white paper on

MANAGING AND REDUCING SOCIAL VULNERABILITIES

FROM COUPLED CRITICAL INFRASTRUCTURES

international risk governance council

international risk governance council

The International Risk Governance Council is a Private Foundation established under Articles 80 and thereafter of the Swiss Civil Code.

international risk governance council
7-9 Chemin de Balexert, Châtelaine
CH-1219 Geneva, Switzerland
tel +41 (0)22 795 1730
fax +41 (0)22 795 1739
www.irgc.org

white paper no. 3

MANAGING AND REDUCING SOCIAL VULNERABILITIES
FROM COUPLED CRITICAL INFRASTRUCTURES

MEMBERS OF THE IRGC SCIENTIFIC AND TECHNICAL COUNCIL

Members of the IRGC Scientific and Technical Council are drawn from a wide variety of experience, background, country, and discipline and, as a result, assure the IRGC's quality and independence. IRGC treats the composition of the Scientific and Technical Council as its first technical priority.

- Prof. Dr. M. Granger Morgan, University and Lord Chair Professor in Engineering and Head, Department of Engineering and Public Policy, Carnegie Mellon University, USA (Chairman)
- Dr. Lutz Cleemann, Managing Director of the Allianz Technology Centre, Ismaning, Germany
- Prof. Jean-Pierre Contzen, Chair Professor, Technical University of Lisbon, Portugal, Chairman, Von Karman Institute for Fluid Dynamics, Belgium, and Chairman, Institute of Advanced Studies, UN University, Japan
- Academician Konstantin Frolov, Director, Mechanical Engineering Research Institute, Russian Academy of Sciences, Moscow, Russian Federation
- Prof. Dr. Manuel Heitor, Secretary of State for Science, Technology and Higher Education, Portugal
- Prof. Dr. Hou Yunde, Director, State Center for Viro-Biotech Engineering and State Key Laboratory for Molecular Virology and Engineering, Beijing, People's Republic of China
- Prof. Dr. Ola M. Johannessen, Director, Nansen Environmental and Remote Sensing Center, Bergen, Norway
- Prof. Dr. Fotis Kafatos, Chair Professor, Insect Immunogenetics, Imperial College of Science, Technology and Medicine, London, UK and Chairman, European Research Council
- Prof. Dr. Wolfgang Kröger, Director of the Laboratory for Safety Analysis, ETH Zurich, Switzerland (IRGC Founding Rector)
- Dr. Patrick Lagadec, Director of Research, Ecole Polytechnique, Paris, France
- Dr. Jeffrey A. McNeely, Chief Scientist, World Conservation Union, Geneva, Switzerland
- Prof. Dr. D. Warner North, NorthWorks, Inc. and Consulting Professor in the Department of Management Science and Engineering, Stanford University, USA
- Prof. Dr. Norio Okada, Disaster Prevention Research Institute, Kyoto University, Japan
- Prof. Dr. Ortwin Renn, Chair of Environmental Sociology at the University of Stuttgart and Director of the Research Institute 'DIALOGIK', Germany
- Dr. Mihail Roco, National Science and Technology Council's subcommittee on Nanoscale Science, Engineering and Technology and Senior Advisor for Nanotechnology at the National Science Foundation, USA
- Prof. Dr. Joyce Tait, Director of INNOGEN, the ESRC Centre for Social and Economic Research on Innovation in Genomics, University of Edinburgh, UK
- Dr. Bernard Tinturier, Scientific Advisor to the President, Electricité de France, Paris, France
- Prof. Dr. Hebe Vessuri, Head of the Department of Science Studies at the Venezuelan Institute of Scientific Research, Caracas, Venezuela
- Dr. Timothy Walker, former Director General, Health and Safety Executive, UK

FOREWORD – ABOUT IRGC AND THIS WHITE PAPER

The International Risk Governance Council (IRGC), a private, independent, not-for-profit Foundation based in Geneva, Switzerland, was founded in 2003. Our mission is to support governments, industry, NGOs and other organisations in their efforts to understand and deal with major and global risks facing society and to foster public confidence in risk governance.

The establishment of IRGC was the direct result of widespread concern within the public sector, the corporate world, academia, the media and society at large that the complexity and interdependence of an increasingly large number of risk issues was making it ever more difficult for risk decision makers to develop and implement adequate risk governance strategies. Consequently, IRGC is committed to identifying new or re-emergent problem fields for which there appear to be gaps in current risk governance structures or processes and undertaking project work which has the objective of supporting these decision makers by developing risk governance recommendations for these issues. We endeavour to work and communicate in ways that account for the needs of both developed and developing countries.

We focus on those risks, whether human induced or natural, which have international implications and have the potential for harm to human health and safety, the economy, the environment, and/or to the fabric of society at large. The issues we address are prioritised by the IRGC's Scientific and Technical Council (S&TC), whose members are all acknowledged experts in risk-related fields and are, collectively and individually, IRGC's primary asset for implementing our mission. IRGC's project work is carried out by S&TC members working with other experts in the field in question.

The risks associated with, and the vulnerabilities of, critical infrastructures have been a priority for IRGC since our founding. Our attention was drawn to them not only by the complexity of the infrastructures themselves, but also by the criticality of the services they provide and by their being subject to fundamental changes in technology and in ownership and market structures.

Our work in the field of critical infrastructures has focused both on the risks associated with individual infrastructures and the risks associated with the increasing interdependence between them – as in the use of one such critical infrastructure, information and communication technology (ICT), to monitor and control almost all other critical infrastructures. We have therefore taken an approach which examines each system and its operational and socio-economic environment separately, but which also views the interdependent infrastructures as, collectively, a highly complex 'system of systems'. All our project work in this field has been defined and undertaken by a project team led by Wolfgang Kröger, supported by members of the S&TC.

This White Paper on 'Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures' is the second in which we publish recommendations for the risk governance of a particular problem field. We have chosen to focus on five infrastructures: electric power supply, gas supply, urban water supply and waste water treatment, rail transport and systems for general information and communication services. These share a number of similarities: all involve distributed complex physical networks, are organised along similar value chains with elements embedded within the socio-political-economic framework and are subject to significant and continually evolving risk-shaping factors and contextual changes.

In this White Paper we provide an overview for policy-makers and opinion leaders of the physical structure and of the governance structures and processes for each of the five critical infrastructures. We also summarise their vulnerabilities and the main drivers of these vulnerabilities, as well as possible political and institutional short-comings. Based on our findings, we outline a number of technical, management and organisational strategies and policy options that may help to reduce the probability of disruption to these systems and consequent interruptions to the vital services they supply.

We follow our look at the individual infrastructures by assessing their characteristics (including their levels of interdependence with other infrastructures), their criticality and the adequacy of their risk governance. From this assessment we conclude that, at least in much of Europe and North America, the electric power and ICT infrastructures are both highly critical and suffer from inadequate risk governance. (We acknowledge that such a conclusion may be different for other parts of the World.) We offer, additionally, some suggestions for areas in which further study may be needed before definitive policy recommendations can be made.

This White Paper, in common with all official IRGC documents, has been subject to a formal and rigorous external peer review which has included the views of experts from within the industrial sectors responsible for these five infrastructures. We are therefore confident of both the theoretical and practical bases for the policy options that we recommend.

This document has been informed by and draws on IRGC's approach to risk characterisation and risk governance and on the knowledge of members of our S&TC and that of many experts with whom we have consulted. It also draws on earlier project work performed for IRGC by a group of experts from the Swiss Federal Institute of Technology in Zurich (ETH), the European Commission's Joint Research Centre in Ispra, and the Technical University of Delft. This approach reflects the 'expertise collégiale' by which we undertake all our project work. We remain open and look forward to receiving and acting on knowledge and thoughts from people who may not have been a part of the process so far – particularly from those to whom we address the policy recommendations.

None of IRGC's work would be possible without the financial support we receive. In publishing this, our third White Paper, IRGC gratefully acknowledges all those organisations whose donations and other financial contributions provide the resources for us to undertake and publish the results of the projects that are the core of our work.

M. Granger Morgan

Chairman of IRGC's Scientific and Technical Council

ACKNOWLEDGEMENTS

This paper is a product of a collaborative effort of the Scientific & Technical Council (S&TC) of the IRGC. A major part of this has been investigation and writing by Wolfgang Kröger with the support of Jürg Birchmeier and Markus Schläpfer, members of staff at the Swiss Federal Institute of Technology Zurich (ETH), of Ernst Basler & Partner Consulting Engineers, and of Caroline Kuenzi and Emily Litten of the IRGC Secretariat. Additional input was also provided by members of staff at Carnegie Mellon University. Granger Morgan assisted with the preparation of the opening and closing chapters and with coordination of the review process.

