medium time, medium to high time, high time when ‘short’ depicts a few hours or days and ‘long’ is a code for a full generation (i.e. 25 years and more)?
- Reversibility of damage: Can the damage be reversed or undone? Is reversibility high, high to medium, medium, medium to low, low?
- Delay effects of damage: Is there a time delay between the triggering event which causes a risk to realise and the actual damage? Is the delay low, low to medium, medium, medium to high, high?
- Level of complexity: How difficult is it to establish precise cause/effect relationships between agents or triggering events and observed adverse effects? Is complexity low, low to medium, medium, medium to high, high?
- Level of uncertainty: Are we facing uncertainty in knowledge, in modelling complex systems or in predicting a risk as a result of its assessment? Is such uncertainty low, low to medium, medium, medium to high, high?

- Level of ambiguity: How many alternative interpretations of the results of risk assessment are there which must be considered both meaningful and legitimate? Is the level of such interpretative differences low, low to medium, medium, medium to high, high?
- Impact on equity: Is there a violation of equity between those stakeholders and members of the general public benefiting from a risk being taken and those affected by its potential damage? Are particular subsets of the general public such as children, women or the elderly particularly vulnerable – i.e. is there discrimination in how a risk affects people? Thus, is the impact on equity to be considered low, low to medium, medium, medium to high, high?
- Public concern: What is a risk's broad social impact – will it arouse social conflict or outrage? Does it have a potential for mobilising people? Is the degree of public concern low, low to medium, medium, medium to high, high?

### Control and Co-ordination

The criteria summarised here directly address some of the core issues of risk governance since they look at responsibilities, mechanisms of control and co-ordination as well as participation:

- Responsibilities pattern: Who is responsible for what with regard to risk-related decision, the way they come about and their actual implementation? Is the responsibility shared between different groups of stakeholders and, if yes, how is the interplay between them? Are such responsibility patterns clear (and well established), mostly clear, partially clear, mostly unclear, unclear (and not or barely established)?
- Regulatory basis: Judging from the nature and characteristics of a risk, on what hierarchical level of governance is the risk to be 'regulated'<sup>2</sup>? Is the natural regulatory base sub-national, national, bi-national or tri-national, regional, international?
- Binding rules: Are there binding and enforceable rules such as laws, regulations, multilateral contracts etc on how to deal with a particular risk and what is the scale on which they can be enforced? Are these rules binding for the whole 'system' under

<sup>2</sup> Broadening the Hood, Rothstein and Baldwin definition of the term regulation is understood as governmental interference with market or social processes to control potential adverse consequences to health, the environment as well as the vital services on which society depends.

question, do they apply to a major part, a part, a minor part or are there no binding rules at all?

- Level of compliance: To what extent are these rules complied with? Is the level of current compliance high, high to medium, medium, medium to low, low?
- Regulation adequacy: Does the current regulatory system achieve its purpose and is the degree of governmental interference adequate? Are there other ways of effecting control and co-ordination which seem less intrusive or more effective and efficient (such as the ‘invisible hand’ of markets or voluntary industry standards etc.)? Is the adequacy of current regulation high, high to medium, medium, medium to low, low?
- International co-operation: Irrespective of existing regulation schemes, has the risk triggered co-operation beyond national frontiers and does such co-operation – be it on a trans-national level or on a truly inter-governmental level – meet the goals set for it? Thus is such co-operation (existing and) fully functional, mostly functional, partly functional, barely functional, not existing?
- Stakeholder participation: Are stakeholders and the general public engaged in decision-making related to the risk? Is there full engagement, substantial engagement, partial engagement, minimal engagement or is engagement absent altogether?

### Further Implications

The criteria under this category look at what larger economic and political consequences a risk can entail and they also raise the issues of insurability as well as the speed of technological progress:

- Impact on global free trade: Is there a potential for the risk’s consequences to cause the disruption of the global system of free trade or to damage trust and confidence in both real or financial markets as well as related market mechanisms? Is such impact on global free trade considered to be low, low to medium, medium, medium to high, high?
- Impact on business: Is the risk likely to entail downstream physical, i.e. secondary, consequences such as impact on business profit or overall trust and confidence in business? Is that impact on business low, low to medium, medium, medium to high, high?

- Impact on actors' power: Can the risk and how it is treated change the existing balance of power and influence – both on a national or international scale? With governments (still) being a major locus of power – does the risk impact on governments' position or is it likely to damage trust and confidence in governments? If so, is this impact on power and influence low, low to medium, medium, medium to high, high?
- Insurability: Can the presumed effects of the risk be covered for by taking out insurance? Does the risk lend itself to full, nearly full, partial or minimum insurability or is there no insurance possible?
- Technology change: How significant is the potential technology change which concurs with taking a particular risk? Has it to be qualified as incremental, incremental to evolutionary, evolutionary, evolutionary to break-through, breakthrough (or radical)?

A risk governance profile developed along the above lines is, without doubt, not able to present a comprehensive picture of reality. Rather, it deliberately attempts to reduce complexity by providing an easy-to-grasp visual and, consequently, forces some of the nuances and 'shades of grey' into a binary decision pattern.

It is nonetheless expected that there is merit in trying to profile risk governance for the result is an overview of major aspects of a particular risk governance situation – or a legitimate interpretation thereof. Furthermore, by discussing a risk and its immediate characteristics in the larger context of responsibilities as well as decision-making and control mechanisms, the focus shifts from what can be said about a risk to what can – and should – actually be done. The profile supports this perspective by pointing out major flaws which requiring remedial action.

In the following, the profiling criteria are applied to the hypothetical case of a major power outage spilling into international dimensions and, consequently a risk governance profile for cascading blackouts is outlined. Rather more than providing a fully-fledged discussion of blackouts with regard to the individual criteria, the below paragraphs serve as pointers or an illustration of how such a profile can help pin down major problem aspects within a common frame of reference.

#### **A.7.1.2 Case Illustration: Cascading Blackout**

The second half of 2003 saw a spate of major power blackouts, with the two most notorious reaching international dimensions: the US-Canadian

blackout of August 14 which affected more than 50 million people in large parts of the Midwest and Northeast US States and of Canada and which, for some regions, lasted as long as four days, and the Italian blackout of September 28 which left virtually all of Italy’s 57 million population as well as Southern parts of Switzerland for some 4–6 hours in the dark (and for a total of 18 hours without electricity) and endangered the continuous operation of the interconnected ‘European’ grid (see Appendix 1 in this book).

How can a major international blackout which is the result of a cascading chain of events be viewed in terms of risk governance – i.e. how does it score with regard to the criteria which the proposed profiling template identifies as contributing to the governance of a certain risk?

Risk Framing	
<ul style="list-style-type: none"> <li>➤ Risk scope</li> </ul>	<ul style="list-style-type: none"> <li>- theoretically equals the scope of the interconnected network, i.e. in Europe the risk of a cascading blackout has international dimensions per se.</li> <li>- the past has alerted us to the far more probable and frequent occurrence of a regional blackout, involving two or more TSOs</li> </ul>
<ul style="list-style-type: none"> <li>➤ Risk perception</li> </ul>	<ul style="list-style-type: none"> <li>- by majority of retail users perceived as potential for annoying but limited disruptions of everyday comfort and services which, in fact, are taken for granted (e.g. smoothly running public transport, fresh products in supermarkets and fridges, running internet and entertainment facilities); hardly ever perceived in the larger context of the availability of energy sources (e.g. fossil fuels, gas, water, nuclear, renewables etc.), corresponding policy choices (e.g. nuclear moratorium), market liberalisation and privatisation (changing investment incentives) etc</li> <li>- by wholesale users perceived as potential disruption of their ability to produce or deliver the products and services that form their core competencies; such disruption is to prevented by</li> </ul>

	<p>all means, requiring defence and back-up mechanisms</p> <ul style="list-style-type: none"> <li>- by governments perceived as the potential for damaged public confidence in the quality of public service or in governments' effectiveness in supervising the private sector etc</li> <li>- while consistent within, e.g., the retail users group in that their perception lacks the broad picture, there is a tendency to divergent perceptions across actor groups</li> </ul>
➤ Public awareness	<ul style="list-style-type: none"> <li>- high with respect to the possibility of a blackout happening which is limited in scale; such awareness is reinforced by regular advance notices of local power supply interruptions due to maintenance work</li> <li>- medium awareness of the risk of an international blackout as well as the full consequences likely to come with it (to the majority of population the US-Canadian power outage and the Italian blackout came as a complete surprise)</li> </ul>
<b>Risk Characterisation</b>	
➤ Probability of occurrence	<ul style="list-style-type: none"> <li>- low to medium depending on – as seems to be the case for the European interconnected network – the presence of enabling factors such as institutional flaws in control, co-ordination and communication mechanisms as well as incentive structures, a multitude of players acting independently, technical shortcomings, human failure such as inadequate maintenance practices, a reality of frequently overloaded transmission lines, adverse weather conditions, etc. (see chapter 2)</li> </ul>
➤ Damage potential	<ul style="list-style-type: none"> <li>- low in terms of deaths and injuries as well as with regard to both the natural and built environment</li> <li>- depending on the duration of the blackout, high</li> </ul>

	<p>damage potential with regard to production and service loss; consequently, there is also a high potential for secondary or indirect damage related to financial assets and investments, public welfare and social comforts, security, cultural heritage as well as people's sanity and public confidence</p>
➤ Ubiquity of damage	<ul style="list-style-type: none"> <li>- regional or international extent as the interconnected network covers all of Europe</li> </ul>
➤ Persistence of damage	<ul style="list-style-type: none"> <li>- damage is created and persists during the entire duration of the blackout</li> <li>- although the loss of production and service will make its way into companies' profit and loss statements and will thus linger on in the guise of financial damage well beyond the moment when electricity is restored, it seems fair to say that the damage incurred due to an international blackout has 'only' short to medium time persistence</li> </ul>
➤ Reversibility of damage	<ul style="list-style-type: none"> <li>- very limited, i.e. low to medium, physical reversibility (e.g. road accidents resulting in deaths, injuries and wrecked cars due to an electricity-induced failure of traffic signals or a large quantity of spoiled dairy products due to failing cooling systems), but there are ways of financial compensation</li> </ul>
➤ Delay effects of damage	<ul style="list-style-type: none"> <li>- damage mostly seems to hit immediately, minor delay effects are imaginable (e.g. with regard to storage facilities which depend on constant cooling such as fish and seafood storage houses)</li> </ul>
➤ Level of complexity	<ul style="list-style-type: none"> <li>- sheer number of actors involved in large-scale blackouts, intrinsic complexity of the systems under investigation, interdependencies between national grids as well as across different infrastructures both on a national and international scale and, consequently, tricky root cause analysis suggest at least a medium level of</li> </ul>



	complexity, (which, in turn, also highly affects the time needed for the restoration of services)
➤ Level of uncertainty	<ul style="list-style-type: none"> <li>- modelling interdependencies in systems as complex as the electricity grid in a liberalised market setting seems to present no small challenge and levels of confidence for established cause effect relationships need to be considered with caution since they might be the result of inadequate reduction of complexity; the level of uncertainty is therefore considered to be medium to high</li> </ul>
➤ Level of ambiguity	<ul style="list-style-type: none"> <li>- pure risk assessment results, as far as they are based on similar facts and knowledge, seem to be relatively straightforward to interpret; ambiguity is therefore not thought to be higher than low to medium</li> <li>- as the Italian black out has demonstrated, however, recommendations which are based on ‘fact findings’ as well as an analysis of the causes can vary considerably depending on the perspective of the organisation who issues them and, equally, buck-passing is widely practiced – ambiguity thus emerges as soon as assessment results need to be translated into policies or a political agenda</li> <li>- with respect to the hazards which can cause a blackout, the level of ambiguity will be high whenever the hazard is suspected to derive from a highly contended and ideology-prone phenomenon such as nuclear energy (e.g. an international blackout caused by a large-scale nuclear accident), causing public debate to shift from its original focus on risk related to blackouts to more threatening scenarios attached to the issue of nuclear energy</li> </ul>
➤ Impact on equity	<ul style="list-style-type: none"> <li>- within a particular society all stakeholders as well as the general public basically face the consequences of a blackout, perhaps with the</li> </ul>

	<p>exception of wholesale users who have invested in back-up capacities; there are however portions of the population who suffer more from the consequences than others – e.g. those in need of getting to a hospital such as pregnant women or elderly falling ill (this will have to be taken into account in load shedding and load restoration policies)</p> <ul style="list-style-type: none"> <li>- between different countries equity impacts seem to be restricted purely by the nature of the interconnected network, which, it seems, is not conducive to insular back-up solutions for individual countries; electricity transit countries such as Switzerland are likely to be more exposed to instability of their grids than non-transit countries, due to the emergent practice of Europe-wide energy trading and concomitant physical trans-border electricity flows over which they exert no control</li> <li>- all in all the impact on equity seems to be limited, i.e. low</li> </ul>
<p>➤ Public concern</p>	<ul style="list-style-type: none"> <li>- although blackouts can be utterly disruptive with regard to the infrastructures and services on which society has come to depend, the degree of public concern seems to be low</li> <li>- in the Western world where people are used to a both reliable and abundant supply of power, blackouts, much as they come as a total surprise, largely tend to be forgotten about after power has been restored – limiting them to a matter of interest to experts only</li> </ul>
<p>Control and Co-ordination</p>	
<p>➤ Responsibilities pattern</p>	<ul style="list-style-type: none"> <li>- expansion of the interconnected network, market liberalisation, privatisation and the deliberate break up of a once vertically integrated electricity value chain have changed the electric power landscape from a handful of government-</li> </ul>

	<p>controlled monopolies to a multitude of actors each of whom exerts only partial control over a small part of the overall system</p> <ul style="list-style-type: none"> <li>- responsibility patters seem to be at best partially clear and the system functions best when it is not under strain; in case of an emergency, however, such shared responsibility slows down immediate reaction and response measures</li> </ul>
<p>➤ Regulatory basis</p>	<ul style="list-style-type: none"> <li>- naturally comprises all of the countries which together form the interconnected network and therefore has to be truly regional or international, i.e. EU-wide regulation is not sufficient since it only applies to a part of the European network</li> </ul>
<p>➤ Binding rules</p>	<ul style="list-style-type: none"> <li>- at EU level, supranational framework legislation establishes binding rules (e.g. EU Electricity directive 2003/54/EC finalising the establishment of an internal electricity market and replacing Directive 96/92/EC and regulation (EEC) No 1228/2003 on network access in cross-border trade; see Appendix 7.1)</li> <li>- at country level and, partially, at sub-country, i.e. federal state or canton, level, a set of framework constitutional articles, laws and ordinances provide binding rules</li> <li>- at the company level, binding rules exist in the form of detailed internal procedures or operating manuals</li> <li>- binding rules do not exist at a level which transcends the EU and comprises all the territorial entities integrated in the interconnected network (Europe-centred UCTE, ETSO, EURELECTRIC etc. guidelines and recommendations are, as of yet, not legally binding and neither is the output of the activities of other institutions such as the World Forum on Energy regulation, the World Energy Council, the Committee on Sustainable Energy of the</li> </ul>