The work benefited enormously from a study of the European electric power system and its interdependency with digitalised information and control systems undertaken by a group of experts, namely Adrian Gheorghe (ETH), Marcelo Masera (European Commission Joint Research Centre, Ispra) and Margot Weijnen and Laurens de Vries (Technical University of Delft).

Significant feedback was also given by members of the S&TC, in particular Konstantin Frolov, Norio Okada, Timothy Walker, Jean-Pierre Contzen (who also arranged for very helpful feedback from staff at Electrabel S.A.), Joyce Tait, Hou Yunde, Jeff McNeely, Patrick Lagadec, Bernard Tinturier, and Warner North. Substantial review comments were provided by Jim Skea (UK Energy Research Centre) and Howard Lipson (Software Engineering Institute – Carnegie Mellon University). Additional reviews and inputs were received from staff of E.ON Energie AG, E.ON Netz GmbH, and Swiss Re, from Hans Achermann (Elektrizitäts-Gesellschaft Laufenburg AG) and, particularly, from Chris Bunting, General Secretary of IRGC.

We are also grateful to Mike Moss for his assistance with the language of this report.

CONTENT OVERVIEW

Content Overview 9

Tables, Figures, and Boxes 10

1 Executive Summary 11

2 Introduction and Framing the Problem and Issues 15

3 Brief Characterisation of Five Critical Infrastructures 21

3.1 Electric Power Supply 21

3.2 Gas Supply System 29

3.3 Urban Water 33

3.4 Transport by Rail 39

3.5 Information and Communication 43

4 Technical, Management and Organisational Strategies 49

5 Policy Options 52

6 Limitations, Outlook 57

7 References 59

8 Glossary 64

TABLES, FIGURES, AND BOXES

Table 1: Illustration of the diversity of factors which can result in varying degrees of criticality for an event using disruption to, or degradation of, services provided by electrical power and urban water supply systems as examples 17

Table 2: Different water utility management models in selected countries and the EU 35

Table 3: Assessment matrix for the five infrastructures selected for this study 50

Table 4: Policy options to improve the protection of critical infrastructures 54

Figure 1: Simplified illustration of some of the different types of events that can result in the failure, or degradation, of the service provided by a critical infrastructure 18

Figure 2: Simple illustration of a few of the interactions that can occur among just the five critical infrastructures considered in this report 19

Figure 3: Trans-boundary physical energy flows (GWh) in Europe in 2005 22

Figure 4: Organisational structure of the liberalised European electricity system 24

Figure 5: Cumulative probability of North American blackouts as a function of power loss 27

Figure 6: Layered model of the gas supply infrastructure 29

Figure 7: Most important gas pipelines and LNG transportation routes in Europe 30

Figure 8: Typical components of the water supply and treatment system 34

Figure 9: System diagram of a typical electric traction rail system 39

Figure 10: Railway electricity systems in Europe 40

Figure 11: Simplified layered model of the Internet 43

Figure 12: Degree of criticality vs. adequacy of risk governance for five critical infrastructures 53

Box 1: Explanation of large-scale (critical) infrastructures 15

Box 2: Risk-shaping factors 16

Box 3: N-1 security criterion – specified for the electric power grid 26

Box 4: Operation of Swiss gas supply – with relevance to other countries 31

Box 5: Gas pipeline explosion at Ghislenghien, Belgium 33

Box 6: The Maroochy Shire sewage spill 36

Box 7: Water system disruptions following the 2003 power blackout in the US and Canada 37

Box 8: Hurricane Katrina – impacts on the New Orleans urban water system 38

Box 9: Failure of the railway control and communication system in the greater Zurich area 42

Box 10: Internet worm Code Red 44

Box 11: Internet crash in Pakistan 46

Box 12: Some specific policy recommendations 55

1 EXECUTIVE SUMMARY

Throughout the industrialised world, society depends on a set of systems that supply food, water, public health services, energy, and transport. Other systems are used to manage information and provide communications services and to remove, dispose of and recycle wastes. In at least limited ways, these systems have always been dependent on each other. However, recent decades have witnessed a much greater and tighter integration and interdependence between them – effectively the creation of a 'system of systems' which has no single owner or operator. While this has often yielded improved service and convenience and promoted greater efficiency, it has also led to increased social vulnerabilities in the face of accidental or intentional disruption. Today, a disruption or malfunction often has much greater impacts than was typically the case in the past, and can also propagate to other systems, resulting in further additional disruptions.

In this report we will focus on five critical infrastructure systems assuming that the basic resources (fuels, water, etc.) for their operation are available: 1) electric power supply; 2) gas supply; 3) urban water supply and waste treatment; 4) rail transport; and, 5) the Internet as well as information and communication technology (ICT) used to monitor and control other infrastructures. These are mutually or circularly dependent and share a number of similarities: all involve distributed complex physical and cyber networks; they are organised along similar value chains with elements embedded within the socio-political-economic framework; and, their operating strategies and end-user behaviours are subject to significant contextual changes and risk-shaping factors, both of which continue to evolve and increase in number. Our focus in this report is on North America and Europe, but many similar issues arise elsewhere around the world.

This report aims to provide pertinent information to senior public and private sector decision makers and end-user groups, to raise wider awareness of critical big-picture issues, to address contradictory aims or trade-offs and – where appropriate – to suggest and stimulate ways to improve risk governance. Some readers may also find benefit in the more extended discussions of specific infrastructures provided in the central sections of the report.

After providing a more precise explanation of critical infrastructures (see Box 1) we explore five issues:

1. What are the factors that have promoted and caused tighter integration of, and greater interdependency among, critical infrastructures?
2. What are the main drivers behind, and vulnerabilities of, this tighter integration?
3. What are the political and institutional short-comings?
4. What technical, management and organisational strategies might reduce social vulnerabilities to disruption of these systems?
5. What policy options could be used to promote improved technical, management and organisational strategies?

The factors which have promoted greater interdependency among, and tighter integration or greater vulnerability of, critical infrastructures are multifaceted in nature. They include:

- Incremental and erratic integration of smaller systems into larger systems, thus creating greater complexity and enabling the trans-boundary propagation of disturbances
- Changes in the economic, environmental, legal, and regulatory settings in which the systems operate, including economic pressures which have reduced operating margins and, thus, squeezed out slack or redundancy in systems
- Growing complexity of new and existing systems (facilitated by more capable ICT)

- Use of off-the-shelf technology, including information and control systems, motivated by short-term economic efficiency
- Lack of adequate awareness of vulnerabilities, of the limitations to achievable reliability, or of concern for low-probability but high-consequence failure modes
- Lack of adequate penalties or costs to, particularly, owners and operators if, and when, system disruptions cause broader societal consequences
- Inadequacy of back-up systems to continue operations when problems develop.

Critical infrastructures must be considered – to different degrees – as complex interconnected systems embedded in a rapidly changing environment in which market liberalisation as well as technological developments and the abandoning of legacy lower-tech systems serve as the main drivers of change. As a consequence, the systems may be operating closer to their limits.

The spectrum of threats faced by these infrastructures continues to broaden. This threat spectrum now includes a variety of natural events such as floods, technical failures and mistakes or even malicious human action, such as cyber or terrorist attacks (see taxonomy illustrated in Figure 1, Chapter 2). Often, single initiating events develop into complicated event sequences. Additionally, there are trends on the horizon which further challenge the stability of networks and the security of uninterrupted supply, such as ever-growing demand, pressure to hold down the price charged to system users, geographical extension, integration of new technologies (e.g. of intermittent renewable energy sources), and evolving attacker tools and techniques.

Western industrialised societies depend on all these infrastructures[1]. Leaders and citizens hold the system owners and operators and government regulators responsible for assuring both low price and acceptable quality, reliability and security in providing the services of these infrastructures. This paper elaborates degrees of criticality from a collective societal perspective, based on factors such as the 'scope', 'magnitude', and the 'effects of time' of a service interruption or degradation.

From this analysis we deduce that our societies are most vulnerable to disruptions of electric power supply and disruptions to, or degradation of, ICT services. We believe that the management or governance of these systems can and should be improved. It is our judgement that a significant problem for owners, managers, and regulators is that the public and many officials in government have limited knowledge of the vulnerabilities of these systems and of the risk factors that have increased during the past several decades. Raising service prices to offset the costs of reducing vulnerability is politically difficult for managers and regulators; such increases are inherently controversial and challenging to the political leadership. Improved communications about system risks and new forms of cooperation are needed within and among the several communities concerned, including the public (customers), especially those particularly interested and affected as a result of their dependence on these systems. We believe that some goals and paradigms as well as strategies, rules and standards need to be revisited in depth, and governance processes adapted to the new circumstances. Security of service supply and the impacts of extensive service interruption should be made a high-level priority for further legislation, planning and evaluation. Policies for prevention and emergency response and for compensation for losses should be reviewed and revised where needed.

A framework needs to be created aiming to achieve a better balance between conflicting social objectives such as, for example, in the trade-off between economic objectives and the provision of sufficient redundancy in systems or of redundant back-up systems and reserve supplies. The IRGC White Paper on Risk Governance provides one starting place for such analysis [IRGC 2005].

1 For some parts of the world they may be more modest concerns as compared to, for example, inadequate supply of food, water, fuel wood, and access to basic medical care.

Recent failures of and attacks on critical infrastructures have amply demonstrated their vulnerability – and hence our society's vulnerability – to a wide variety of events. Strategies to reduce system and associated social vulnerabilities must embrace technical, management and organisational issues and be based on appropriate capabilities as well as the willingness to act. Strategies must be developed with an eye to their broader implications and be holistic in nature. We believe the planning and management process for institutions and organisations responsible for critical infrastructures can be significantly improved, particularly by increased cooperation and policy making across traditional barriers, especially in situations where the infrastructure and the market environment are undergoing evolution.

The first steps in preventing detrimental events are to undertake independent failure analysis, to identify critical accidental and intentional disruption scenarios, and to recognise possible system weaknesses – including potential common-mode failures and bottlenecks – that would impair operations under such conditions. Based on our investigations to date, we believe that more comprehensive analysis is needed, including the increased use of state-of-the-art quantitative methods such as probabilistic risk analysis, systems modelling and the simulation of failures, contingencies, service interruptions and other ensuing consequences. In many cases, such tools are already available and being used among technical specialists in some sectors and/or countries. In some cases, the necessary tools may require further development for use on this more comprehensive, trans-sectorial, international scale. We believe an ongoing and iterative process of analysis using advanced tools and dialogue about risk holds great potential for improving the process of risk governance for these infrastructure systems which, in turn, should lead to better balanced systems and, where appropriate, contingency planning.

As one specific example, key security criteria (such as N-1 or N-2 rules, see Box 3) and standards need to be revisited; there also needs to be adequate provision for their application, at least for the most complex and critical infrastructures. Rules needed to assure adequate reliability in system operation and to better cope with combinations of failures must be agreed to by all parties or even be made mandatory, then implemented with adequate provisions for inspection and monitoring. Trust among the parties is a very important aspect of risk governance.

A number of critical infrastructures have grown in scale and are being used in ways that were not foreseen when these infrastructures were planned, sometimes without basic changes in operation and control. Coherent expansion planning and associated capacity expansion is essential, but is often in conflict with issues of ownership and competition between different organisations in serving competitive markets. Gradually, strategies are being evolved to reconcile these tensions but, in the case of several systems, much additional attention and closer cooperation are needed.

In addition to the above general strategies, we identify some more detailed measures and strategies specific to each of the five infrastructures studied. Furthermore, we put forward a number of policy options for further study and investigation. We believe these policy options can lead to socially desirable improvements, but they may need further analysis and evaluation; an inclusive dialogue will be an essential part of the process of developing the measures needed to reduce and control the growing risk posed by the failure of critical infrastructures.

Policy options that could be considered include:

- The creation of institutional platforms and governance processes that involve all relevant parties, including end-users
- The independent monitoring of compliance with mandatory requirements or adherence to existing industry standards

- Legal mandates for specific system structures and capabilities
- Clear delineation of responsibility and liability in the event of system failures; the creation of insurance mechanisms to compensate losses
- Tax-based and other incentives to create desired behaviours and assure adequate investments, especially in the long term
- Government interventions to support socially desirable functions that cannot be supported by market-based or other means, such as increased robustness against terrorist attacks
- The creation of institutions that identify, codify and promulgate voluntary standards and best professional design practice
- Mandating basic technology research as a 'cost of doing business' for all players.

Many countries and regions have established or will set up programmes to identify and protect critical infrastructures against threats including malicious attacks[2]. Such programmes should include and adequately address at least the five infrastructures addressed in this IRGC report.

To give two examples of our specific recommendations for the individual infrastructures, we believe that the public Internet should not be used for any function that is vital to the supervision, operation, or control of any critical infrastructure, without prior careful assessment of threats and the implementation of adequate measures to assure security against cyber attack. We also believe that, because the water system is a possible target for terrorist attack, including via poisons and pathogens, policy should include anticipating potential threats, restricting human access to critical water system components, including water works and distribution systems, and monitoring water and sewerage systems for early detection of a potential attack. Dams and other major facilities should be protected against terrorist attacks.

While it is tempting to focus exclusively on the importance of critical infrastructures and the prevention of major disruptions, one should remember that failures cannot be ruled out and that it is the services they provide, not the systems themselves, that are most valued by society. The implication of this insight is that, in addition to doing what can reasonably be done to assure the continued operation of the system, attention should also be directed at failure tolerance and increased resilience, respectively, by:

- Reducing the degree of coupling between systems when feasible
- Promoting demand management and priority setting
- Reducing restoration times with special equipment and planned procedures
- Enabling critical social services to be maintained in the face of primary system failure.

In accordance with its mission, IRGC intends to stimulate additional work needed in this vital field. Proceeding from the acknowledged limitations of this initial study we make proposals at the end of our report on elaborating the approach for risk and criticality assessment. Future work may also involve the application of our approach to other geographic regions, to other infrastructures and to a wider range of threats, such as the impact on critical infrastructures, and the services they provide, of a potential influenza pandemic.

2 For example the European Union (EU) is launching a programme for critical infrastructure protection (ECIP); a Green Paper has been published recently [EC 2005b].

2 INTRODUCTION AND FRAMING THE PROBLEM AND ISSUES

Much is being written about critical infrastructures at the present time [see, for example, the US Patriot Act 2001] but just what is meant by this term? Different authors adopt slightly different meanings, with a recent EU communication document [EC 2004] listing nine examples:

- Energy facilities and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)
- Information and communication technology (e.g. telecommunications, broadcasting, software, hardware and networks including the Internet)
- Finance (e.g. banking, securities and investment)
- Health care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services[3])
- Food (e.g. safety, production means, wholesale distribution and food industry[4])
- Water (e.g. dams, storage, treatment and networks)
- Transport (e.g. airports, ports, intermodal facilities, railways and mass transit networks, traffic control systems)
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
- Government (e.g. crucial services, facilities, information networks, assets, and key national sites and monuments).

A more formal or academic explanation of the term is given in Box 1.

Box 1: Explanation of large-scale (critical) infrastructures

Large-scale critical infrastructures:

- Are "a network of independent, large-scale, man-made systems (set of hard and soft structures) … that function collaboratively and synergistically to produce a continuous flow of essential goods and services" [PCCIP1997] and are, finally, essential for economic development and social well-being
- Are designed to satisfy specific social needs but shape social change at a much broader and complex level
- Are subject to multiple threats (technical, intentional or unintentional human, physical, natural, cyber, contextual) and pose risks themselves, e.g. electromagnetic field (EMF) emissions
- Are highly dynamic and complex and are interdependent, both physically and through a host of ICT; reliability and quality of service are determined by the integrated system performance
- Disruptions may have cascading effects (e.g. blackouts), even normal service interruptions can impose high costs in industrialised countries
- Are mostly privately-owned but have no single owner / operator / regulator; are based on different goals and logics; competition alone will not ensure the most efficient allocation of resources.

In this initial study we will focus on five of these: the electric power network; gas supply systems; urban water supply and waste water treatment; rail transport; and, general information and communication services particularly as provided by the Internet as well as ICT as used to monitor and control other infrastructures. They all involve distributed complex physical networks consisting of several layers and are organised along similar value chains, i.e:

3 To which we would also add general public health infrastructure and services.

4 To which we would add pests and animal pathogens and diseases.

- Supply and availability of resources (e.g. of fuel for plants, gas for pipelines, engines and rolling stock for trains)
- Production or processing
- Transmission or transport, typically over long distances
- Distribution (local connectors to end-users).

Box 2: Risk-shaping factors

- Market organisation (e.g. competition, oligopoly, monopoly, hybrids)
  - Transition from one market system to another (e.g. liberalisation, privatisation), and the speed of transition
  - Control structure (e.g. unbundling, ownership patterns, legally binding operational rules, voluntary agreements)
  - Investment incentives and financial risks (maintenance and new facilities)
  - Business principles (e.g. redundancy versus cost of service trade-off, profit maximisation)
  - Price and price regulation as paradigms: how price of service is based on cost
  - Behavioural issues (e.g. of corporate and political leaders, service end-users, and others)
- Government policy-making (e.g. Kyoto protocol, policies (e.g. renewables, nuclear))
- Legislation / regulation (responsibilities, institutional complexity, differences within integrated networks, e.g. between EU and non-EU Member States)
- Technology-related
  - Potential for storage; inherent inertia
  - Localised versus pan-state and multi-state vulnerabilities
  - Customised versus off-the-shelf systems
  - Susceptibility to failures / accidents
  - Speed of developments / innovations
- Infrastructure-related
  - Degree of 'criticality', potential for choice
  - Technical design and operating principles (e.g. N-1 criterion, maintenance)
  - Space extension and exposure
- Degree of interconnectedness, complexity
  - Interdependences within single infrastructures
  - Interdependences across infrastructures and regions
- Availability of resources
  - Shortage, depletion of scarce resources
  - Contamination or degradation of supply
- Natural conditions (weather) and hazards
- Context of risk and threats, openness of society
  - Attractiveness for, and vulnerability to, malicious attacks (cyber, terrorism)
  - Public acceptance and risk awareness
  - Strategic issues
- Urbanisation, demographics
- Historical development of socio-economic structures (e.g. railway system).