	<p>UN's Economic Commission for Europe (ECE) or the International Energy Agency (IEA); see Appendix 7.3)</p> <ul style="list-style-type: none"> <li>- legally binding rules thus only exist for part of the interconnected European network and they are largely limited to setting the framework or boundary conditions within which these system parts are to work</li> </ul>
<ul style="list-style-type: none"> <li>➤ Level of compliance</li> </ul>	<ul style="list-style-type: none"> <li>- at EU-level somewhat compromised by generous transition periods</li> <li>- while, at country level, enforceable rules are a natural part of the legislative framework, it is also a widespread reality that regulators and TSOs are rarely endowed with the power and the resources to ensure compliance; for this reason, it is also difficult to assess compliance at company level, which, overall, shall be considered as medium</li> </ul>
<ul style="list-style-type: none"> <li>➤ Regulation adequacy</li> </ul>	<ul style="list-style-type: none"> <li>- low due a situation of multiple actors and multiple jurisdictions where there is no single decision-making authority</li> </ul>
<ul style="list-style-type: none"> <li>➤ International co-operation</li> </ul>	<ul style="list-style-type: none"> <li>- apart from the supranational efforts within the EU, transnational and truly trans-European – i.e. reaching beyond EU level – collaboration in the areas of electricity transmission, generation and supply as well as trading is undertaken and fostered by organisations such as UCTE, NORDEL, ETSO, EURELECTRIC, IFIEC, EuroPEX, EFET, co-operation among regulators of EU and EEA member states can be found within CEER and a new form of ‘horizontal governance’ is experimented with in the context of the Florence forum which bring together government representatives, regulators, TSOs and market participants of both EU and EEA member states in order to further discuss issues related to a single EU electricity market (see Chapter 4)</li> </ul>

	<ul style="list-style-type: none"> <li>- international co-operation focusing on the prevention of blackouts seems to happen within UCTE's 'Investigation Committee on the 28 September 2003 Blackout in Italy'; other taskforces (see Chapter 2) which were formed in order to investigate the Italian blackout seem to be dissolved by now</li> <li>- while these initiatives are certainly very helpful in that they provide for (altogether voluntary) co-ordination mechanisms as well as points of contact, none of them includes all countries which need to be part of the decision process, their mechanisms for resolution passing and reconciliation are not among the fastest, they are prone to yield to EU pressure and, as a matter of fact, they did not prevent the Italian blackout from happening</li> <li>- all in all international co-operation is therefore thought to be partially functional</li> </ul>
<p>➤ Stakeholder participation</p>	<ul style="list-style-type: none"> <li>- on a European scale, different stakeholders all engage in their own fragmented decision-making procedures dealing with those parts and individual functions of the overall system which are of direct concern to them (i.e. regulators are active within their exclusive council dealing with regulatory affairs, industry and power exchanges engage within their respective branch associations etc)</li> <li>- on a national scale, participation seems to be somewhat easier since the legal systems of several countries (e.g. Switzerland) require consultation procedures for draft laws, thereby giving a voice to a vast range of stakeholders including organisations representing the general public; similarly, in some countries consumer watchdogs have acquired quite an influential position in the national energy debate</li> <li>- at the local level, emergency planning and</li> </ul>

	<p>recovery requires a strong focus on implementation (as opposed to mere technology and science) and there is therefore a need to better engage those likely to be affected by a blackout</p> <ul style="list-style-type: none"> <li>- at best we have partial engagement given that there is no common European strategy or foresight body which brings together and engages all the different stakeholders as well as representatives of the general public, with a view to creating a consistent and coherent structure for risk governance embracing the entire infrastructure both with regard to technical and socio-economic aspects</li> </ul>
<b>Further Implications</b>	
<ul style="list-style-type: none"> <li>➤ Impact on global free trade</li> </ul>	<ul style="list-style-type: none"> <li>- likely to remain low although damage – in particular financial loss due to production stop and non-delivery of services – resulting from an international blackout can be high and even lead to temporary repercussions on a country's financial markets and currency</li> </ul>
<ul style="list-style-type: none"> <li>➤ Impact on business</li> </ul>	<ul style="list-style-type: none"> <li>- likely to be high due to potentially high secondary financial damage</li> <li>- a vast blackout might also impact the business structure, since it potentially affects the relationships among the TSOs</li> </ul>
<ul style="list-style-type: none"> <li>➤ Impact on actors' power</li> </ul>	<ul style="list-style-type: none"> <li>- although a major blackout can temporarily perturb public confidence in government and in the corporate sector, it is nonetheless thought that the impact on the existing balance of power and influence remains low given electricity is restored both timely and durably</li> </ul>
<ul style="list-style-type: none"> <li>➤ Insurability</li> </ul>	<ul style="list-style-type: none"> <li>- the physical damage from a blackout seems to be fully insurable, subsequent damage to a company's reputation, market value as well as the strain put on people to make up for what has been lost cannot be covered by insurance</li> </ul>

<p>➤ Technology change</p>	<ul style="list-style-type: none"> <li>- Both the experience and the (increased) risk of a blackout can accelerate the adoption of existing technologies and exert a pull for new technological developments; this might also affect the links with industrial operators and equipment vendors</li> <li>- A blackout potentially also has strong implications for defence plans, operation handbooks, grid codes and security policies in force, as well as the settings and maintenance policies of the control and protection equipment</li> </ul>
----------------------------	--

To conclude, the below graph (Figure A.7.2) profiles risk governance related to major blackouts and, in doing so, provides a visual summary of where the major gaps in risk governance are located.

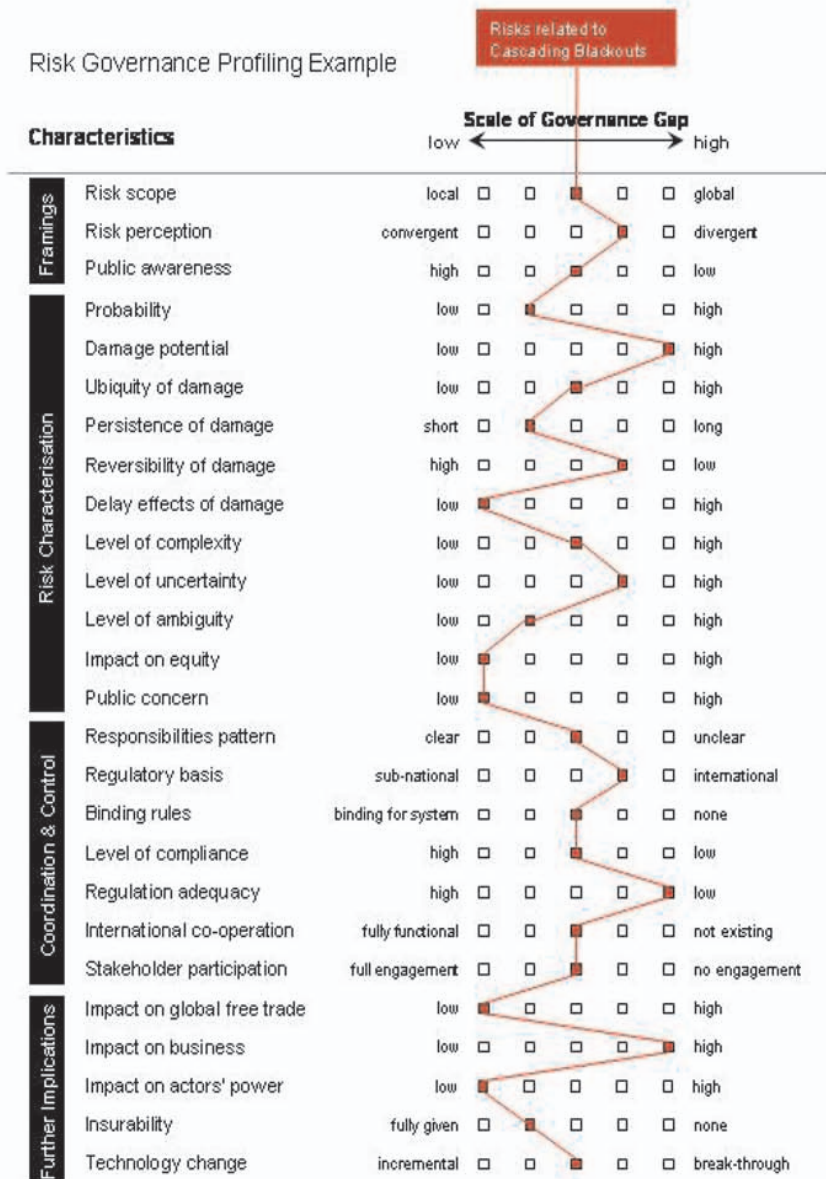


Figure A.7.2. Risk profiling example: cascading blackouts



## Appendix 8

# The Institutional and Regulatory Context for Risk Governance of the European Critical Electricity Infrastructure

*Marcelo Masera, Maurizio Sajevo*

### A.8.1 Introduction

This appendix presents a partial overview of the complex legislative and regulatory framework that surrounds the European Critical Electricity Infrastructure (ECEI), and will eventually define a framework for the risk governance process presented in Chapter 5.

At a first look we can immediately notice that the main regulatory activity is related to the fields of market and competition, security of energy supply, international cooperation.

The following tables present the main legislation and regulatory norms in force and the main institutional actors of ECEI. The first table describes the European Union context; the second and third give two examples of EU Members States (namely Italy and Finland); the fourth presents some relevant international organisations; the fifth regional bodies; the sixth professional associations; and the seventh market related associations.

This non-exhaustive list illustrates the complexity of the scenario, from the policy, industrial and technical standpoints, without disregarding that each Member State of the European Union has their own internal legislation, and that ECEI involves countries outside the EU.

In addition, several other actors will have to be considered for a complete picture of the context. Due to the intensive use of information and communication components, and the interactions with the information infrastructure, also the associations and bodies regulating these fields should be taken into account. Moreover, one will have to contemplate, national Critical Infrastructures initiatives, and international programmes related to threats and security that might be relevant for the poer infrastructure. Examples of this are the Council of Europe Convention on cybercrime, and the OECD's Global Forum on information systems and networks security.

<b>Institutional and regulatory context</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
<b>EU</b>			
European Union	Decisions 1254/96/CE; 1229/2003/CE 29/06/2003; interoperability and development of networks	Promotion of the internal European energy market, reinforcement of economic and social cohesion in the depressed areas, increase of security of supply from outside Europe, diversification of sources and integration of renewable sources of energy, interoperability of European energy networks with those of the new member countries, the Mediterranean basin and the Black Sea basin.	europa.eu.int/com m/energy/electricity /legislation/index_e n.htm
	Directive 2001/77/CE	Identification of quotes of electricity produced from renewable sources for each Member State	
	Directive 2004/88/CE	Promotion of cogeneration	
	Directive 2003/54/CE; 2003/55/CE European internal electrical market	Conditions of equity of the supply against dominant positions, discriminations, for the protection of small consumers and the promotion of R&D	
	Regulation 1228/2003	Regulation of cross-border trade in electricity – sets rules for transmission of electricity between the Member States	
<b>EU advisory bodies &amp; initiatives</b>			
Electricity Regulatory Forum of Florence	Neutral and informal EU level framework for discussion of issued and exchange of experiences	Discussing the creation of a true internal electricity market. The Forum currently addresses cross border trade of electricity, in particular the tariffication of cross border electricity exchanges and the management of scarce interconnection capacity.	europa.eu.int/comm/e nergy/ electricity/florence/inde x_en.htm
European Regulators Group for Electricity and Gas (ERGEG)	Independent advisory body, set up by the EC	Harmonisation of a common energy market, through a coordinated application of European Directives. Advice and assistance to the EC in ensuring the creation and smooth functioning of the internal energy market	www.ergreg.org/

<b>Institutional and regulatory context - EU Member States (1)</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
Italian Parliament	Law 14th November 1995, n. 481, on the Authority for electricity and gas	Regulation and control of electricity and gas for tariffs, quality of service, market structure, competition, licensing, administrative and accountants separation, verification and control, claims and inquiries, management of controversies, information and transparency	<a href="http://www.autorita.energia.it/">www.autorita.energia.it/</a>
	Legge 23rd August 2004, n. 239	Competition protection, for ensuring energy cost-performance offered to final customers and the non-discrimination of the national operators	<a href="http://www.acquirenteunico.it/ita/mercato/procedure/liberalizzazione.asp">http://www.acquirenteunico.it/ita/mercato/procedure/liberalizzazione.asp</a>
	Law n. 290/03	Competences of the Ministry of Productive Activities (Attivita' Produttive)	<a href="http://www.autorita.energia.it/relaz_ann/index.htm">www.autorita.energia.it/relaz_ann/index.htm</a>
Italian Government	Decree-law order of Ministry on the National Single Buyer	Attribution of competences to the National Electricity Single Buyer (Acquirente Unico), responsible for procuring electricity to captive customers	<a href="http://www.acquirenteunico.it/ita/home/procedure/home.asp">www.acquirenteunico.it/ita/home/procedure/home.asp</a>
	Decree-law order n. 79 - 16th March 1999	Reform of Directive 96/92 on generation, transport and dispatching, distribution and sale of electrical energy	<a href="http://www.acquirenteunico.it/ita/Mercato/Documenti/79-99.pdf">www.acquirenteunico.it/ita/Mercato/Documenti/79-99.pdf</a>
Authority for electrical energy and gas	Deliberative Authority for the regulation and control of electric energy and gas	Regulation and control of electricity and gas for tariffs, quality of service, market structure, competition, licensing, administrative and accountants separation, verification and control, claims and inquiries, management of controversies, information and transparency	<a href="http://www.autorita.energia.it/">http://www.autorita.energia.it/</a>
GRTN	Independent Transmission System Operator	GRTN has the mission of transmitting and dispatching electricity, as well as of managing & operating the national high- and extra-high voltage power transmission grid, as set forth in Legislative Decree no. 79 of 1999, in the respect of the public interest. Produces the Italian Grid Code	<a href="http://www.grtn.it/">www.grtn.it/</a>