Each of these systems involves a combination of private and publicly-owned entities enmeshed in a broader socio-political-economic network. Their form and operation is governed by legislation and regulation. The infrastructures are coupled or interconnected to different degrees and finally must be regarded as a 'system of systems'. Their operating strategies and end-user behaviours are subject to significant contextual changes and an increasing number of risk-shaping factors (Box 2).

An infrastructure becomes critical when it provides some service without which society or the economy cannot engage in normal operations. Of course, in this sense different systems can be critical to different degrees and from different perspectives. Service interruption or degradation can range from mild inconvenience to large economic losses and/or serious threats to human health and safety. Focussing on society as a whole at a higher level, the criticality of the system can be described [EC 2004] in terms of scope (extent of geographic area affected), magnitude (degree of impact or loss) and effects of time[5].

Table 1: Illustration of the diversity of factors which can result in varying degrees of criticality for an event using disruption to, or degradation of, services provided by electrical power and urban water supply systems as examples

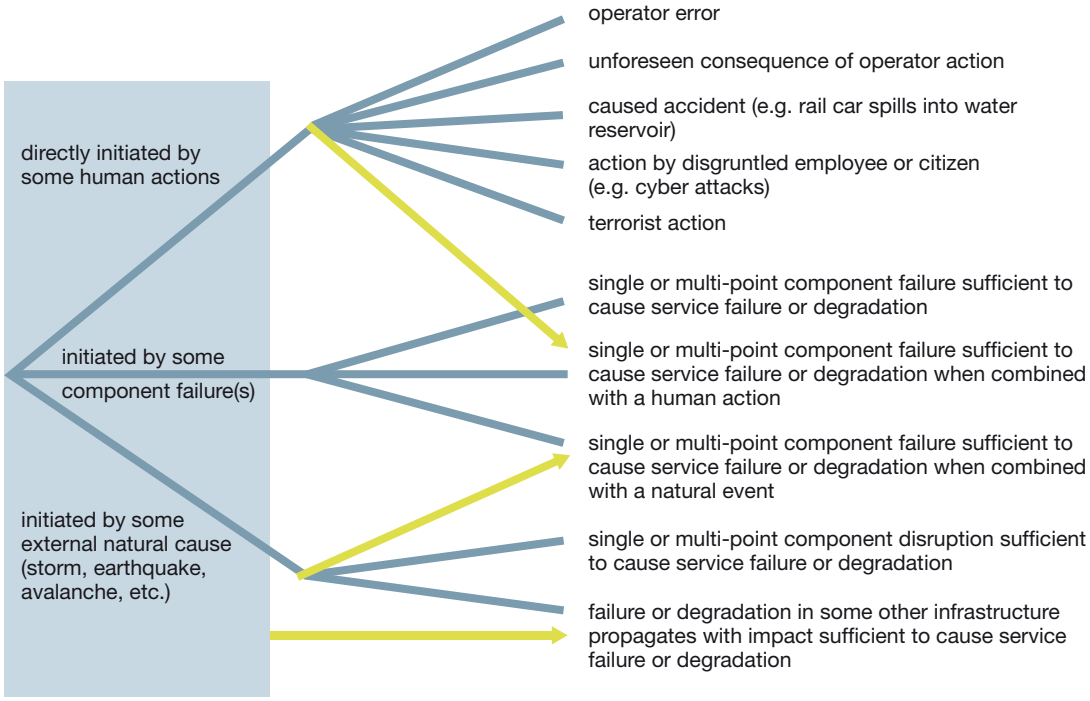
Nature of infrastructure failure or service degradation	Spatial extent (radius)	Health and safety consequences	Economic consequences	Impacts to other infrastructures and/or socio-political systems	Resulting level of criticality
Local electrical power outage of ~ 3 hours duration (e.g. from a local thunder storm)	a few km	Little to none unless local emergency services have no back-up and there are other contributing factors such as extreme heat	Modest unless firms which have a high need for secure power have no back-up	Some disruption of ICT and other services which have no back-up. Few consequences to public or power company officials unless this is part of a recurring event, or happens at a critical time	Modest unless outage occurs in parallel with some other event (e.g. a terrorist bombing and traffic lights go out preventing emergency vehicle access)
Multi-national electric power outage of more than one week duration (e.g. from ice or wind storms or terror attacks on multiple substations)	100s of km	Potentially large as back-up fails, water and sewer systems that require pumps fail, food supplies run short and/or there are other contributing factors such as extreme heat or cold	Large, indeed catastrophic for some firms	Enormous	Extremely high
Urban water supply disruptions of about 3 hours duration (e.g. from a pump failure)	a few km	Very limited unless there are other contributing factors such as extreme heat	Very limited unless there are other contributing factors such as extreme heat	Very limited	Very low
Urban water supply contamination with a serious pathogen for more than one week duration before detection via sick people	a few km	Extensive illness and significant mortality	Large, due to loss of work, and other costs of widespread illness	Little or no impact on other infrastructures (unless infection spreads to other locations and affiliated staff does not show up for work). Significant consequences for responsible public and private officials and loss of public confidence	Extremely high

5 This criteria ascertains at what point the loss could have a serious impact (i.e. immediate, 1-2 days, one week, other).

Using examples drawn from just the electric power system, and urban water supply, Table 1 illustrates some of the factors that determine how critical an infrastructure disruption or service degradation may be. Note that, while the geographical scope, duration and magnitude of an event all matter, even events with very limited geographic extent can be of high criticality.

Such malfunctions can arise from a variety of events including extreme weather conditions, accidental or mistaken human action, or pernicious human disruption by disgruntled citizens or terrorists. Figure 1 provides a simplified taxonomy of such initiating events. In reality, event sequences can be extremely complex. For example, a component failure may result from inadequate inspection or maintenance and this may interact with other external factors and operator error. The taxonomy does not include extenuating social and organisational factors such as the presence or absence of a safety culture, which can dramatically change the probability that some of these events will occur.

Figure 1: Simplified illustration of some of the different types of events that can result in the failure, or degradation, of the service provided by a critical infrastructure. Initiating event (left) can take on a number of different forms (right). A few interactions between events are illustrated by lighter shaded arrows.



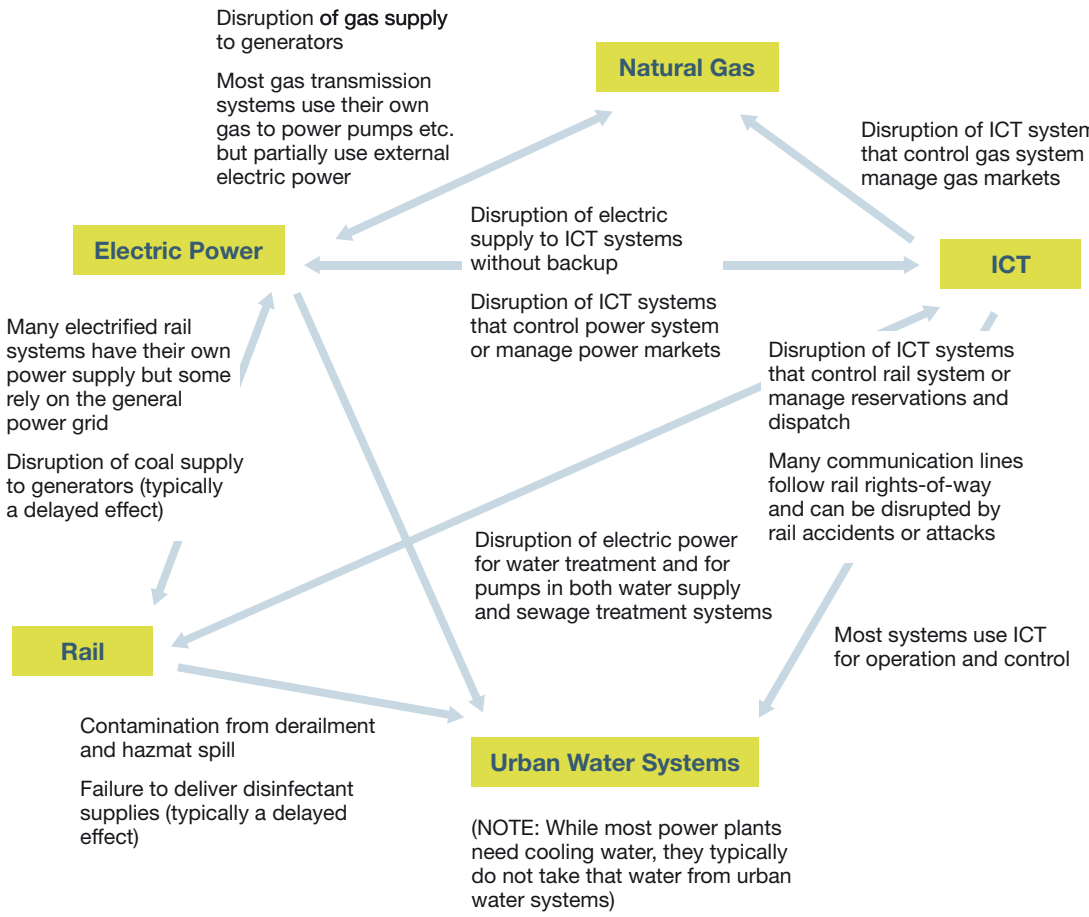
Many infrastructures are interdependent or depend on a host technology, such as electric power or ICT. For example, unless special precautions have been taken, the operation of pumps in drinking water systems, or of the traffic lights that direct the smooth flow of traffic on urban streets, depend on the availability of electricity from the power grid. Similarly, unless special care has been taken to provide independent communications channels, the control of many market functions, such as bids for the sale of blocks of electric power from one nation to another, may depend on the availability of the public Internet (see Figure 2, also [Rinaldi 2001] for further details).

While some coupling between infrastructures has always existed, today, because so many critical social services now depend on one or more of these systems, a disruption or malfunction often has much greater direct impacts than was typically the case in the past, and can also propagate to other systems, resulting in further additional disruptions.

In many cases, vulnerabilities that could lead to service disruption or quality degradation are introduced via perfectly innocent procurement choices to use off-the-shelf commercial systems. However, commercial systems often do not include provision for independent or back-up electric power (as is the case with, for example, many modern telephone sets). Furthermore, information and communication systems do not incorporate a level of security appropriate for infrastructure applications given the risks posed by accidental disruption or malicious attacks, and may have less specific functionality than the older, customised systems they replace. Sometimes, desirable functionality is not available in off-the-shelf commercial systems because of limited diversity of supply. The failure of both cell- and land-line telephone systems in New Orleans after Hurricane Katrina is one recent example in which a lack of back-up capability led to a serious loss of telecommunication service with devastating health and social consequences, after initiation from a foreseeable storm event.

As systems become more complex, they can often only be successfully operated with the expanded use of ICT. It is inconceivable that a modern transportation system could be operated without computer reservation systems or traffic flow control systems. The same is true for many other important economic and social systems. But this very complexity, and the ICT that is used to manage and control it, can increase vulnerability.

Figure 2: Simple illustration of a few of the interactions that can occur among just the five critical infrastructures considered in this report



One of the features that can make a system more robust is the presence of slack, spare capacity which can absorb unanticipated stresses or unexpected demands. However, relentless pressure for greater economic efficiency and lower prices of service often has the effect of squeezing out slack or redundancy in systems, resulting in tighter operational margins. Vulnerability can also arise when separate smaller systems are integrated into a larger system, thus creating greater complexity and the increased potential for trans-boundary propagation of disturbances, both of which have occurred in the case of the electric power grid.

Another process that is especially apparent in the case of the electric power system (although similar issues have also arisen in other settings such as rail systems) are vulnerabilities that arise when a system that was designed, built and operated under public ownership in a non-competitive environment is suddenly expected to operate in a quite different way in a competitive, albeit regulated, market.

In power systems it may still be possible to send a crew out with a truck to manually open and close circuit breakers if advanced control systems fail. Similarly, crews may be able to manually open and close railway switches. However, in advanced communication systems and computer networks, such manual operation is often not feasible and may not be helpful in highly complex systems.

Finally, there are a number of social and institutional factors that can contribute to the growth of vulnerabilities. For example, if there is no careful accounting of performance, or penalties or costs to owners and operators when system disruptions cause broader social consequences, there is unlikely to be a strong incentive to manage those risks. More generally, factors such as the absence of awareness of vulnerabilities, of limitations to achievable reliability, or of concern for low-probability but high-consequence failure modes, can contribute to levels of complacency that can make a society and its critical infrastructures more vulnerable.

This report aims to provide an overview of critical infrastructure risk issues for senior public and private sector decision makers so as to increase their awareness of relevant issues and to motivate further investigation, analysis, and multi-party dialogue in support of actions appropriate to reducing the risks associated with critical infrastructure systems. In addition, senior experts may benefit from broadening their perspective from purely technical to socio-economic factors (or vice versa) and from single systems or even elements of systems to a 'system of systems' point of view.

The sections that follow will:

- Provide a more precise understanding of what critical infrastructures are and how they depend upon each other
- Address factors that make the infrastructures more interdependent, weak and vulnerable
- Begin to assess the degree of criticality of the five infrastructures selected for this study and the adequacy of related institutional responses / governance approaches
- Propose technical, management and organisational strategies and outline policy options that might be adopted after the socio-political and regulatory framework has been set and that could be used to reduce social vulnerabilities; and finally
- Discuss the limitations of this first study and outline the need for further studies.

3 BRIEF CHARACTERISATION OF FIVE CRITICAL INFRASTRUCTURES

The five infrastructures selected for this study (electric power, natural gas, rail, urban water systems, and a variety of ICT systems) are all, in principle, critical to the successful functioning of Western industrialised societies. To at least some extent, they are mutually dependent, or commonly dependent on underlying technical and social systems. In many infrastructures, rules and procedures are used as a means to assure a sufficient degree of security, e.g. the N-1 criterion which is specified for many electric power grids (see Box 3).

3.1 Electric Power Supply

Most of modern society runs on electricity. Today, most electricity is generated in large central plants. According to the International Energy Agency [IEA 2004], 51.7% of the electricity in the US and 30.4% in the EU is generated by burning coal (in most cases delivered to the plant by rail). There are, however, exceptions. For example, roughly 80% of the electricity generated in France comes from nuclear reactors, and well over 90% of the electricity generated in Norway comes from hydro-electric plants.

Once electricity is generated the voltage is increased so that it can be efficiently transmitted over long distances via high voltage transmission lines. With a few exceptions, these lines operate as an interconnected ('meshed') grid, often with multiple routes available for power to reach the same destination. In conventional Alternating Current (AC) transmission grids, how the power flows is controlled by the electrical properties of the network; system operators have relatively little ability to change the flow patterns. Throughout the high voltage grid there are a variety of circuit breakers and other protective and control devices. Once electricity nears the end-users, transformers are used to lower the voltage as it enters the distribution system. While distribution systems in cities may also operate as an interconnected grid, most operate as tree ('radial') structures which feed power out to the final customers.

A variety of measuring devices, both at generation plants and spread across the transmission grid, are connected to control centres where they allow operators to monitor the state of the system. By sending electronic commands back out, operators can control the settings of generator plants, reconfigure the grid, and, at least in limited ways, affect its electrical properties.

The electric power system is a complex, large-scale, extensive and vulnerable infrastructure. It qualifies as critical because power supply is very important for many social and economic activities and services as well as for the functioning of other vital infrastructures. Modern societies cannot afford disruptions, at least not over a wide area and long time period. The degree of criticality is high as the impact of a failure, loss or unavailability is high in scope (potentially international), magnitude (major) and effects of time (immediate).