<b>Institutional and regulatory context - EU Member States (2)</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
Parliament of Finland	Electricity Market Act (386/1995)	Ensure preconditions for an efficiently functioning electricity market so as to secure the sufficient supply of high-standard electricity at reasonable prices. The primary means are competition in electricity production and sales and reasonable and equitable service principles in the operation of electricity networks.	<a href="http://www.energiamarkkinavirasto.fi/select.asp?gid=128&amp;pgid=128">www.energiamarkkinavirasto.fi/select.asp?gid=128&amp;pgid=128</a>
Energy Market Authority	Regulation of the market according to the electricity market act	The Energy Market Authority monitors compliance with the Electricity Market Act and the related statutes and to promote the operation of the competitive electricity and natural gas markets. It grants the emissions permits, supervises the monitoring and reporting of emissions data and maintains the Emissions Trading Registry of Finland.	<a href="http://www.energiamarkkinavirasto.fi/">www.energiamarkkinavirasto.fi/</a>
National Emergency Supply Agency (NESA)	Regulation on security of energy services	NESA finances and controls the critical emergency stocks and backup systems, and coordinates the assurance of critical infrastructures and basic services.	<a href="http://www.nesa.fi/hvkeskus.html">www.nesa.fi/hvkeskus.html</a>
Fingrid Oyj	Transmission system operator	Fingrid Oyj provides, in addition to Grid services, Cross-border services (connecting with the Nordic electricity markets, Nordic Elspot and Elbas exchange trading, and with Russian electricity market parties), and Balance services.	<a href="http://www.fingrid.fi">www.fingrid.fi</a>

<b>Institutional and regulatory context</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
<b>International</b>			
World Forum on Energy Regulation	Guidelines for energy regulation	Analysis of global and local development with reference to regulation, competition and liberalisation of energy market. Promotion of investments, regulatory policies, independence of the regulator, methods for regulation and monitoring of markets, enforcement of cooperation	<a href="http://www.autorita.energia.it/wfer/smith-eng.pdf">www.autorita.energia.it/wfer/smith-eng.pdf</a>
World Energy Council (WEC)	Promotion of sustainable supply and use of energy	Services, programmes and activities on policy and strategy recommendations on the entire energy spectrum -- coal, oil, natural gas, nuclear, hydro and new renewables -- Focus on market restructuring; energy efficiency; energy and the environment; financing energy systems; energy pricing and subsidies; energy poverty; ethics; benchmarking and standards; use of new technologies; and energy issues in developed, transitional, developing countries	<a href="http://www.worldenergy.org">www.worldenergy.org</a>
Committee on Sustainable Energy of the UN's Economic Commission for Europe (ECE)	Ad Hoc Group of Experts on Electric Power	Focus on the progress of the EU towards liberalisation of electricity markets, including barriers and prospects to the creation of an EU-wide electricity market; the impact of electricity market liberalisation on sustainable energy development; third party access i.e. regulated and negotiated versus single buyer; and the role of independent regulators	<a href="http://www.unece.org/ie/s/e/elec.html">www.unece.org/ie/s/e/elec.html</a>
International Energy Agency (IEA) - OECD	Intergovernmental body for the security of energy supply, economic growth and environmental sustainability	Several programmes of policy co-operation related to power sources (geothermal, hydro, hydrogen, solar, wind, ocean, fuel cells, superconductivity)	<a href="http://www.iea.org">www.iea.org</a>

<b>Institutional and regulatory context</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
<b>Regional bodies</b>			
ERRA	Energy Regulators Regional Association of the Central/Eastern European and NIS region	Voluntary organization of independent energy regulatory bodies of the Central/Eastern European and Newly Independent States region. Technical and market regulation activities	<a href="http://www.erranet.org">www.erranet.org</a>
CEER	Council of European Energy Regulators	Regulators from the Member States of the European Union (EU) and European Economic Area (EEA). Task-forces for cooperation and consultation	<a href="http://www.ceer-eu.org">www.ceer-eu.org</a>
ETSO	European Transmission System Operators	Association of TSOs, the association of TSOs in Ireland; UKTSOA, the United Kingdom TSO association; NORDEL, the Nordic TSOs, and UCTE, the Union for the Co ordination of Transmission of Electricity; and association of CENTREL, TSOs of the Continental countries of Western and Central Europe	<a href="http://www.ets-net.org/">www.ets-net.org/</a>
UCTE	Union for the Co-ordination of Transmission of Electricity	Association of transmission system operators in continental Europe. Produces rRelevant technical standards and recommendations, including operation policies for generation control, performance monitoring and reporting, reserves, security criteria and special operational measures. The Operation Handbook ensures the interoperability	<a href="http://www.ucte.org">www.ucte.org</a>
NORDEL	Association of the transmission system operators (TSOs) in the Nordic countries (Denmark, Finland, Iceland, Norway and Sweden)	Advice and recommendations promoting an efficient electric power system in the Nordic region, taking into account the conditions prevailing in each country.	<a href="http://www.nordel.org">www.nordel.org</a>
		Technical co-ordination and determination of recommendations within following spheres: system development and transmission planning criteria, system operations, reliability and exchange of information, principles for transmission pricing	

<b>Institutional and regulatory context</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
<b>Associations</b>			
Association of Electricity Producers (AEP)	Leading trade association for the UK electricity market	Promote the interests of its members.	<a href="http://www.aepuk.com/">www.aepuk.com/</a>
Energy Network Association (ENA)	UK gas and electricity transmission and distribution licence holders	Promote the interests, growth, good standing and competitiveness of the UK energy networks industry in the UK and overseas..	<a href="http://www.energynetworks.org">www.energynetworks.org</a>
The European Renewable Energies Federation (EREF)	Represents the independent producers of renewable sources in Europe,	The missions are both to create an operational network of Renewable Energy (RE) power producers and to raise awareness in the public and European Institutions and others about the sector as it develops.	<a href="http://www.eref-europe.org/">www.eref-europe.org/</a>
EURELECTRIC - Union of the Electricity Industry	Professional association which represents the common interests of the electricity industry at pan-European level, plus its affiliates and associates on several other continents	Objectives: supporting the process of market liberalisation in our sector, helping to create a pan-European energy market through harmonisation and industry action	<a href="http://www.eurelectric.org">www.eurelectric.org</a>
Electricity Association (EA)	Association of the UK electricity industry	Promoting the industry's message, and electricity as a product, lobbying and representational role, intelligence-gathering and briefing services, early warnings of developments	<a href="http://www.electricity.org.uk">www.electricity.org.uk</a>

<b>Institutional and regulatory context</b>			
<b>Actors</b>	<b>Object</b>	<b>Description</b>	<b>Reference</b>
<b>Market</b>			
European Federation of Energy Traders (EFET)	Association of more than 70 energy trading companies from 18 European countries dedicated to stimulate and promote energy trading throughout Europe	The activities of EFET include: lobbying with authorities and communicating with market and grid operators and their associations; public relations: distribution of information to participating companies; working group meetings; standardisation & harmonisation; research	<a href="http://www.efet.org">www.efet.org</a>
International Federation of Industrial Energy Consumers (IFIEC World)	International Non-Governmental Organization (NGO) working closely with other global organizations such as the United Nations (UNO), the World Energy Council (WEC), the International Chamber of Commerce (ICC), the International Energy Agency (IEA)	IFIEC WORLD fundamental objective is to cater for the needs of the industrial energy consumers in discussion with political decision makers at all levels (national, regional, international) by promoting co-operation with other Trade Associations with similar goals in relation to energy issues affecting the long term competitiveness of consuming energy industries.	<a href="http://www.ifiiec.org">www.ifiiec.org</a>
EuroPEX (Association of European Power Exchanges)	Non profit making association of derived from the founders of EUROPEX and the APEX European Members	Promote power exchange for increasing competition by creating price transparency and implementing the European single electricity market; support liberalisation; deal with international trading and congestion; establish dialogue with ETSO, EFET and others.	<a href="http://www.europex.org">www.europex.org</a>



## Appendix 9

# Costs of Power Infrastructure Malfunctioning

*Viren Ajodhia*

### A.9.1 Introduction

Given the wide range of costs and damages incurred by so many different stakeholders and organizations, and given the lack of systematic data collection on the costs of past infrastructure service disruptions in the EU Member States, a total cost estimate is a fruitless attempt.

It must also be kept in mind that damage statements and cost estimates are coloured by strategic considerations. Parties may have an incentive to overestimate costs if they see possibilities of claiming damages or if they market a product that helps to prevent disruptions. Others might have an interest in a conservative estimate because they may be held liable for the damages resulting from the disruption. To gain some insight into the order of magnitude of the cost of service interruptions nevertheless, we have collected a sample of available figures about the cost of interruptions in the transport, energy and telecommunications sectors.

The costs of routine failure in transport are high. The costs of “normal” road congestion in the EU, for example, are estimated at around 2% of GDP approximately. Road traffic accidents add another 1.5-2% of GNP in developed countries. When looking at incidental failures, the effects on air traffic of the September 11 attacks come to mind. For US airlines alone, these costs were estimated to be over one billion euros. But the costs of lesser interruptions are also substantial.

The energy sector has very accurate service interruption statistics, but fewer sophisticated estimates of the associated costs – let alone aggregate figures.<sup>1</sup> To nevertheless give an estimate, the major power outage in the USA and Canada on August 14, 2003, affected 50 million people. The cost was estimated at around 6 billion US dollars. The power outage in Italy on September 28, 2003, affected some 57 million people. However, the total

costs of the outage have so far remained unreported. One newspaper report mentioned that the costs of perished foods and missed retail earnings alone resulted in damages of 120 million euro. The divergent estimates for these disruptions indicate the seriousness of the situation, although they also show that the estimates are sensitive to the methods used.

In the telecoms sector, it is even harder to find reliable estimates.<sup>ii</sup> Breaks in cables – the largely undisputed primary cause of outage of telecoms services – annually cause damage worth up to \$500 million in the US. But apart from this type of physical disruptions, there are other causes (software errors, human errors, overload) that undoubtedly raise this amount.

All forms of digital attacks (hacking, malware, spam, viruses) are another cause of substantial economic damage. Estimates of the damage are widely divergent (e.g. Information Week Research and PriceWaterhouseCoopers). Estimated the global cost of security breaches, downtime and virus-attack cleanups were at 1600 billion US dollars in 2000. Computer Economics, on the other hand, estimated the worldwide economic damage of computer worms and viruses in 2001 at “just” 13.2 billion US dollars.<sup>iii</sup>

Granted that there are many uncertainties, we may conclude that even the more conservative estimates of the direct costs of interruptions in the transport, energy and telecoms sector in the EU Member States amount to many billions of Euros per year. This amount is multiplied when using less conservative estimates – certainly if indirect costs are added.

In addition to the financial costs and the direct effects of infrastructure malfunctioning to the economy, there can be many other adverse effects of infrastructure malfunctioning. Road congestion has direct negative consequences in terms of enhanced emissions, including particle emissions, CO and NOx emissions that all have known detrimental effects on public health.

## **A.9.2 Electricity Power Interruption Costs**

An interruption takes place when due to a shortage customers are delivered with less electricity from the power system than originally planned. If the actual consumption is zero then the interruption is full, otherwise the interruption is partial. According to Sanghvi (1982), the costs of an interruption are the result of two variables i.e. the type of the shortage and the shortage management strategy: The shortage can either be capacity or energy related. Capacity shortages relate to situations where the available capacity is lower than peak load. These situations can for

example result from generation or network failures, or simply because of insufficient installed capacity resulting from under-investments.

An energy shortage occurs when the amount of electricity that would be purchased on an average during some period, exceeds the energy available during that period. These shortages are often related to fuel shortages or low reservoir water levels in hydroelectric plants. From the customer's perspective, the results of a capacity or energy shortage can take different forms, depending on the shortage management strategy employed by the system e.g. peak shaving, rotating blackouts, interruptions. Different shortage management strategies have different impact on interruption costs. For example, constraining peak demand – by the price mechanism or by rationing – to a level at which the operating reserve is equal to the normal margin results in customers reducing or shift their peak demand. Alternatively, reducing the operating reserve margin – leading to a situation of unchecked reliability degradation – can lead to more frequent and persistent interruptions with no warning. The costs under the former are likely to be less than in the latter. This is because under the former methods of management any un-served energy arises on a planned basis, whilst in the latter degradation of service reliability brings unexpected interruptions.

In the case of electricity networks, it is primarily capacity shortages that are of concern. These are often the result of failures in the network. The type of network and the interruption management strategy employed largely influence the characteristics of the interruption and consequently the interruption costs. Failures at the transmission level rarely result in interruptions due to the high redundancy. These networks are often operated on the basis of contingency criteria (e.g. N-1), which require that a failure in any random component should not lead to an interruption. Contingency at the distribution level on the other hand is much less stringent. Here, failure often results in an interruption although the impact – relative to that in the case of transmission – typically more limited.

### **A.9.3 Interruption Costs Measurement Techniques**

The literature presents a large number of techniques to measure interruption costs; the most common techniques are discussed in this section. A distinction is made between indirect methods and survey methods. Survey methods acquire interruption cost information directly from customers while indirect methods use other information sources for this purpose. Surveys are again divided into ex post and ex ante surveys,

which respectively refer to requesting consumer information about actual and hypothetical interruptions. (see Figure A.9.1)

### Indirect - proxies

Proxy methods use indirect data to derive information on interruption costs. In recent decades a couple of proxies have been developed. The ratio of Gross National Product (GNP) to the electricity consumed forms roughly the upper bound for the interruption costs (Shipley et al. 1972, Telson 1975). The ratio of the electricity bill and the energy consumption then provides the lower bound. For residential customers, the wage rate has been used as a measure of the foregone leisure in case of an interruption (Munasinghe 1980) or the value of lost production for a firm during an interruption (Munasinghe 1981). Loss of production has also been applied to households (see for example Gilmer and Mack 1983).

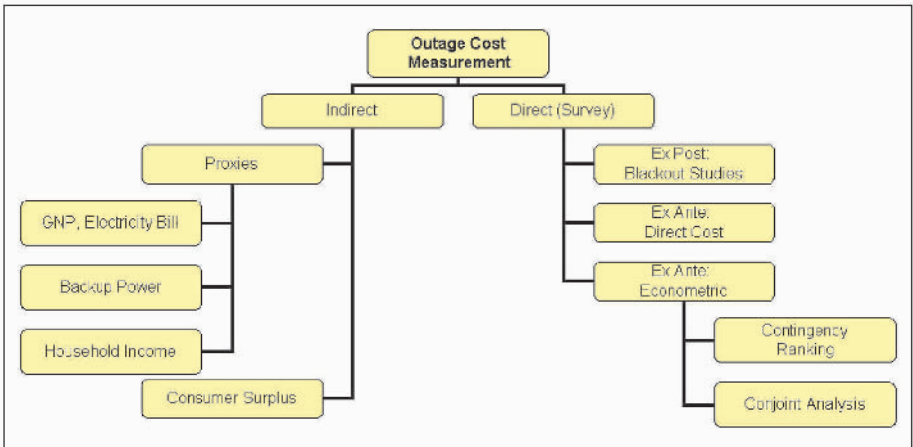


Figure A.9.1. Overview of interruption cost measurement techniques

### Indirect - Consumer Surplus Methods

Customer surplus methods derive interruption costs information from electricity demand curves. The idea is that the willingness-to-pay for electricity depends on the degree to which the consumption of each unit can be deferred to another hour. When elasticity is low then the consumer surplus loss – which is equivalent to the households' willingness-to-pay to avoid a total interruption in that hour – is larger. The consumer surplus losses minus the bill savings provide a measure of the interruption costs (Sanghvi 1982).