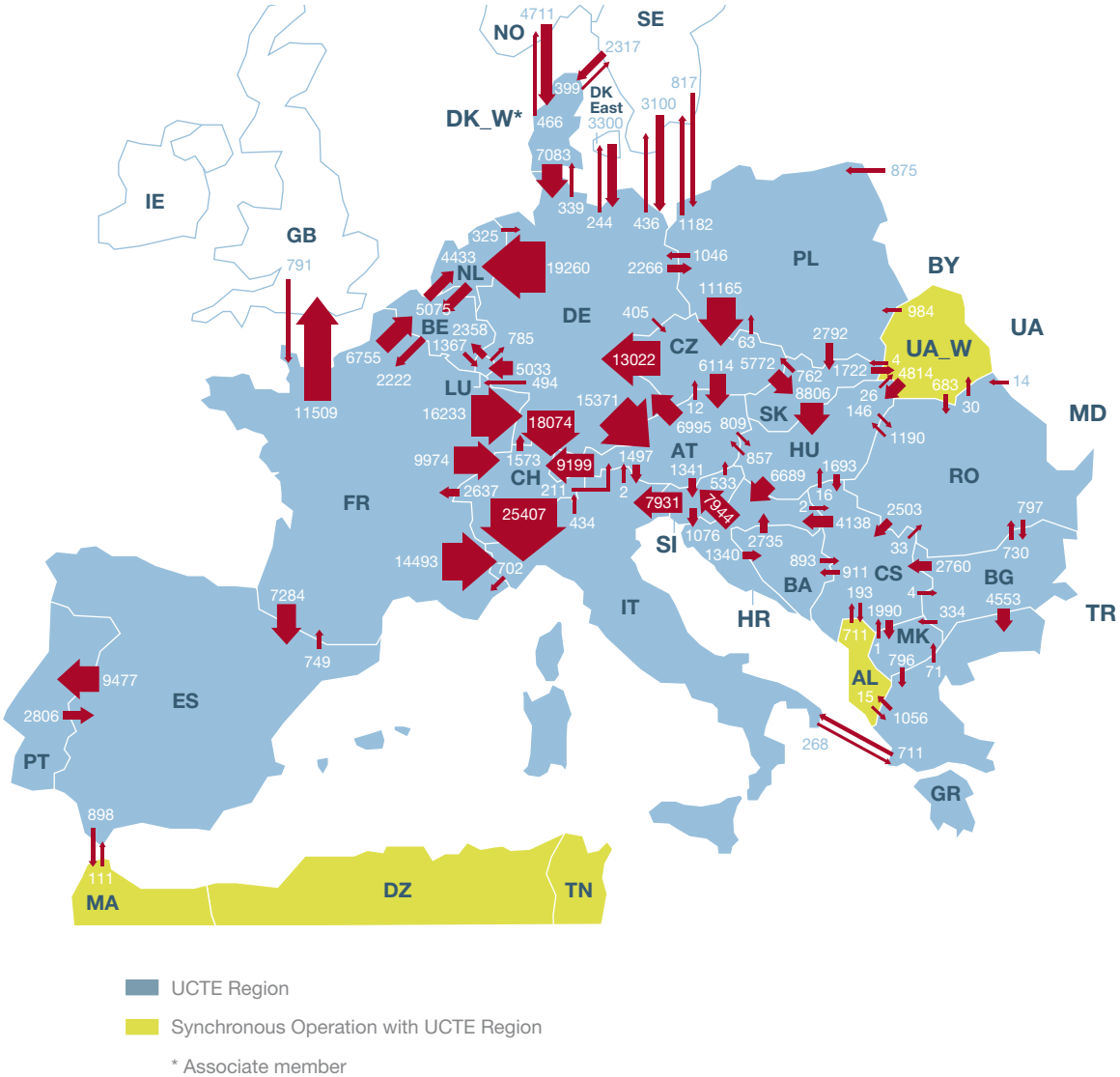
The overall vulnerability of the electric power critical infrastructure appears to be high and growing due to factors to follow, underlined by lessons learned from recent major blackouts:

- Aug. 14, 2003 – Eastern US and Canada
- Aug. 28, 2003 – London
- Sept. 23, 2003 – Denmark / Sweden
- Sept. 28, 2003 – Italy
- Nov. 7, 2003 – Chile
- July 12, 2004 – Athens
- May 25, 2005 – Moscow
- June 22, 2005 – Switzerland (railway supply system)

The evaluation of blackouts identifies a common pattern and clearly confirms that the risks involved are systemic in nature:

- Each system has been developed in the past 50 years with a view to assuring mutual assistance amongst system operators in case of contingencies. The way in which these systems are now operated is often beyond the original design parameters, mainly due to market liberalisation
- A minor single event (e.g. a line overload or a tree flashover due to inadequate tree-cutting) may snowball into massive problems for a highly burdened[6] electrical power system with long transmission distances
- The malfunction of critical equipment (possibly as a result of inadequate diagnostic support), and the behaviour of protective devices complicated the management of these events; the available system automation turned out to be insufficient to cope with these kinds of event sequences
- Nevertheless, in addition to purely technical factors, there were human-related, economic and contextual aggravating factors including a general lack both of situational awareness of potentially far-reaching failures and of short-term emergency preparedness
- The impacts on other infrastructures and our societies are significant although, in the incidents listed above, the affected population reacted calmly.

Figure 3: Trans-boundary physical energy flows (GWh) in Europe in 2005 [UCTE 2006]



6 E.g. due to economic pressure put on the system's operator to operate the system at or even beyond its well-known limits.

Both in the US and in Europe, the continental-scale high-voltage transmission grids have developed through the continued addition of higher voltage systems on top of existing systems, and through the interconnection of regional and national systems in order to provide wider access to reliable sources of power.

For example, the European electric power system has been evolving rapidly in the last decade. A Directive [EC 1996], adopted in 1996, sets common rules for the European internal competitive market (although we acknowledge that the detail of such rules can vary between Member States as a result of the particular enabling legislation, which is passed by each national parliament). Management and coordination of the Union for the Coordination of Transmission of Electricity's (UCTE) framework[7] has historically been based on a series of gentlemen's agreements and, for a short time, supported by binding, enforceable rules and standards, including the unrevised N-1 security criterion. Power flow and wide-area exchanges follow impedance law; at interconnectors (cross-frontier lines) between the Netherlands and Germany, between France and Spain, and between France and Italy, control devices (Phase-Shifting Transformers (PST)) are installed. These trans-boundary connections are also among the lines' considered weak points [EC 2005a] (see also Figure 3).

The uneven implementation of the principles and evolution of the internal market, as well as obstacles and shortcomings identified in annual benchmarking reports, provided the impetus to amend the 1996 Directive. A more recent EU Directive [EC 2003c] enacts common rules aiming at full opening of the electricity market for all non-household customers by July 2004, and for all customers by July 2007. In addition, a Regulation on conditions for access to the network for cross-border trade has been introduced [EC 2003d]. The EU's Member States are asked to "designate one or more competent bodies with the function of regulatory authorities to ensure that congestion management mechanisms evolve in a manner compatible with the objectives of the internal market" [EC 2003d, Article 8(4)]; they "shall be wholly independent from the interests of the electricity industry" [EC 2003c, Article 23(1)]. Member States should be responsible for guidelines on compensation for cross-border flows, on harmonisation of national tariff systems and on management and allocation of transfer capacity responsible for establishing transmission and distribution tariffs which allow the necessary investments in the viable networks to be carried out [EC 2003c, Article 23(2)].

In these documents security is addressed and should be ensured by monitoring [EC 2003c, Article 4]. However, it appears to be more a subsidiary than a primary goal. The "responsibility for ensuring a secure, reliable and efficient electricity system" [EC 2003c, Article 9] is largely transferred to the independent Transmission System Operator (TSO). Provisions are (1) "coordination and exchange mechanisms to ensure that congestion management mechanisms evolve in a manner compatible with the objectives of the internal market" [EC 2003d, Article 8(4)], (2) the use of (approved) "safety, operational and planning standards" and (3) "estimates of available transfer capacity for each day", "week-ahead and month-ahead estimates" as well as a "quantitative indication of the expected reliability of the available capacity" [EC 2003d, Article 5], all to be described in publicly available documents.

The introduction of market liberalisation has substantially complicated the situation since the grids are now being asked to move power in ways they were not originally designed to do. The timing and pace of the liberalisation process varied considerably across countries / regions and has

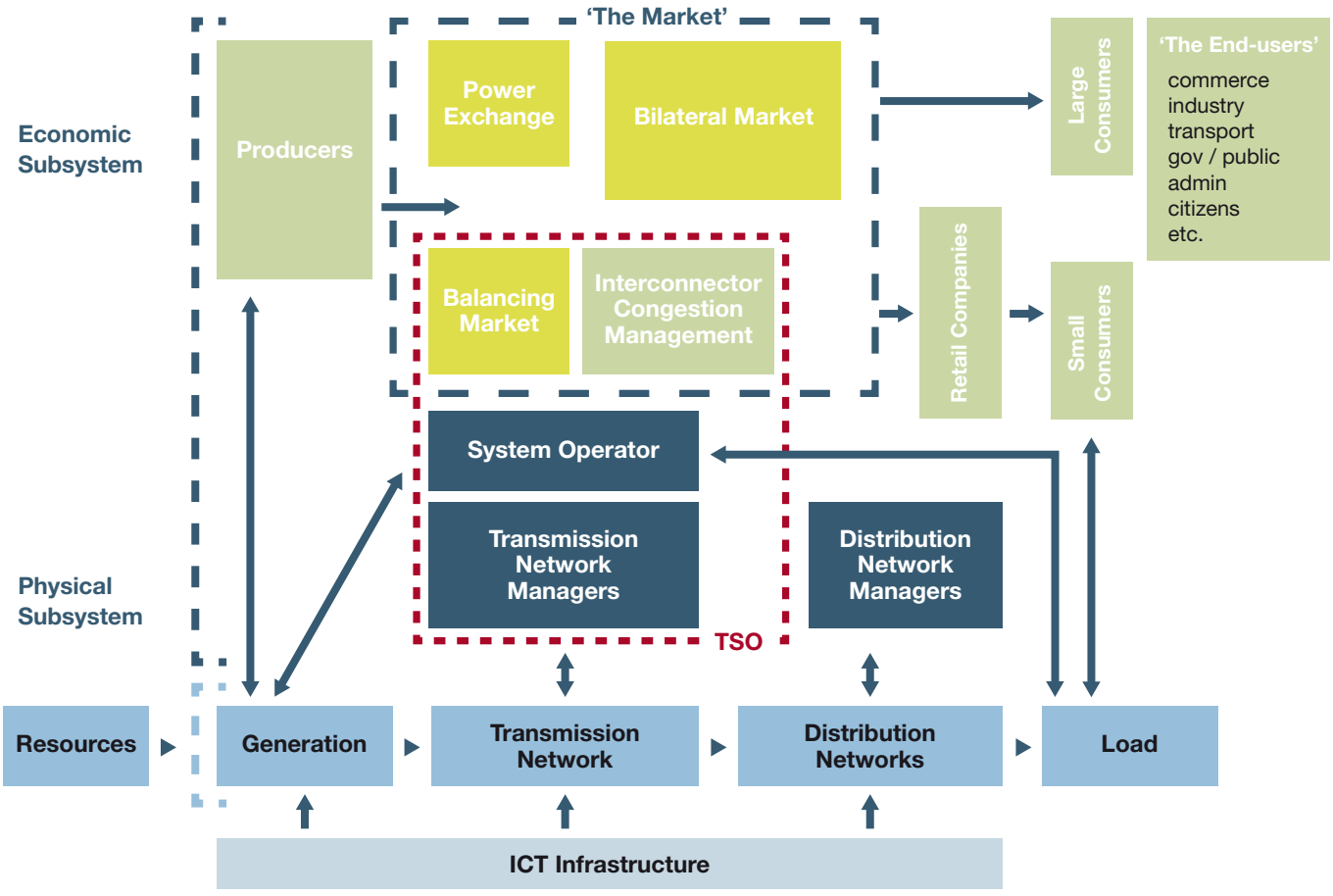
> "Market reforms have often been poorly designed, both in terms of respecting the basic laws of physics … and with rules differing from country to country … between areas or states within a country" [Yeager 2004].

7 The Union for the Coordination of Transmission of Electricity (UCTE), is an international non-governmental association of the Continental European Transmission System Operators (TSOs).

increased complexity by, for example, adding a variety of additional institutional players and different control structures (see Figure 4). Prevailing business principles and behaviours have caused effects that some argue are positive from a consumers' point of view (more potential suppliers, prices follow market rules). However, as Apt et al. [Apt 2004] have shown, at least in the US, prices for industrial customers have not fallen in states that have unbundled their systems relative to those in states that have not.

Rapid restructuring has also complicated reliability. There has been a considerable reduction in investment in new transmission infrastructure in both Europe and the US[8]. Siting new facilities has grown increasingly difficult and in many restructured regions the cost of capital for new facilities has become much higher, since rates of return are no longer guaranteed. Research investments have shrunk, and in some cases preventive maintenance (including such activities as tree trimming) has been inadequate.

Figure 4: Organisational structure of the liberalised European electricity system, based on [Knops 2004]



The net effect of market liberalisation has been that many systems are now being operated much closer to their limits so that, if and when a problem arises, cascading outages may be more likely. This trend

8 Investments in the US decreased in the mid 1990s but increased dramatically over the past few years, peaking at close to $ 57 bn in 2001. Investments in the EU electricity industry are currently running at about $ 30 bn per year, on average lower in the 1990s than in the 80s. Italy decided in 1986 to give up nuclear energy and to import electricity (2004: 12% on average peaking at 25%) without adding adequate transmission capacities.

has provoked a debate about the adequate level of safety margins and redundancies and, particularly, about the value of security of continuous electricity supply.

Nowadays control rooms operate as the central hubs in the operation of power systems, as well as in implementing regional markets and their coordination at a trans-regional level. TSOs are of paramount importance as they are responsible for and challenged by:

- System balancing, interaction among agents (generators, spot and long-term market participants, distribution companies and their customers)
- Transmission network and congestion management
- Appropriate coordination and information exchange mechanisms
- Assuring network stability in the face of prevailing market behaviours.

Policy often aims to create large competitive markets and "establishes measures aimed at ensuring its proper functioning by safeguarding security of electricity supply and by ensuring an adequate level of interconnection" [EC 2003b]. As a key security standard, the N-1 criterion has been widely employed – in the past mostly voluntarily but it is now mandatory in some systems[9]. It ensures stable operation of the grid in the event of a normal contingency (see Box 3). Although it is a powerful deterministic tool, experts question whether it is adequately implemented and monitored in today's systems and whether the N-1 criterion is still fit-for-purpose. Some, e.g. [Bialek 2004], [Kirschen 2005], claim that it should be revisited, with full account taken of the potential trade-off between increased security and low-price transfer / transportation capacity.

Growing demand, complexity and economic transactions call for enhanced control and efficiency based on the "right information in the right place at the right time" [Cleveland 2005]. The need for greater levels and immediacy of information is exacerbated by growing numbers of short-term market transactions and a lack of transmission capacity. These developments have themselves been encouraged, in part, by the existence of modern ICT-based System Control and Data Acquisition (SCADA) and Energy Management Systems (EMS). Day-ahead congestion management and security checks have been or will be complemented by closer-to-real-time adaptive approaches based on an almost continuous acquisition of data[10].

While, in the past, information and communication networks and systems were designed and built for different purposes[11] with more limited interconnections and data exchange, today they are more tightly coupled. Although still considered as separate networks, they are partly connected with external Internet and dial-up connections[12]. They may merge into one integrated administration / business and control network with access through the Internet and connections to customers and service providers' networks [Ericsson 2004].

9 The operational standards of the UCTE became binding for its members (TSOs) on 1 July 2005 [UCTE 2006]. In the US the Energy Policy Act of 2005, which entered into force on August 8, 2005, makes compliance with NERC (North American Electric Reliability Council) standards mandatory [NERC 2006].

10 In many countries, compliance with the N-1 criterion is checked every few minutes.

11 Primarily plant operation and protection, secondarily power systems operation and control, market and business operation and administration purposes.

12 Hazardous facilities such as Nuclear Power Plants (NPP) still follow strictly the 'island approach'.

Box 3: N-1 security criterion – specified for the electric power grid

The N-1 security criterion specifies that "any probable single event leading to a loss of a power system element should not endanger the security of the interconnected operation, that is, trigger a cascade of trippings or the loss of a significant amount of consumption. The remaining network elements, which are still in operation, should be able to accommodate the additional load or change of generation, voltage deviation or transient stability regime caused by the initial failure. It is acceptable that in some cases, TSOs allow a loss of consumption in their own area on condition that this amount is compatible with a secure operation, predictable and locally limited" [UCTE 2004a].

TSOs monitor "the N-1 criterion for their own system through observation of the interconnected system (their own system and some defined parts of adjacent systems) and carry out security computations for risk analysis". After a contingency occurs, each TSO works to rapidly restore his power system to an N-1 compliant condition and, in case of any delay, immediately informs other TSOs affected [UCTE 2004a].

This is a deterministic approach which does not address the occurrence of more than one failure or of more complex failure combinations. In addition to some methodological deficits, inappropriate application of the N-1 has clearly contributed to major blackouts [UCTE 2004b].

While providing new opportunities, the more intensive use of (commercial) ICT would appear to increase the exposure of the power system to equipment (common-cause) failures, human errors and malicious attacks [EC 2005] and to imply emerging security challenges[13].

As we have learned from blackouts, single initial failures may cause instabilities and not only affect large areas of the electricity supply system but also snowball into other infrastructures. Electricity is essential for the support, operation and control of other critical infrastructures. Unless there are adequate back-up systems, a failure may cause immediate (e.g. rail transport, traffic control) or delayed (e.g. water, cell towers with only battery back-up) loss of service.