### Indirect - Costs of Backup Power

Customers may take preparatory actions to prevent the costs that arise from interruptions by installing backup power. Bental and Ravid (1982) suggest that a profit maximising corporate end-user will invest in backup power until the expected gain from the marginal self-generated kWh is also the expected loss of the marginal kWh which is not supplied to that firm. The marginal cost of generating its own power may then serve as an estimate for the marginal interruption costs.

### Ex post Surveys - Blackout Studies

Blackout studies collect information about interruption costs from actual interruptions. This method is usually applied in case of large-scale interruptions. Next to quantifying costs, black-out studies often also study the societal impact and preparedness for large interruptions such as police and fire responsiveness, environmental damage etc.

### Ex ante Surveys - Direct Costs

Direct cost surveys request interruption costs directly from customers. First, customers are requested to identify the different costs categories in case of an interruption. For industrial and commercial customers these may be lost sales or production, spoilage, damage, etc. The second step is to attach an economic value to each category. The interruption costs are then the sum of all these individual costs. Optionally, a list of possible measures and associated costs can be provided and customers are asked to indicate which measure they would employ for different interruption scenarios.

### Ex ante Surveys - Contingency Ranking and Conjoint Analysis

Under the contingency ranking method, customers are asked to value reliability as if there were a market for it. Thus, a hypothetical market is created in which customers are asked to indicate either willingness-to-pay (WTP) for higher reliability, or the willingness-to-accept (WTA) lower reliability levels. Conjoint analysis is similar to contingency valuation with the difference that the WTA and WTP figures are derived indirectly. Here customers are requested to rank in order of preference different mutually exclusive combinations of price and reliability levels – the price range is determined ex ante by the researcher.

To compare the methods, the following criteria are used: (1) costs and data requirement, (2) accuracy of results and (3) amount of information acquired. With respect to the cost and data requirement criteria, indirect methods score better. Especially proxy methods require very little and easily obtainable data and thus form an excellent tool to estimate the upper and lower bounds of interruption costs. However, the results are not likely to be very accurate and only give highly aggregated information.

Consumer surplus methods require substantial more data than proxy methods although the results may not be proportionally more accurate. There are two fundamental reasons for this: First, the observed willingness-to-pay for planned electricity consumption is not an accurate indicator of what one would be willing-to-pay to avoid an unplanned interruption. Second, when measuring system interruption costs, this method would assume that load shedding takes place according to some predetermined order. In practice this is hardly ever the case (Munasinghe 1981). The cost of backup power method seems to provide a good balance between costs and accuracy. The advantage of this method is that information is revealed from actual customer behaviour. A disadvantage of this approach is that it is based on the assumptions that firms install generators for backup purposes only and that the installed capacity is below normal peak demand. These assumptions do not always hold in practice. Installed generators often have joint applications while it may well be that installed backup power is equal or higher than peak load due to indivisibility of capacity or low prices of backup power (e.g. UPS technology has improved significantly over the years). Furthermore, this method is only applicable to larger customers as only these are likely to install backup power.

With respect to information, indirect measures score poor compared to survey methods. Surveys are expensive to carry out but can deliver quite detailed information about the different factors that influence interruption costs. Blackout studies for example can be used to evaluate the vulnerability of society with regard to an interruption and identify preparatory actions. The problem with blackout studies is that they can only be applied in case of an actual interruption. Ex ante surveys on the other hand, can be planned well ahead in time and can also provide substantial amounts of information. The advantage is that the different aspects that impact interruption costs can be studied such as interruption or customer characteristics. The general problem with ex ante surveys is their hypothetical character. In theory, the WTP and WTA values that are derived should be the same (Willig 1976). In practice however, it is found that obtained WTP figures are usually equal to zero or otherwise order-of-magnitudes smaller than WTA figures. Beenstock et al. (1998) argue that the explanation for this can be found in status quo and asymmetry effects. Under the former, the customer has a resistance to prospective change per se, no matter whether the service is improved or deteriorated. The asymmetry effect (or loss aversion) leads to a difference between WTP and WTA as consumers value prospective service improvements by some fraction of their value of deterioration.

## **A.9.4 Factors that Influence Cost**

There are a large number of factors that influence the actual level of interruption costs. These factors have been extensively studied in the interruption costs literature – most notably with the use of survey methods. Note that a cost-influencing factor should not be considered in isolation. In practice, it is likely a combination of factors that determine the costs that customers experience during an interruption. The different factors are now discussed.

### Duration

As an interruption prolongs, interruption costs increase. Caves et al. (1990) analyse the rate at which these costs increase by comparing results from different studies. For the industrial sector they find that normalised costs decrease with duration. This suggests that there is a large initial fixed cost component and variable component that decreases with duration. Similar comparisons were made for residential, retail, office building, government and farm customers, which however show large inconsistencies between the results studied.

### Perceived Reliability Level

Another factor that influences the level of costs of an interruption is the reliability level at which the consumer is supplied at. Generally, the higher the reliability level, the more severe will be the impact of an interruption. A study in Nepal showed that 38 per cent of residential customers considered the number of interruptions to be “low” or “very low” although the average number of interruptions was four per week (Pandey and Billinton 1999). Similar results were found in a Brazilian study where more than half of the residential customers interviewed valued the quality of service provided as “good” although half of these customers had experienced at least one interruption per month (Gastaldo et al. 2001). In most Western countries such interruption frequencies would not have delivered such positive outcomes for customer satisfaction. A possible explanation for this is that as the frequency of interruptions increases, customers can make a better trade off between expected interruption costs and the adaptive response costs thus minimising total interruption costs. Also, dependency on electricity may not be as high as in Western countries thus leading the relative impact of interruptions to be limited.

### Timing

Interruption costs vary with the time of the year, day of the week and time of the day. For residential customers, winter interruptions lead to higher costs than in the summer while morning or afternoon interruptions

are less costly than afternoon ones (Woo and Pupps 1992). For non-residential customers, the amount of costs is closely related to the level of firm output. For example Billinton et al. (1982) find that for retail customers in Canada, the interruption costs during the Christmas season and on Saturdays are significantly higher. An interesting result reported is that for retail and commercial customers, the least costly hour of during the working hours is lunch (Pandey and Billinton 1999, Gates et al. 1999). For large industrial customers, the timing of interruptions tends to have little effect; this reflects the constant output delivered in these industries (Dialynas et al. 2001, Gates et al. 1999).

#### Advance Notice

If an interruption is planned e.g. in case of energy shortages or maintenance activities, advanced notice may be provided to customers about the occurrence or duration of the interruption. Such actions tend to decrease interruption costs as customers may take preventive actions or incorporate appropriate rescheduling. Note that this is in line with the previous observation that customers experiencing frequent interruptions exhibit lower costs due to increased preparedness. A Scandinavian study report that planned interruptions can significantly reduce instantaneous interruption costs (Lehtonen and Lehstrom 1995). Similar results have been reported in other countries including the U.S., Canada and Nepal with reduction varying between 20 and 50 per cent (Billinton et al. 1982, Gates et al. 1999, Dialynas et al. 2001).

#### Customer Dependency

The degree of dependency of consumers on a reliable electricity supply also influences the level of interruption costs. Some consumers may be more dependent than others e.g. hospitals are much more vulnerable to an interruption than a residential customer. Doane et al. (1988) find a positive correlation between the presence of electric equipment in a household and the level of interruption costs. Customers' dependency also increases over time: Sullivan and Sheehan (2000) report a doubling in the real economic quantification of reliability by households in the U.S. over a 10-year period. Andersson and Taylor (1986) report an increase in the real interruption costs from 1969 till 1980 in Sweden. These results are attributed to the increased reliance of customers on electricity supply.

### **A.9.5 Cross-comparison of Interruption Cost Studies**

Interruption costs tend to vary as a function of different factors; this makes comparison of the results of different studies a difficult undertaking.



No interruption is the same; it may differ with respect to the time it occurs, the duration, etc. Similarly, the consumers affected by the interruption are also different; the costs experienced by these consumers will also tend to be different. These differences may partly be captured by differentiating between types of consumers but as may be observed from Table 1 there tend to be substantial differences in the results obtained by different interruption cost studies.

For practical purposes, the comparison presents interruption costs normalised per kWh of non-delivered energy; most studies express costs in these terms. Part of the large differences may be explained by the fact that the use of this denominator ignores that fact that interruption costs vary with the duration of the interruption.<sup>1</sup> Another explanation for the large differences is the fact that costs may differ by level of economic development (which may differ both geographically as over time). Also, it is not likely that the measurements capture all potential factors that influence the interruption costs.

Given that costs may vary substantially amongst consumers; this effect is not fully captured in the simple comparisons made in Table A.9.1.

The large observed differences from the comparison are somewhat discouraging. They suggest that in order to fully capture all possible factors that influence costs, a more complicated measure would be needed. Simple comparisons on the basis of kWh non-delivered energy are not likely to capture these. Ideally, the incentive would need to be set for each consumer individually and would need to take into account the true costs experienced by that consumer. This, however, is not a practical approach given the enormous administrative burden that would be involved. Rather, the regulator will set the incentive level based on some average measure of costs, possibly differentiated by consumer group. For practical purposes, the incentive would also be defined as a constant i.e. would not vary as a function of the quality level. Although such simplifications would possibly provide distorted incentives, they have the advantage of being relatively simple and easy to comprehend not only by the corporate user but also by consumers. The added value of a more sophisticated incentive system is not likely to outweigh the regulatory costs of implementing and administering a more complex incentive system.

<sup>1</sup> Some authors use the energy not supplied during the interruption as normalization factor while others use annual energy consumed or peak load. This tends to lead to some confusion.

*Table A.9.1.* Cross-comparison of interruption cost studies. All costs are normalised per kWh non-delivered energy and are in 2004 US dollars.<sup>2</sup>

<b>Residential</b>				
<b>Study</b>	<b>Methodology</b>	<b>Year</b>	<b>Country</b>	<b>2004 USD / kWh</b>
Khan (1997)	Survey	1997	Australia	0.00
Upadhyay	Survey	1996	India	0.23
Sarkar and Shreshta	Survey	1988	India	0.26
	Survey	1995	Iran	2.60
De Nooij et al.	GDP	2003	Netherlands	19.35
KEMA	Survey	2003	Netherlands	22.99
Young (1987)	Survey	1987	New Zealand	5.25
Turner (1977)	Proxy	1977	New Zealand	1.83
Trengeireid (2003)	Survey	2003	Norway	0.55
	Survey	1991	Saudi Arabia	1.29
Andersson and Taylor	Survey	1980	Sweden	4.18
Lolander (1945)	N/A	1948	Sweden	2.25
Swedish Joint Commission (1969)	Direct	1969	Sweden	4.91
UNPEDE (1970)	Survey	1970	Sweden	4.30
Kariuki and Allan	Survey	1996	UK	0.00
Sheppard (1965)	Proxy	1965	UK	2.81
UNPEDE (1970)	Proxy	1970	UK	8.34
Burns and Gross	Survey	1988	USA	6.70
Krohnm (1978)	Black Out	1978	USA	2.88
Faucett (1979)	Black Out	1979	USA	0.13
Sanghvi (1980)	Survey	1980	USA	0.56

<b>Commercial</b>				
<b>Study</b>	<b>Methodology</b>	<b>Year</b>	<b>Country</b>	<b>2004 USD / kWh</b>
Khan (1997)	Survey	1997	Australia	0.01
Sarkar and Shreshta	Survey	1988	India	10.12
	Survey	1995	Iran	3.98

<sup>2</sup> Amounts in local currency have been inflated first to 2004 levels, and then converted to US Dollars using the average exchange rate for 2004. Exchange rates were obtained from the CIA World Factbook, inflation data were obtained from the IMF. These are available at [www.cia.gov/cia/publications/factbook](http://www.cia.gov/cia/publications/factbook) and [www.imf.org/external/pubs/ft/wco/2004/02/data/pcpi\\_a.csv](http://www.imf.org/external/pubs/ft/wco/2004/02/data/pcpi_a.csv), respectively.

De Nooij et al.	GDP	2003	Netherlands	9.38
Young (1987)	Survey	1987	New Zealand	31.15
Trengereid (2003)	Survey	2003	Norway	6.76
	Survey	1991	Saudi Arabia	58.10
Andersson and Taylor	Survey	1980	Sweden	48.10
Kariuki and Allan	Survey	1996	UK	0.04
Burns and Gross	Survey	1988	USA	65.67

<b>Industrial</b>				
<b>Study</b>	<b>Methodology</b>	<b>Year</b>	<b>Country</b>	<b>2004 USD / kWh</b>
Khan (1997)	Survey	1997	Australia	0.00
Sarkar and Shreshta	Survey	1988	India	9.19
	Survey	1995	Iran	5.25
Young (1987)	Survey	1987	New Zealand	5.25
Turner (1977)	Proxy	1977	New Zealand	5.04
Heising (1966)	N/A	1966	Norway	6.09
Andersson and Taylor	Survey	1980	Sweden	18.25
Munasinghe	Survey	1988	Sweden	4.24
Lolander (1945)	N/A	1948	Sweden	6.48
Swedish Joint Commission (1969)	Survey	1969	Sweden	7.75
UNIPED (1970)	Survey	1970	Sweden	10.33
Hsu et al.	GDP	1991	Taiwan	1.79
Hsu et al.	Survey	1991	Taiwan	3.37
Munasinghe	Proxy	1988	Taiwan	1.47
Taiwan Power Co (1975)	Proxy	1975	Taiwan	1.22
Kariuki and Allan	Survey	1996	UK	0.07
Sheppard (1965)	Proxy	1965	UK	8.38
UNIPED (1970)	Proxy	1970	UK	9.99
Jackson and Salvage	Survey	1970	UK	4.15
(1974)				
Burns and Gross	Survey	1988	USA	11.22
Grosfeld-Nir and Tishler	Proxy	1987	USA	17.19
Modern Manufacturing (1969)	Survey	1969	USA	5.80
SRI (1980)	Black Out	1980	USA	13.30

<b>Agricultural</b>				
<b>Study</b>	<b>Methodology</b>	<b>Year</b>	<b>Country</b>	<b>2004 USD / kWh</b>
De Nooij et al.	GDP	2003	Netherlands	4.61
Khan (1997)	Survey	1997	Australia	0.04
Andersson and Taylor	Survey	1980	Sweden	7.20
Burns and Gross	Survey	1988	USA	5.84

<b>Whole Economy</b>				
<b>Study</b>	<b>Methodology</b>	<b>Year</b>	<b>Country</b>	<b>2004 USD / kWh</b>
De Nooij et al.	GDP	2003	Netherlands	10.11
Wijayatunga and Jayalath	GDP	2001	Sri Lanka	1.21
Hsu et al.	GDP	1991	Taiwan	0.07
Aiyar	Proxy	1995	India	0.20
Parik et al.	Proxy	1994	India	0.09

i See for the cost estimate of the U.S. power outage: Elcon (2004), *The Economic Impacts of the August 2003 Blackout*, Washington D.C.,

<http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf>.

The U.S. Department of Energy estimated a total cost of around \$6 billion (pp.2). The Anderson Economic Group (AEG, however estimates the total cost between \$4.5 and \$8.2 billion (pp. 1).

See for the blackout in Italy, Eurelectric (2004), *Power Outages in 2003*, Report nr. 2004-181-0007, Brussels. See for the estimated costs of the Italian outage: Povoledo, E.

Blackouts cuts power for hours in Italy, in: *International Harold Tribune*, 29 September 2003, <http://www.iht.com/articles/111673.html>.

ii Estimate of cable outages, Grover, W. (2004), *Fiber Cable Failure Impacts, Survivability Principles, and Measures of Survivability*,

<http://www.informit.com/articles/printerfriendly.asp?p=169456>.

iii See for estimates about the costs of downtime, Hulme, G.V. (2000), *It's Time to Clamp Down*, in: *Information Week*, July 10, 2000,

<http://www.informationweek.com/794/security.htm>.

See for the 2001 estimate of Computer Economics,

<http://www.computereconomics.com/article.cfm?id=133>.

# References

- Adibi M. M. (2000). "Power System Restoration: Methodologies and Implementation Strategies." Wiley-IEEE Press.
- AEEG (2003). "Enquiry into the interruptions to the electricity service on 26 June 2003 completed." Press release. Rome. Available at [www.autorita.energia.it](http://www.autorita.energia.it)
- AEEG (2004). "Resoconto dell' attivita conoscitiva in ordine alla interruzione del servizio elettrico verificatasi il giorno 28 settembre 2003." Milano. Available at [www.autorita.energia.it/](http://www.autorita.energia.it/)
- AEEG and CRE (2004). "Report on the events of September 28th, 2003, culminating in the separation of the Italian power system from the other UCTE networks." Milano and Paris. Available at [www.cre.fr/](http://www.cre.fr/).
- Ajodhia, V., Hakvoort, R. (2005). "Economic regulation of quality in electricity distribution networks." *Utilities Policy*, in press.
- Ajodhia, V., Hakvoort, R.A. and Van Gemert, M. (2002). "Electricity Outage Cost Valuation: A Survey", In: *Proceedings of CEPSI 2002*, Fukuoka, Japan.
- Amin M. (2002). "Modeling and Control of Complex Interactive Networks." IEEE Control Systems Magazine, pp 22-27, February.
- Amin M. (2005). "Powering the 21<sup>st</sup> Century: We can –and must– modernize the grid." IEEE Power and Energy Magazine, pp. 93-95, March-April.
- Amin, M. (2001). "Toward self-healing infrastructure systems," IEEE Computer Applications in Power, pp. 20-28, January.
- Anderson H. (2001). "Increased threat of outages in California," UPI, February 14.
- Arrillaga P.(2001). "Nation: Energy crisis is not limited to California," February 4. <http://www.nandotimes.com>.
- Avizienis A, J.C. Laprie, B. Randell, C.E. Landwher (2004). "Basic Concepts and Taxonomy of Dependable and Secure Computing." IEEE Trans. Dependable Sec. Comp. 1 (1), pp. 11-33.

- Avizienis, A., Laprie, J.C., B. Randell (2001). "Fundamental Concepts of Computer System Dependability." IARP/IEEE-RAS Workshop on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments. Seoul, May.
- Axelrod, A. M.D. Cohen (1999). "Harnessing Complexity: Organizational Implications of a Scientific Frontier." pp. 32-61, New York: Free Press.
- Balkovich, E. E, R. Anderson (2004). "Critical Infrastructures will remain vulnerable: neighborhoods must fend for themselves." *Int. J. Critical Infrastructures*, Vol. 1, no. 1, pp. 8-20.
- Barabási, A.-L. (2002). "Linked". Penguin, ISBN 0-452-28439-2.
- Baran J. (1994). "Statistics for Long-Memory Processes." Chapman & Hall.
- Barton, D.C., Eidson, E.D., Schoenwald, D.A., Stamber, K.L., Reinert, R.K., (2000). "An agent based model of infrastructure interdependency." SAND Report 2000-2925, 61.
- Bauer J.M., M.P.C. Weijnen, A.L. Turk, P.M. Herder (2003). "Delineating the scope of convergence in infrastructures: new frontiers for competition." In: Thissen W.A.H., P.M. Herder (eds.), *Critical Infrastructures - State of the Art in Research and Application*, Kluwer Academic Publishers, Boston/Dordrecht/London, USA, pp. 209-232.
- BBC News (2003a). "Power cut causes chaos." Internet release, UK Edition, August 28. Available at <http://news.bbc.co.uk/>.
- BBC News (2003b). "Danish capital loses power." Internet release, UK Edition, September 23. Available at <http://news.bbc.co.uk/>.
- BBC News (2004). "Greek capital hit by power cut." Internet release, UK Edition, July 12. Available at <http://news.bbc.co.uk/>.
- Berger, F. (2005). "Security of Supply – Challenges Arising from Intermittent Generation." Presentation at the Conference on European Security of Electricity Supply, Brussels, 15 March.
- Bernardi, S. Donatelli, G. Dondossola (2004). "Towards a Methodological Approach to Specification and Analysis of Dependable Automation Systems." Joint Conference on Formal Modelling and Analysis of Timed Systems (FORMATS) and Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT). September 22-24.

Billinton, R. (1994). "Evaluation of reliability worth in an electric power system", *Reliability Engineering and System Safety* 46: 15-23.

Board of Review (1977a). "First Phase Report: System Blackout and System Restoration." Edison, July 13-14.

Board of Review (1977b). "Second Phase Report: System Blackout and System Restoration". Con Edison, August 24.

Boisseleau, F. (2004). "The role of power exchanges for the creation of a single European electricity market: market design and market regulation." Dissertation, Delft University of Technology.

Brown, T., W. Beyeler (2001). "Analysis of the Potential Economic Impacts of Electric Power Outages in California." Sandia National Laboratories, Project Report to DOE/OCIP, Albuquerque NM, SAND 2001-3368P, 32 pp.

Brunk G. (2000). "Understanding Self-Organized Criticality as a Statistical Process", in *Complexity*. John Wiley & Sons, Vol. 5, No. 3.

Bush, B., Giguere, P., Holland, J., Linger, S., McCown, A., Salazer, M., Unal, C., Visarraga, D., Werley, K., Fisher, R., Folga S., Jusko, M., Kavicky, J., McLamore, M., Portante, E., Shamsuddin, S. (2002). "NISAC Energy Sector: Interdependent Energy Infrastructure Simulation System (IEISS)." Los Alamos National Laboratory Report (LA-UR-03-1159),

Caramanis, M.C. (1982). "Investment decisions and long-term planning under electricity spot pricing", *IEEE Transactions on Power Apparatus and Systems* 101 (12): 4640-4648.

Cazalet, E.G., Clark, C.E. and Keelin, T.W. (1978). "Costs and Benefits of Over/Under Capacity in Electric Power System Planning." Palo Alto (California), EPRI.

CEER (2004). "Key interactions and potential trade distortions between electricity markets." CEER Working Paper, Florence Forum, Final Report, September 12.

Ciapessoni E., Crespi-Reghizzi, S., Maestri, F., Ornstein, A., Psaila, G., and J. Szanto (2001). "Partitioning of Hierarchical Automation Systems." 13th Euromicro Conference on Real-Time Systems, Delft, The Netherlands. June.

CIGRE (2004). "Managing information security in an electric utility." Joint Working Group D2-B3-C2.01, Electra, n. 216, October.

CIGRE (2005). "Cybersecurity considerations in Power System Operations." Joint Working Group D2-B3-C2.01, Electra, n. 218, February

CNN.com (2003a). "Rush hour power cut hits London". Internet release, August 28. Available at [www.cnn.com](http://www.cnn.com).

CNN.com (2003b). "Danish capital, Sweden lose power." Internet release, September 23. Available at [www.cnn.com](http://www.cnn.com).

Commission of the European Communities (1998). Report to the Council and the European Parliament on harmonisation requirements – Directive 96/92/EC concerning common rules for the internal market in electricity, COM(1998) 167 final, Brussels.

Commission of the European Communities (1999). Second Report to the Council and the European Parliament on harmonisation requirements – Directive 96/92/EC concerning common rules for the internal market in electricity, SEC 1999/470, Brussels.

Commission of the European Communities (2000a). Communication from the Commission to the Council and the European Parliament on Recent progress with building the internal electricity market, COM(2000) 297 final, Brussels

Commission of the European Communities (2000b). Green Paper on a European strategy for the security of energy supply, COM(2000) 769, Brussels.

Commission of the European Communities (2001a). Communication from the Commission to the European Parliament and the Council on a European energy infrastructure, (as well as Proposal for a Decision of the European Parliament and of the Council amending Decision No 1254/96/EC laying down a series of guidelines for trans-European energy networks and Report from the Commission to the European Parliament, The Council, The Economic and Social committee and the Committee of the Regions on the implementation of the guidelines for Trans-European Energy Networks in the period 1996-2001), COM(2001) 775 final, Brussels

Commission of the European Communities (2001b). Completing the internal energy market, commission staff working paper, SEC(2001) 438, Brussels.



Commission of the European Communities (2001c). European Governance, White Paper, COM(2001) 428 final, Brussels.

Commission of the European Communities (2001d). First benchmarking report on the implementation of the internal electricity and gas market, commission staff working document, SEC(2001) 1957, Brussels.

Commission of the European Communities (2002). Communication from the Commission to the Council and the European Parliament – Final report on the Green Paper "Towards a European strategy for the security of energy supply", COM(2002) 321 final, Brussels.

Commission of the European Communities (2003a). Communication from the Commission to the European Parliament and the Council. Energy Infrastructures and Security of Supply, Brussels, COM (2003) 743

Commission of the European Communities (2003b). Communication from the Commission to the Council and the European Parliament on completing the internal energy market, COM(2001) 125 final, Brussels.

Commission of the European Communities (2003c). Communication from the Commission to the Council and the European Parliament on energy infrastructure and security of supply, COM(2003) 743, Brussels.

Commission of the European Communities (2003d). Communication from the Commission to the Council and the European Parliament on the development of energy policy for the enlarged European Union, its neighbours and partner countries, COM(2003) 262/2, Brussels.

Commission of the European Communities (2003e). Decision of the European Parliament and of the Council laying down guidelines for trans-European energy networks and repealing Decisions No 96/391/EC and No 1229/2003/EC – Extended Impact Assessment, commission staff working paper, SEC(2003) 1369, Brussels.

Commission of the European Communities (2003f). Directive of the European Parliament and of the Council concerning measures to safeguard security of electricity supply and infrastructure investment – Extended Impact Assessment, commission staff working paper, SEC(2003) 1368, Brussels.

Commission of the European Communities (2003g). Energy: Commission proposes decisive action on Infrastructure and Security of Supply, press release, IP/03/1694, Brussels.

Commission of the European Communities (2003h). *Proposal for a Decision of the European Parliament and of the Council laying down guidelines for trans-European energy networks and repealing Decisions No 96/391/EC and No 1229/2003/EC*, COM(2003) 742 final, Brussels.

Commission of the European Communities (2003i). *Proposal for a directive of the European Parliament and of the Council concerning measures to safeguard security of electricity supply and infrastructure investment*, COM(2003) 740 final, Brussels.

Commission of the European Communities (2003j). *Second benchmarking report on the implementation of the internal electricity and gas market*, (updated report incorporating Candidate Countries), commission staff working document, SEC(2003) 448, Brussels.

Commission of the European Communities (2003k). *Undergrounding of Electricity Lines in Europe*, background paper, Brussels.

Commission of the European Communities (2003l). "European energy and transport trends to 2030." Luxembourg: Office for Official Publications of the European Communities.

Commission of the European Communities (2004a). *Communication from the Commission to the Council and the European Parliament Communication on Critical Infrastructure Protection in the fight against terrorism*, COM(2004)704, Brussels.

Commission of the European Communities (2004b). *Third benchmarking report on the implementation of the internal electricity and gas market*, draft working paper, Directorate-General for Energy and Transport (DG TREN), Brussels.

Commission of the European Communities (2004c). "Third benchmarking report on the implementation of the internal electricity and gas market, DG TREN Draft Working Paper," Brussels: EC, DG TREN.

Commission of the European Communities (2005a). *Annual Report on the Implementation of the Gas and Electricity Internal Market*, commission report, COM(2004) 863 final, Brussels.

Commission of the European Communities (2005b). *Technical Annexes to the Report from the Commission on the Implementation of the Gas and Electricity Internal Market*, commission staff working document, SEC(2004) 1720, Brussels.

Commission of the European Communities (2005c). *Green Paper on a European Programme for Critical Infrastructure Protection*, COM (2005) 576 final, Brussels.

Confcommercio (2003). "Confcommercio su black-out: danni rilevanti per i pubblici esercizi e piccolo commercio." Press release, September 28.

CRS Report for Congress (2001a). "Critical Infrastructures and Key Assets: Definition and Identification." October 1, order code RL32631.

CRS Report for Congress (2001b). "Critical Infrastructures: Background, Policy, and Implementation." December 14, order code RL30153.

CRS Report for Congress (2003). "Critical Infrastructures: What Makes an Infrastructure Critical." January 29, order code RL31556.

De Bruijne, M. (2004). "Reliability against the odds: California's electricity crises." *1st Annual CZAEE International Conference "Critical Infrastructure in the energy sector: Vulnerabilities and protection"*, Prague.

De Jong, H.M. (2004a). "Towards a Single European Electricity market: An integral process approach.", Issuepaper PhD Research Proposal, Delft University of Technology: Section Energy & Industry. Delft.

De Jong, H.M. and R.A. Hakvoort (2004b). "Interconnectors as Gateways to the European Electricity Market." In: *Proceedings, The European Electricity Market*, Lodz (Poland), September 20-22.

De Jong, H.M. and R.A. Hakvoort (2005a). "The Dynamic Regulatory Process towards a Single European Electricity Market." In *Proceedings, The IASTED International Conference on Energy and Power Systems*, Krabi (Thailand), April 18-22.

De Jong, H.M. and R.A. Hakvoort (2005b). "Competition for transparency as a carrier of competition: Transparency needs in the European wholesale electricity markets." In *Proceedings, SNF-IAEE European Energy Conference European Energy Markets in Transition*, Bergen (Norway), August 28-30.

De Vries, L.J. (2004). "*Securing the public interest in electricity generation markets, the myths of the invisible hand and the copper plate.*" Ph.D. Dissertation, Delft University of Technology, The Netherlands.

De Vries, L.J. and Hakvoort, R.A. (2002). "An Economic Assessment of Congestion Management Methods for Electricity Transmission Networks." *Journal of Network Industries* 3 (4), 425-466.

De Vries, L.J. and Hakvoort, R.A. (2003). "The question of generation adequacy in liberalized electricity markets". In: *Proceedings, 26th IAEE International Conference*, Prague.

DG TREN (2002). *Congestion Management in the EU Electricity Transmission Network – status report*.

Directive 2001/77/EC of the European Parliament and of the Council of 27 September 2001 on the promotion of electricity produced from renewable energy sources in the internal electricity market. *Official Journal of the European Union* 2001 L283, 33-40.

Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003, concerning common rules for the internal market in electricity and repealing Directive 96/92/EC. *Official Journal of the European Union*, L 176: 37-55, 2003.

Directive 96/92/EC of the European Parliament and of the Council of 19 December 1996 concerning common rules for the internal market in electricity. *Official Journal of the European Union*, 1997, L 27, 20-29.

Dobson, I., B. Carreras, J. Thorp (2002). "Risk, Criticality and Self-Organization in Large Blackouts involving Cascading Failure." U.S. DOE, Ed., Transmission Reliability Research Review.

Dondossola G., M. Masera, O. Lamquet (2004). "Emerging standards and methodological issues for the security analysis of the Power System information infrastructures." CRIS 2004 Conference: Securing critical infrastructures, Grenoble 25-27 October.

DTe (2004). *Decision Number: 101783\_2-76: on the application by TenneT for permission to finance the NorNed cable in accordance with section 31 (6) of the Electricity Act of 1998*. The Hague: DTe.

DTe/CREG/CRE (2005). *Regional market integration between the wholesale electricity markets of the Netherlands, Belgium and France – A consultation document prepared by DTe, CREG and CRE*. The Hague: DTe.

- Dunn M. (2005). "The socio-political dimensions of critical information infrastructure protection (CIIP)." *Int. J. Critical Infrastructures*, Vol. 1, nos. 2/3, pp. 258-269.
- EC (2001). "European Governance: A White Paper." COM (2001), 25 July 2001.
- Einarsson, S., Rausand, M. (1998). "An Approach to Vulnerability Analysis of Complex Industrial Systems". *Journal of Risk Analysis*.
- Einhorn M., R. Siddiqi, (editors) (1996). "Electricity Transmission Pricing and Technology." Kluwer Academic Publishers.
- Elkraft System (2003). "Power failure in Eastern Denmark and Southern Sweden on 23 September 2003 – Final report on the course of events." Ballerup, Denmark. Available at [www.elkraft-system.dk](http://www.elkraft-system.dk).
- EPRI (2002). "Complex Interactive Networks/Systems Initiative: First Annual Report." Palo Alto CA.
- EPRI/PIER (2002). "*California's Electricity Restructuring*." Technical Report prepared for EPRI & PIER by Mills College & Delft University of Technology; available online: [http://www.epri.com/attachments/287226\\_1007388.pdf](http://www.epri.com/attachments/287226_1007388.pdf)
- ERGEG (2004). Comments on the Proposal of Guidelines on Transmission Tariffs drafted by the European Commission, Brussels, August 10.
- Erwann, M.-K. (2003). "*New Challenges in Critical Infrastructures: A US Perspective*." working paper # 03-25, Center for Risk and Decision Processes, The Wharton School of the University of Pennsylvania.
- ETSO (2004). Web site: <http://www.etso-net.org>.
- ETSO/EuroPex (2004). "*A Joint ETSO-EuroPEX Proposal for Cross-Border Congestion Management and Integration of Electricity Markets in Europe*." Interim Report.
- Eurelectric (2004a). "Power Outages in 2003." Brussels. Available at [www.eurelectric.org](http://www.eurelectric.org)
- Eurelectric (2004b). "Statistics and Prospects for the European Electricity Sector (1980–1990, 2000–2020)," Brussels.

Eurelectric (2004c). "Latest Industry Statistics as at 31 December 2003," Brussels. Available at [www.Eurelectric.org](http://www.Eurelectric.org).

Eurelectric (2004d). "Security of Electricity supply." Discussion Paper, 2004-180-0019. Available from <http://www.eurelectric.org/>.

European Commission (1999). Council decision (1999/468/EC) of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission

European Commission (2001a). *Analysis of Electricity Network Capacities and Identification of Congestion* 2001, final report, study commissioned by the European Commission's Directorate-General Energy and Transport, Brussels.

European Commission (2001b). *Electricity liberalisation indicators in Europe* 2001, study commissioned by the European Commission's Directorate-General Energy and Transport, Brussels.

European Commission (2003a). Commission Decision of 11 November 2003 on establishing the European Regulators Group for Electricity and Gas, Brussels, 2003.

European Commission (2003b). Directorate General for Energy and Transport, *Energy infrastructures: increasing security of supply in the Union – new legislative rules proposed*, memorandum, Information and Communication Unit of DG Energy and Transport, Brussels.

European Commission (2003c). Commission Decision (2003/796/EC) of 11 November 2003 on establishing the European Regulators Group for Electricity and Gas.

European Commission (2004a). *Analysis of Cross-Border Congestion Management Methods for the EU Internal Electricity Market* 2004, final report, study commissioned by the European Commission's Directorate-General Energy and Transport, Brussels.

European Commission (2004b). "Medium term vision for the internal electricity market", Brussels-

European Commission (2004c)- Directorate General for Energy and Transport Guidelines on Transmission Tarification, Explorative Note , September 1.

European Commission (2004d) Joint Research Centre Electric System Vulnerabilities: a State of the art of Defence Technologies, IPSC, November 11.

European Commission (2004e). Directorate General for Energy and Transport, *Towards a competitive and regulated European electricity and gas market*, memorandum, Strategy, Coordination, Information and Communication Unit of DG Energy and Transport, Brussels.

European Commission (2005). European Regulators Group for Electricity and Gas 2005, *Global Assessment of the Results of the 1st Series of Mini Fora on Congestion Management and Potential Impacts on the Draft Guidelines*, Working Paper, Brussels.

European Parliament (1997). Directive 96/92/EC of the European Parliament and of the Council of 19 December 1996 concerning common rules for the internal market in electricity. *Official Journal of the European Union*, 1997, L 27, 20-29.

European Parliament (2001). Directive 2001/77/EC of the European Parliament and of the Council of 27 September 2001 on the promotion of electricity produced from renewable energy sources in the internal electricity market. *Official Journal of the European Union* 2001 L283, 33-40.

European Parliament (2003a). Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003 concerning common rules for the internal market in electricity and repealing Directive 96/92/EC, Official Journal L 176, 15/07/2003.

European Parliament (2003b). *Proposal for a directive of the European Parliament and of the Council on energy end-use efficiency and energy services*, COM(2003) 739 final, Brussels.

European Parliament (2003c). Directive 2003/55/EC of the European Parliament and the Council of 26 June 2003 concerning common rules for the internal gas market and repealing Directive 98/30/EC, Official Journal L 176, 15/07/2003.

European Parliament (2003d). Regulation (EC) No 1228/2003 of the European Parliament and of the Council of 26 June 2003 on conditions for access to the network for cross-border exchanges in electricity, OJ L 176, 15.7.2003.

European Union (2004), Website:

<http://europa.eu.int/scadplus/leg/en/cig/g4000c.htm>, 2004.

EuroPex (2005). *Guidelines on Congestion Management*. Presentation at ERGEG's Public Hearing (June 30).

Ezell, B., Farr, J., Wiese, I. (2002). „Infrastructure Risk Analysis Model.” *Journal of Infrastructure Systems*, September.

Federation of American Scientists (2003). “Critical Infrastructures - What Makes an Infrastructure Critical.” Report for the U.S. Congress. January.

Finergy (2003). “European Electricity Market Perspective.” Project Report no. 11, Helsinki.

Fletcher S.(2001). "Electric power interruptions curtail California oil and gas production." *Oil and Gas Journal*, February 13.

Ford, A. (1999). “Cycles in competitive electricity markets: a simulation study of the western United States”. *Energy Policy* (27): 637-658.

Forum Florence (2003). *Electricity Regulatory Forum of Florence 2003, Conclusions, Tenth Meeting of the European Electricity Regulatory Forum Rome, 8-9 July*.

Forum Florence (2004). *Electricity Regulatory Forum of Florence 2004, Conclusions, Eleventh Meeting of the European Electricity Regulatory Forum Rome, 16-17 September*.

Frigg, R. (2003). “Self-organised criticality—what it is and what it isn't.” *Studies In History and Philosophy of Science Part A*, vol.34, no 3, pp.613-632 - available online: [dx.doi.org/10.1016/S0039-3681\(03\)00046-3](https://doi.org/10.1016/S0039-3681(03)00046-3).

Frownfelter-Lohrke, J. E. Hunton (2002). “New opportunities for Information Systems”. *Information Systems Control Journal*, Vol 3.

G. L. Wilson, P. Zarakas (1978). "Anatomy of a Blackout." *IEEE Spectrum*, Vol. 15, No. 2, pp. 38-46, February.

German Advisory Council on Global Change (WBGU) (2000). “*Strategies for Managing Global Environmental Risks*.” Annual Report 1998, (H.-J. Schellnhuber, chairperson), Springer, Berlin, Heidelberg.

Gheorghe A. V., Dan Vamanu (2004a). “Towards QVA – Quantitative Vulnerability Assessment: a generic practical model”. *Journal of Risk Research*, Vol. 7, Issue 6, September, pp. 613-629.



- Gheorghe A. V., Dan Vamanu (2004b). "Complexity induced vulnerability." *Int. J. Critical Infrastructures*, Vol. 1, no. 1, pp. 76-86.
- Gheorghe A. V., Vamanu D. (2003). "Indicators for Vulnerability Assessment and Management of Critical Infrastructures" in *Proceedings IIASA - Disaster Risk Management*, Vienna, Austria.
- Gheorghe A., Schlöpfer M. (2004c). "Critical Infrastructures – Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures." *ETH Working Paper*. November. Zurich.
- Gheorghe A.V., Dan Vamanu (2005). "On the vulnerability of critical infrastructures: seeing it coming." *Int. J. Critical Infrastructures*, Vol. 1, nos. 2/3, pp. 216-247.
- Giesbertz, P.G.M., H.M. de Jong and J.C. van der Lippe (2005). "A regulatory view on market integration and cross border congestion management." In: *Proceedings, 2nd CIGRE / IEEE PES Symposium Congestion Management in a Market Environment*, New Orleans, October 5-7.
- GRTN (2004). "Provisional data on electricity consumption in 2003: demand up by 2.9% on 2002." Press release. Rome. Available at [www.grtn.it](http://www.grtn.it).
- Gutierrez E. (2004). "Time series analysis of European Grid Blackouts." Technical note, European Commission Joint Research Centres, Ispra.
- Haimes, Y.Y. (1998). "Risk Modeling, Assessment, and Management." New York: John Wiley & Sons.
- Haimes, Y.Y., Jiang, P (2001). "Leontief-Based Model of Risk in Complex Interconnected Infrastructures." *Journal of Infrastructure Systems* 7, 1-12.
- Hardin, G. (1968). "The Tragedy of the Commons." *Science*, 162, pp1243-1248.
- Haubrich, H.-J., Fritz, W. & Vennegeerts, H. (1999). "*Cross-Border Electricity Transmission Tariffs*." Final report, study commissioned by the European Commission's DG XVII / C1, Brussels.
- Hauer J., J. E. Dagle (1999). Consortium for Electric Reliability Technology Solutions Grid of the Future White Paper on Review of Recent Reliability Issues and system Events. Office of Power Technologies, Assistant Secretary for Energy Efficiency and Renewable Energy, U.S. Department of Energy, December.

- Hawkins, D. (2001). “*The California Report.*” PowerPoint presentation, California ISO, Oct. 2.
- Heitmeyer, C. (1996). “Formal Methods for Real-Time Computing.” Heitmeyer, C. and D. Mandrioli, editors, Vol. 5 of Trends in Software. Wiley.
- Heller, M (2001). “Interdependencies in Civil Infrastructure Systems.” The Bridge 31 (4), 9-15.
- Hesselmans, A.N. (1995). “*De ware ingenieur.*” Thesis, Delft University of Technology; Stichting Histosearch, Utrecht; ISBN 90-72105-04-4.
- Hobbs, B., Iñón, J. and Stoft, S.E. (2001). “Installed Capacity Requirements and Price Caps: Oil on the Water, or Fuel on the Fire?” *The Electricity Journal* 14 (6): 23-34.
- Holmgren, M. (2001): “*Vulnerability of Complex Infrastructures - Power Systems & Supporting Digital Communication Systems.*” Holmgren, Molin & Thedéen joint with the Centre for Safety Research, Stockholm.
- Hood, C., H. Rothstein, and R. Baldwin, (2001). “*The Government of Risk: Understanding Risk regulation Regimes.*” Oxford University Press.
- Hunt S, S. Shuttleworth (1996). "Unlocking the Grid." IEEE Spectrum, pp. 20-25. July.
- Hunt, S. (2002). “*Making competition work in electricity.*” New York: John Wiley & Sons.
- IEC 812 (1985). Analysis techniques for system reliability- procedure for failure mode and effect analysis.
- IEC (2003). Technical Report TR 62210, Power system control and associated communications – Data and communication security, May. Available from <http://www.iec.ch/>.
- IEEE (2000a). Power Engineering Society, IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security. IEEE.
- IEEE (2000b). Power: A Survey History of Electric Power Technology since 1946. Available from [http://www.ieee.org/history\\_center/](http://www.ieee.org/history_center/)
- IEEE/CIGRE (2003). “Overview on Definition and Classification of Power System Stability.” IEEE/CIGRE Joint Task Force on Stability Terms and

Definitions, CIGRE/IEEE-PES International Symposium on Quality and Security of Electric Power Delivery Systems, Montréal, Canada, October 7-10.

IEEE/CIGRE (2004a). "Definition and Classification of Power System Stability." IEEE/CIGRE: Joint Task Force on Stability Terms and Definitions, IEEE Transactions on Power Systems, 1387- 1401, Vol. 19, Issue 3, Aug. ISSN: 0885-8950.

IEEE/PSRC (2004). Working Group 13, "Transmission Protective Relay System Performance Measuring Methodology." Submitted for publication.

IEEC Europe (2004). Power market design and industrial consumers in Europe, Florence Forum, September.

Il Corriere della Sera (2003a). "Blackout, in Italia la luce torna quasi ovunque". Internet release, September 28. Available at [www.corriere.it](http://www.corriere.it).

Il Corriere della Sera (2003b). Diverse articles. Internet release, June 27. Available at [www.corriere.it](http://www.corriere.it).

Il Sole 24 Ore (2003). Diverse articles. Internet release, September 28. Available at <http://www.ilsole24ore.com/>.

Ilic M., F. Galiana, L. Fink, (editors) (1998). "Power Systems Restructuring: Engineering and Economics." Kluwer Academic Publishers.

Joskow, P. and Kahn, E. (2002). "A Quantitative Analysis of Pricing Behavior in California's Wholesale Market During Summer 2000". *The Energy Journal* 23 (4): 1-35.

Kariuki, K.K. and Allan, R.N. (1996a). "Evaluation of reliability worth and value of lost load." *IEE Proceedings on Generation, Transmission and Distribution* 143 (2): 171-180.

Kariuki, K.K. and Allan, R.N. (1996b). "Factors affecting customer outage costs due to electric service interruptions." *IEE Proceedings on Generation, Transmission, Distribution* 143 (6): 521-528.

Klaar, D. and Panciatici, P. (2004). *Collaboration between European Transmission System Operators for Day Ahead Congestion Management*. Cigré.

Kleindorfer, P. (2004). "Economic Regulation under Distributed Ownership: The Case of Electric Power Transmission." Paper, written as part of an overall assessment of the August 14, 2003 blackout, Center for Risk Management and Decision Process, The Wharton School of the University of Pennsylvania.

- Knops, H.P.A., De Vries, L.J. and Correljé, A.F. (2004). “*Energiekeuze(s) belicht Beleidskeuzes voor de inrichting van de elektriciteits- en de gassector in Nederland.*” The Hague: Wetenschappelijk Instituut voor het CDA.
- Kok, Wim (2004). “*Facing the Challenge—The Lisbon strategy for growth and employment.*” Report from the High Level Group, European Communities; ISBN 92-894-7054-2; available online: [http://europa.eu.int/growthandjobs/pdf/kok\\_report\\_en.pdf](http://europa.eu.int/growthandjobs/pdf/kok_report_en.pdf)
- Kröger, W. (2004). “The Multiple Dimensions of Risk within Critical Infrastructures.” Presentation at the annual SRA meeting Palm Springs, USA, December
- Kubicek M., M. Marek (1983). “Computational Methods in Bifurcation Theory and Dissipative Structure.” Springer-Verlag.
- Kumamoto H., E.J. Henley (1996). “Probabilistic Risk Assessment and Management for Engineers and Scientists.” 2nd Edition, IEEE Press.
- Kupers R. (2001). “What Organizational Leaders Should Know about the New Science of Complexity.” *Complexity*, John Wiley & Sons, Vol. 6, No.1.
- La Repubblica (2003). Diverse articles. Internet release, September 28. Available at <http://www.repubblica.it>.
- Laprie J. C.(1995). “Dependability - its attributes, impairments and means”, in Predictably Dependable Computing Systems, B. Randell, J.C. Laprie, H. Kopetz, B. Littlewood (eds.), Springer. pp. 3-24.
- Laprie J.C. (1992). “*Dependability: Basic Concepts and Terminology.*” J.C. Laprie (ed), Springer-Verlag, New York.
- Le Du, M., B. Rassinoux, P. Cochet, (2002). « The French power network facing the 1999 storms.” *Power Systems and Communications Infrastructures for the future*, Beijing.
- Little, R.G. (2003). “Towards More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems.” Proceedings of the 36th Hawaii International Conference on System Sciences, IEEE Computer Society.
- Los Alamos National Laboratory (2004). Website, visited on April, 22. 2004. <http://public.lanl.gov.bwb>.

- Luijijf, H., Klaver, M. (2002). "In Bits and Pieces - Vulnerability of the Netherlands ICT-infrastructure and Consequences for the Information Society." TNO Physics and Electronics Laboratory.
- M.J.G. van Eeten (2003). "Networked Reliability.", in: M.P.C. Weijnen, E.F. ten Heuvelhof, P.M. Herder, M. Kuit (eds.), *Next Generation Infrastructures*, Delft, pp. 117-129.
- Masera, M. (2002). "An Approach to the Understanding of Interdependencies." International Institute for Critical National Infrastructures. September.
- Mayer (2003). "Regulation of Security of Supply." Presentation at Conference "Current Challenges facing Electricity, Cambridge, September.
- Merriam Webster's Collegiate Dictionary (10th Ed.), Springfield, MA, (1993).
- Mili L., Q. Qiu, A. Phadke (2004). "Risk assessment of catastrophic failures in electric power systems." *Int. J. Critical Infrastructures*, Vol. 1, no. 1, pp. 38-64.
- Morgan, M. G. and M. Henrion, (1992). "*Uncertainty. A guide to dealing with uncertainty in Quantitative Risk and Policy Analysis.*" Cambridge University Press.
- Morgan, M. G., H. K. Florig, M. L. Dekay, and P. Fischbeck (2000). "Categorizing risk for risk ranking." *Risk analysis*, 20, 49-58.
- Moteff, J. et al. (2003): "What makes an Infrastructure Critical?" Report for Congress RL31556, Library of Congress, Washington DC.
- Narich R. (2005). "Critical infrastructure, continuity of services and international cooperation." in *Int. J. Critical Infrastructures*, Vol. 1, nos. 2/3, pp. 293-298.
- National Grid Company plc., (2003). "Investigation Report into the Loss of Supply Incident affecting parts of South London at 18:20 on Thursday, 28. August 2003." Warwick. Available at [www.nationalgrid.com](http://www.nationalgrid.com).
- National Research Council (Committee on Risk Categorization), (1996). "*Understanding Risk: Informing Decisions in a Democratic Society.*" National Academy Press.
- National Security Telecommunications Committee Information Assurance Task Force: Electric Power Risk Assessment. March (1997).

- National Strategy for Homeland Security (2002), Office of Homeland Security, Washington D.C., July 2002, pg. 34
- NERC (1989). Disturbance Reports. North American Electric Reliability Council, New Jersey, 1984-1988. <http://www.nerc.com/dawg/database.html>.
- NERC (2005). Web site: <http://www.nerc.com>.
- Neuhoff, K. and De Vries, L.J. (2004). "Insufficient incentives for investment in electricity generation". *Utilities Policy* 12 (4): 253-267.
- New Zealand State Services Commission (2000): E-Government - Protecting New Zealand's Infrastructure from Cyber-Threats. December.
- Nordel (2004) "Nordic Grid Code 2004 (Nordisk regelsamling)." Vällingby, Sweden.
- NordPool (2004). Interim review 1 january-30 june 2004, website: <http://www.nordpool.no/information/publications/Nord%20Pool%20Q2004.pdf>
- North, M. (2001). "Agent-based modeling of complex infrastructures," in Proc. Workshop on Simulation of Social Agents: Architectures and Institutions, Chicago, IL, 2000, pp. 239-251, published by Argonne National Laboratory, June.
- Nozick L. et al., (2005). "Assessing the performance of interdependent infrastructures and optimizing investments." *Int. J. Critical Infrastructures*, Vol. 1, nos. 2/3, pp. 144-155.
- Nye and Donahue (2000). "Governance in a Globalising World." Brookings Institution, Washington.
- O'Riordan, B. Wynne (1987) in "Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond". P.R. Kleindorfer, H.C. Kunreuther (eds.), Springer,.
- Ocaña, C. (2002). "Regulatory Reform in the Electricity Supply Industry: An Overview." Working paper, IEA.
- OECD (2001). "Governance in the 21st Century". OECD Publications, Paris.
- OECD (2003). "Report on Emerging Risks in the 21st Century – An Agenda for Action." OECD Publications, Paris.
- OECD/IEA (2001). "Regulatory Institutions in Liberalised Electricity Markets." Series in Energy Market Reform, OECD/IEA Publications, Paris.

OECD/IEA (2002). “*Security of Supply in Electricity Markets – Evidence and Policy Issues.*” Series in Energy Market Reform, OECD/IEA Publications, Paris.

Ofgem (2004). “Report on support investigations into recent blackouts in London and West Midlands.” London. Available at [www.ofgem.gov.uk](http://www.ofgem.gov.uk).

*Overview of the Potential for Undergrounding the Electricity Networks in Europe* 2003, final report, study prepared for the European Commission’s Directorate-General Energy and Transport, Brussels.

Palmer, J., Boardman, B., Buerger, V. & Timpe C. (2003). “*Consumer Information on Electricity.*” final report of the project ‘Consumer Information on Electricity’ (CIE), project sponsored by the European Commission, Brussels.

PCCIP (1997). “Critical Foundations: Protecting America’s Infrastructures.” President’ Commission on Critical Infrastructure Protection, Washington D.C.

Pélissier, R. (1971). “Les réseaux d’énergie électrique.” Paris : Dunod.

Pérez-Arriaga, I.J. & Olmos Camacho, L. (2003). “*Cost components of cross border exchanges of electricity.*” Final report, project extension prepared for the European Commission’s Directorate-General Energy and Transport, Brussels.

Pérez-Arriaga, I.J., Olmos Camacho, L., Rubio Odérez F.J. (2002). “*Benchmark of Electricity Transmission Tariffs.*” Final report, report prepared for the European Commission’s Directorate-General Energy and Transport, Brussels.

Pérez-Arriaga, I.J., Olmos Camacho, L., Rubio Odérez F.J. (2002). “*Cost components of cross border exchanges of electricity.*” Final report, report prepared for the European Commission’s Directorate-General Energy and Transport, Brussels.

Pérez-Arriaga, I.J., Perán Montero, F. and Rubio Odérez, F.J. (2002). “*Benchmark of Electricity Transmission Tariffs.*” Report prepared for the Directorate-General for Energy and Transport of the European Commission. Madrid: Universidad Pontificia Comillas.

Perrow, C. (1984). “*Normal accidents: Living with high risk technologies.*” Princeton University Press.

Phadke A. (2004). “Hidden failures in electric power systems.” in Int. J. Critical Infrastructures, Vol. 1, no. 1, pp. 64-76.

- Phadke, A. G., J. S. Thorp (1996). "Expose Hidden Failures to Prevent Cascading Outages." IEEE Computer Applications in Power, pp. 20-23, July.
- Phadke, A.G. (2001). "Power Line Communication for Defense against Catastrophic Failures of Complex Interactive Power Networks." Keynote Address at ISPLC Conference, April, Malmo, Sweden.
- Qiang Liu, Jenq-Neng Hwang, Chen-Ching Liu (2002). "Vulnerability Assessment of Communication Network in An Electric Power System." University of Washington.
- Regulation (EC) No 1228/2003 of the European Parliament and of the Council of 26 June 2003, on conditions for access to the network for cross-border exchanges. *Official Journal of the European Union* 2003 L 176, 1-10.
- Reinema R. (2004). ACIP Analysis & Assessment for Critical Infrastructure Protection, Fraunhofer Institute, Malta Lecture, Malta, January 29-30.
- Renn, O. (2005). "White Paper on Risk Governance – Towards an Integrative Approach." Prepared for the International Risk Governance Council, September.
- Rinaldi, S.M.(2004). "Modeling and Simulating Infrastructures and Their Interdependencies". Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE Computer Society.
- Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). "Critical Infrastructure Interdependencies." IEEE Control Systems Magazine 21.
- Rosenau, J.N. & Czempiel, E.-O. (1992). „*Governance without Government: Order and Change in World Politics.*” Cambridge University Press, Cambridge.
- Roth C., Michael Siegrist (2001). "Cyber threats in the field of CIP: trust and risk perception." University of Zurich, October, A study for CRN.
- Sage, A.P (1992). "Systems Engineering." New York: John Wiley & Sons.
- Salmeron, J., Wood, K., Baldick, R. (2004). "Analysis of Electric Grid Security Under Terrorist Threat." Naval Postgraduate School Monterey.
- Sambeek, E., Beurskens, L. and Roos, C. (2004). "Background study – Balancing system of the Netherlands," Petten/Amsterdam: ECN. Available at [www.greennet.at](http://www.greennet.at).



- Samotyi, M. (2003). *“Power System Infrastructure for a Digital Society: Creating the New Frontier.”* M. Samotyi, CIGRE Symposium on Quality and Security of Power Delivery Montreal.
- Samotyj, M., Von Dollen, D., Howe, B (2002). “Powering the Digital Revolution - Electric Power Security, Quality, Reliability and Availability in the Digital Age.” International Institute for Critical National Infrastructures, Virginia.
- Schneider, K., C.-C. Liu, (2004). “A proposed method of partially-decentralised power system protection.” International Conference on Securing Critical Infrastructures, CRIS 2004, Grenoble, France, October 25-27, 2004.
- Selcuk, A.S., Y.M.Semih (1999). “Reliability of lifeline networks under seismic hazard.” *Reliability Engineering System Safety*. 65(3):213-227.
- SFOE (2003). “Report on the Blackout in Italy on September 2003.” Bern. Available at [www.energie-schweiz.ch](http://www.energie-schweiz.ch).
- Shuttleworth, G., Falk, J., Meehan, E., Rosenzweig, M. and Fraser, H. (2002). *“Electricity Markets and Capacity Obligations, A Report for the Department of Trade and Industry.”* London: NERA.
- Simpson D. et al. (2005). “Framing a new approach to critical infrastructures modeling and extreme events.” *Int. J. Critical Infrastructures*, Vol. 1, nos. 2/3, pp. 125-144.
- Slovic, P. and E. U. Weber (2002). “Perceptions of Risk posed by extreme events.” *Risk management Strategies in an uncertain world*, New York.
- Sobajic D., Hirsch P. (2004). “Security and reliability of the United States Electricity Infrastructure.”. CRIS October 25-27, Grenoble, France.
- Stamp J. et. al (2003). “Common Vulnerabilities in Critical Infrastructures Control Systems.” Sandia National Laboratories, Albuquerque, May 22, SAND2003-1772C.
- Stoft, S.E. (2002). *“Power System Economics: Designing Markets for Electricity.”* Piscataway (NJ): IEEE Press.
- Stoll H.G. (ed.) (1989). “Least-Cost Electric Utility Planning.” New York: John Wiley.
- Svenska Kraftnät (2003). “The black-out in southern Sweden and eastern Denmark, September 23, 2003.” Vällingby, Sweden. Available at [www.svk.se](http://www.svk.se).

- Talukdar, S., Apt, J., Ilic, M., Lave, L., Morgan, G (2003). "Cascading Failures: Survival vs. Prevention." *The Electricity Journal*, December.
- Tamronglak S. (1994). "Analysis of Power System Disturbances due to Relay Hidden Failures." Ph.D. Thesis. Virginia Polytechnic Institute and State University, March.
- Tamronglak S., S. H. Horowitz, A. G. Phadke, J. S. Thorp (1996). "Anatomy of Power System Blackouts: Preventive Relaying Strategies." *IEEE Transactions on Power Delivery*, Vol. 11, No. 2, pp. 708-715, April.
- Ten Heuvelhof, E.F., M. Kuit & H.D. Stout (2004). "Innovations in Infrastructures: New solutions to increase the reliability of vital infrastructures" Conference Papers, TTE Conference, pp.6-17. [www.tteconference.nl](http://www.tteconference.nl).
- TenneT (2003). "Capacity increase not possible yet," news release, October 17, available at [www.tennet.org](http://www.tennet.org).
- The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Direction 61, The White House, Washington D.C., May 22, (1998).
- The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, The White House, Washington D.C., February (2003), <http://www.whitehouse.gov/pcipb/physical.html>.
- Thissen, Wil A., H. Paulien, M. Herder (2003). "Critical Infrastructures - State of the Art in Research and Application." Kluwer Academic Publisher, Boston / Dordrecht.
- Thorp J.S., A.G. Phadke (1999). "Protecting Power Systems in the Post-Restructuring Era." *IEEE Computer Applications in Power*, pp. 33-37, January.
- Thorp J.S., A.G. Phadke, S.H. Horowitz, and S. Tamronglak (1998). "Anatomy of Power System Disturbances: Importance Sampling" *Electrical Power & Energy Systems*, Vol. 20, No. 2, pp. 147-152.
- U.S. Department of Energy (2002). "Vulnerability Assessment Methodology - Electric Power Infrastructure." September.
- U.S. Department of Energy (2003). "Grid 2030 - A National Vision for Electricity's Second 100 Years." July.

U.S.-Canada Power System Outage Task Force (2003). "Interim Report: Causes of the August 14th Blackout in the United States and Canada." November, available at [www.nerc.com/~filez/blackout.html](http://www.nerc.com/~filez/blackout.html).

UCTE (2004). "Operation Handbook." Brussels. Available from <http://www.ucte.org/>.

UCTE (2004a). "Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy." Brussels. Available at [www.ucte.org](http://www.ucte.org).

UCTE (2004b). Web site: [www.ucte.org](http://www.ucte.org)

UCTE (2004c). "Operational Handbook: I – Introduction to the UCTE Operation Handbook (OpHB)." Final Draft. [http://www.ucte.org/pdf/ohb/introduction\\_v24.pdf](http://www.ucte.org/pdf/ohb/introduction_v24.pdf).

UCTE (2004d). "The UCTE operation handbook - 2nd progress report." Presentation at the 11th Regulatory Forum 16/17 September.

UCTE (2005a). "UCTE System Adequacy Forecast 2005 – 2015." Brussels.

UCTE (2005b). Web site: [www.ucte.org](http://www.ucte.org).

Unal, C., Werley, K., Giguere, P. (2002). "Modeling of Interdependent Infrastructures." Los Alamos National Laboratory Report (LA-UR-02-0856).

Unindustria Padova (2003). "Black-out: Bonàiti, 'vulnerabilità' inaccettabile. Serve una vera politica energetica". *Unindustria Padova (press release)*, September 29. Available at <http://www.unindustria.pd.it/>

*Unit Costs of constructing new transmission assets at 380kV within the European Union, Norway and Switzerland 2002*, final report, study prepared for the European Commission's Directorate-General Energy and Transport, Brussels.

Ursu I., Vamanu D., Gheorghe A., Purica I.I. (1985). "Socioeconomic Risk in Development of Energy Systems." *Risk Analysis* 5, 315.

USA Patriot Act, Public Law 107-56, October 26, 2001.

USAtoday.com (2004). "A month from Games, major power blackout hits Greece." Internet release, July 12. Available at [www.usatoday.com](http://www.usatoday.com).

Van der Linde, C. (2004). "*Study on Energy Supply Security and Geopolitics.*" final report, study prepared for the European Commission's Directorate-General Energy and Transport, Brussels.

- Van Grembergen, W., S. De Haes, I. Amelinckx (2003). "Using COBIT and the Balance Scorecard as instruments for service level management." *Information Systems Control Journal*, Vol. 4.
- Van Mieghem, P. (2005). "Robustness of Large Networks." To be published in: IEEE SMC 2005 Conference on Systems, Man and Cybernetics; Hawaii, USA, October.
- Verbund-APG (2004). "Disturbance in Central Part of UCTE Power System." Vienna. To be published.
- Verton, A. (2001). "Experts debate U.S. power grid's vulnerabilities to hackers." *Computerworld*, March 2.
- Vournas, C. (2004). "Technical summary on the Athens and Southern Greece Blackout of July 12, 2004." Athens: National Technical University.
- Weare, C. (2003). "*The California Electricity Crisis: Causes and Policy Options.*" San Francisco: Public Policy Institute of California. Obtained from: [www.ppic.org/content/pubs/R\\_103CWR.pdf](http://www.ppic.org/content/pubs/R_103CWR.pdf).
- Wenger A., Metzger J., Dunn, M. (2002). „Critical Information Infrastructure Protection Handbook." ETH Zurich.
- Wijnia, Y. C. and P. M. Herder (2004). "Modeling Interdependencies in electricity infrastructure risk." *1st Annual CZEEE International Conference "Critical Infrastructure in the energy sector: Vulnerabilities and protection"*, Prague.
- Wijnia, Y. C. and P. M. Herder (2005). "Options for real options: Dealing with uncertainty in investment decisions for electricity networks." presented at International conference on Systems, Man and Cybernetics, Hawaii.
- Willis, K.G. and Garrod, G.D. (1997). "Electric Supply Reliability, Estimating the Value of Lost Load." *Energy Policy* 25 (1): 97-103.
- Yanner Bar-Yam (1992). "Dynamics of Complex Systems." Addison-Wesley, Reading, Mass.

## Glossary

***Cascading failure*** occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure.

***Common cause failure*** occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause.

***Critical Infrastructures*** are defined as the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security, the smooth functioning of governments at all levels, and society as a whole (adopted from the President's Commission on Critical Infrastructure Protection, USA 1996).

***Dependency*** is defined as a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other (adopted from Kelly, IEEE 2001).

***Digitalization*** means the process automation related activities as well as the intensive use of various kind of computers and modelling work associated with operational, tactical, as well as the strategic phase of a given infrastructure.

***Escalating failure*** occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity or the time for recovery or restoration of the second failure.

***Hazard*** is a source of danger to a system; a possibility of incurring loss.

***Interdependency*** is defined as a bi-directional relationship between two infrastructures, through which the state of each infrastructure influences or is correlated to the state of the other (adopted from Kelly, IEEE 2001).

***Pervasive computing***, or so called *ubiquity of computing* (in contrast with the ubiquity of digitalization) indicates that computing is no longer a

discrete activity bound to a desktop, but rather microscopically small computers integrated into a large variety of different sort of objects and their omnipresence in the daily life.

**Reliability** indicates the capability of a system its design function within a given time interval under specified operational conditions.

**Resilience** refers to a system's ability to accept and withstand unexpected applications and operational conditions. The system may change and adapt to the new situation. (adopted from Einarsson and Rausand, SRA 1998)

**Risk** is defined as the combination of the probability/likelihood of an accidental event with the subsequent losses.

**Robustness** is defined as a system's ability to endure threats and survive accidental events that originates both within and outside the system's boundaries, and if disturbed, return to a state where the operating characteristics correspond to the assigned function. (adopted from Einarsson and Rausand, SRA 1998)

**Safety** indicates an acceptable level of risk build or an absence of potential damaging consequences.

**Security** indicates the internal capability of a system to protect itself against potential negative impacts.

**System of Systems** is a way of describing the compound of several interdependent critical infrastructures showing characteristics of one single system but without having a centralized control.

**Ubiquity** indicates "the capacity of being everywhere or in all places at the same time" (Oxford) or the "presence everywhere or in many places especially simultaneously" (Merriam Webster Dictionary)

**Vulnerability** is defined as the property of an (infrastructure) system that limits its ability to endure threats and survive accidental events that originates both within and outside the system's boundaries (adopted from Einarsson and Rausand, SRA 1998)

**Threat** is defined as a specified hazard.

# SUBJECT INDEX

## A

Adequacy • 55, 252  
Ageing • 7, 79, 128  
Availability • 40, 183

## B

Blackouts  
costs • 331  
general • 3, 6, 98, 150, 193  
lessons learned • 108, 164, 211  
sequence of events • 164, 169,  
173, 182, 185  
societal impact • 160, 168, 335

## C

Cascading failures • 84, 111  
CII (Critical Information  
Infrastructures)  
general aspects • 271  
legal aspects • 295  
Comitology • 74  
Complexity • 2, 8, 25, 87  
Confidentiality • 103, 256  
Congestion management • 64, 181  
Contingency management • 60, 107  
Counter trading • 65, 234  
Critical infrastructures  
classification • 201  
criticality • 25  
definition •  
general • 26  
resilience •  
Cyber(threats) • 91, 230, 291

## D

Decentralization • 28, 48  
Denial of service • 112  
Dependability • 256, 257  
Deregulation • 19, 195  
Digitalization • 94, 206, 221, 242  
Distributed generation • 46, 57  
Distribution • 31, 41, 42, 82

## E

E+I paradigme • 85  
ECEI (European Critical Electricity  
Infrastructure)  
general • 117  
ECSEP (European Council for the  
Security of Electric Power) • 153,  
159, 161, 162  
Electric power system • 47, 51  
Electricity deregulation • 55  
ETSO • 62

## F

Florence Forum • 72

## G

Generation (electricity) • 40, 83  
Governance • 92  
Grid • 22

**H**

Human factor • 130

**I**

ICS • 85, 86

Infrastructures

critical • 94

definitions • 4

general • 2

Integrity • 103, 105

Interdependencies • 8, 23, 35, 191,  
210, 244, 275, 284

Internationalization • 3, 92, 193, 259

Investment cycles • 55

**M**

Market liberalization • 2, 164, 177,  
195, 198, 203, 213, 216

Multi criteria decision analysis • 205,  
276

**N**

N-1 criterion • 110, 171, 177,  
189,

Natural hazards • 128, 132

Near misses • 79, 163, 185, 193

Network complexity

physical • 20, 47

social • 21, 53

NIMBY (Not in my back yard) • 220

Nordel • 62, 317, 328

**P**

Public values • 32, 155, 271

Public private partnership • 115,  
162, 296

**R**

Re-despatching • 64

Regulatory process • 54, 70, 73, 75,  
76

Reliability • 12, 41, 44, 53, 255

Renewables • 202, 208, 216

Resilience (robustness) • 20, 210,  
273, 284

Risk

assessment • 98, 104, 111

aversion • 57

definition • 115, 118, 256

factors • 79

framing • 274, 303, 305, 311

general • 6, 32, 33, 110, 131

governance • 34, 134, 135, 210, 274,  
303, 319

management • 25, 134

perception • 119, 293, 304

profiling • 303

systemic • 34, 242

values • 119

Root cause • 163, 166, 171, 175,  
177, 184

**S**

SCADA • 89

Security

criteria • 80-82

culture • 234, 244

general • 21, 68, 80, 150, 229, 261



standards • 261  
Self regulation • 142  
Stability • 44, 46, 250, 255  
Systemic failures • 34, 128, 132  
System-of-systems • 15, 36

## **T**

Tariff structure • 204, 211, 216, 224,  
231,  
Taxonomy of risk • 117  
Terrorism • 25, 109, 141  
Threat  
assessment • 275, 284  
general • 20, 32, 81, 105, 110  
Timeliness • 106  
Transmission • 40, 41  
TSO (Transmission System  
Operator) • 39, 43, 44  
TSOI • 62

## **U**

UCTE • 38, 39, 68, 71  
UKTSOA • 63, 138  
Unbundling • 50, 139, 204, 212

## **V**

Vulnerability  
assessment • 47, 114, 198  
definition • 256  
general • 32, 33, 110, 149, 187,  
193

## **W**

Welfare function • 58

# TOPICS IN SAFETY, RISK, RELIABILITY AND QUALITY

---

1. P. Sander and R. Badoux (eds.): *Bayesian Methods in Reliability*. 1991 ISBN 0-7923-1414-X
2. M. Tichý: *Applied Methods of Structural Reliability*. 1993 ISBN 0-7923-2349-1
3. K.K. Aggarwal: *Reliability Engineering*. 1993 ISBN 0-7923-2524-9
4. G.E.G. Beroggi and W.A. Wallace (eds.): *Computer Supported Risk Management*. 1995 ISBN 0-7923-3372-1
5. M. Nicolet-Monnier and A.V. Gheorghe: *Quantitative Risk Assessment of Hazardous Materials Transport Systems*. Rail, Road, Pipelines and Ship. 1996 ISBN 0-7923-3923-1
6. A.V. Gheorghe and R. Mock: *Risk Engineering*. Bridging Risk Analysis with Stakeholders Value. 1999 ISBN 0-7923-5574-1
7. I.N. Vuchkov and L.N. Boyadjieva: *Quality Improvement with Design of Experiments*. A Response Surface Approach. 2001 ISBN 0-7923-6827-4
8. A.V. Gheorghe (ed.): *Integrated Risk and Vulnerability Management Assisted by Decision Support Systems*. Relevance and Impact on Governance. 2005 ISBN 1-4020-3451-2
9. A.V. Gheorghe, M. Masera, M. Weijnen and de L. Vries (eds.): *Critical Infrastructures at Risk*. Securing the European Electric Power System. 2006 ISBN 1-4020-4306-6