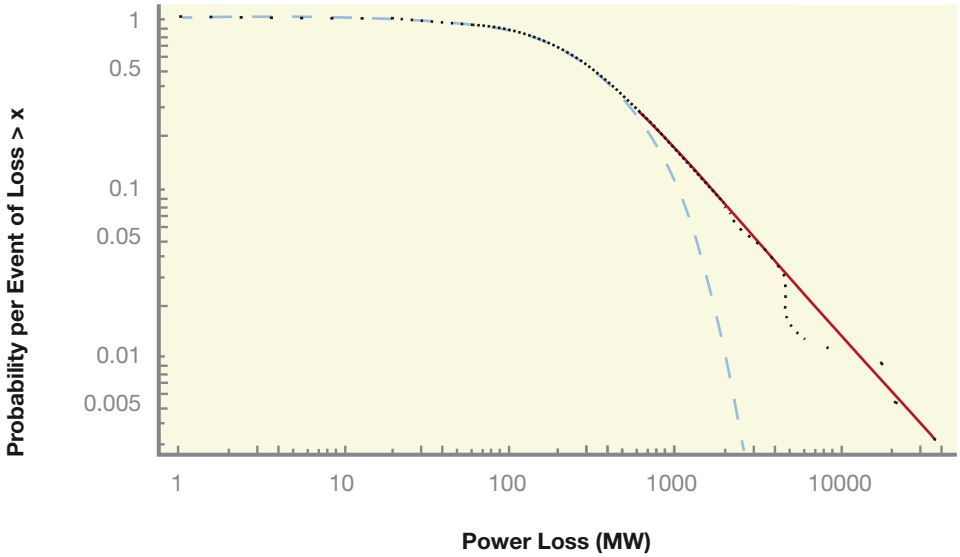
Although large-scale blackouts are very low probability events, they carry immense costs and inconveniencies for consumers and society as well as for power companies. For example, costs totalled between US$ 2–10 billion in the recent (2003) North-eastern US and Canada blackout, affected 60 million people in the Italian blackout (2003) and involved recovery times varying from 2–4 hours in the Swedish / Danish blackout (also 2003), 5–9 hours in some Italian cities and more than a day in New York City and Detroit (and weeks and months in parts of Ontario, Canada) [Gheorghe 2006].

Analysis of power interruption data indicates a marked increase in the frequency of major blackouts in the US since 1994 "caused by pushing systems closer to their limits" [Madani 2005]. In both the US and Europe[14] the likelihood of large-area failures seems to be greater than one would expect on the basis of extrapolation from small failures (Figure 5), which is symptomatic for self-organised systems and analogous to sand pile models [Carreras 2001].

13 The reason why major system operators still strictly abstain from using the Internet for management and control purposes.

14 Integrated data available since 2002.

Figure 5: Cumulative probability of North American blackouts as a function of power loss. The exponential distribution (dashed line) fitted for small events significantly underestimates the probability of large events (solid line), compiled by J. Apt from US NERC data, 1984-2000.



As a result of its structure, architecture and spatial extent, the electric power system (and large parts of its elements) is subject to many kinds of well-known threats including technical and human failure, extreme weather conditions and other natural events. Some generating plants (e.g. nuclear, hydro) and elements of the grid (e.g. transformers, substations) as well as control rooms are the most vulnerable targets for physical terrorist attacks and cyber intrusion into operation and control systems[15].

The importance of reliability and security of electricity supply within our society and the question of what constitutes adequate target levels need to be addressed from a broad perspective that includes a consideration of:

- Short and long-term social vulnerabilities, including end-users' willingness to pay
- Making optimum use of what has effectively become management by public-private partnerships
- Political issues such as reliability goals or targets, the set of threats to be taken into account, and trans-boundary data exchange, as well as mechanisms to deal with trade-offs, cost assignment, responsibilities, and financial risk transfer instruments, e.g. insurance
- Regulation and standards such as investment planning, mandatory operational rules, availability of adequate data on power flows and transmission system components
- Technical fixes such as adding generation and transmission paths, reactive power support, proper maintenance, and alignment of protection schemes and settings, as well as closer-to-real-time system monitoring and control, improved situational awareness, and scenario-based operator training in contingency recognition and response
- Special issues including improved modelling capabilities and understanding of complex systems, professional accident investigations, refraining from using the Internet (without adequate security), reasonable sizing of the interconnected synchronous grid (coherent expansion planning), and proper integration of dispersed intermittent generators (wind, solar).

15 While there have been no publicly reported successful attacks on power system SCADA systems, there have been more than forty real-world cases in which other kinds of industrial control systems have been impacted by electronic means [Ericsson 2004], such as a Slammer worm infection of a private computer network at Davis-Besse nuclear power plant.

Analysis by a multidisciplinary group convened by IRGC has identified multifaceted weaknesses and threats [Gheorghe 2006]. The team concluded that political aims in the EU are too strongly focussed on costs, and that systemic risks and new security issues have not received adequate attention. They believe there is a need to consider and balance conflicting social objectives for which new institutions and governance processes should be created, involving all relevant actors including consumers. The group concluded that, while the Florence Forum and Regional Fora gave the appearance of being appropriate institutions, their current structure, market-oriented mission and working style, which was not decision-oriented, limited their suitability. They drew the following conclusions:

- The European electric power system, which is embedded in a political framework given by the EU Directives for internal (liberalised) markets, is a new reality of interconnected physical and social networks that is being placed under stress by various factors and fragmented institutional setups. The design and operational criteria need to be better aligned with current use and practice
- The current trend to under-investment[16] has to be fully recognised by all parties and, then, be countered by appropriate (regulatory) provisions that reflect agreed long-term objectives
- There is an increasing need for safe operation and control in closer-to-real-time mode based on adequate data acquisition and binding rules including contingency procedures. Coordination between TSOs needs to be further improved
- Digitalised, non-dedicated control systems are becoming increasingly ubiquitous, partly making use of open access ICT, introducing potential vulnerabilities to malicious attacks; the use of inadequately secured Internet should be avoided for systems used in monitoring and control
- 'Island solutions' for hazardous facilities and activities should be further developed and maintained
- Interdependency issues may become even more important, with which our mindset / awareness and intellectual modelling capabilities cannot even currently keep pace; this requires intensified dialogue and new initiatives.

Many people may believe, incorrectly, that the electric power system is already very reliable and stable, or that it can be made totally reliable and stable. In reality there is a great need for more transparent objective- and agenda-setting and for a more balanced approach to, for example, the pricing for electricity, security of supply and the relationship between the two. This may come from viewing the system as a whole and seeing its place within a dramatically changed environment in which all relevant actors (governments/regulators, industries, customers) should participate in an integrated approach to governance. Trends such as growing demand, further geographical expansion of the network, and the integration within the system of decentralised intermittent power generation (wind and solar, for example) may also pose new risks to the stability of the grid and deserve a similarly inclusive approach to policy decision-making.

We conclude that the security of continuous electricity supply is of paramount importance for our society and that it should be considered as a new overarching principle to guide the formulation of policy. The most recent EU Green Paper on 'A European Strategy for Sustainable, Competitive and Secure Energy' [EC 2006] already goes in this direction by asking "the most fundamental question whether there is agreement on the need to develop a new common European strategy for energy, and whether sustainability, competitiveness and security should become the core principles to underpin the strategy."

16 It should be mentioned that public non-acceptance of new transmission lines and the behaviour of traders may also contribute to limited transmission capacities.

Despite all measures to make the electric power system more robust, major disruptions cannot be totally ruled out and will continue to happen. Therefore, strategies must include:

- Demand management and priority setting
- Equipment reliability and planned steps to reduce restoration times
- Technologies such as micro-grids and back-up systems to reduce dependence on the grid.

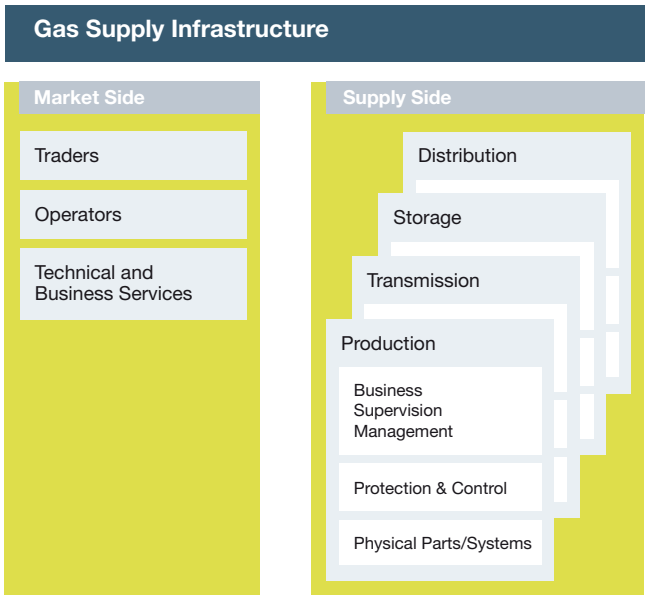
3.2 Gas Supply System

The supply side of the system for natural gas consists of the following elements:

- Upstream facilities such as wells and gathering pipelines
- Midstream facilities such as processing plants, e.g. for dehydration
- Land-based long-distance transport via systems of high pressure steel pipelines (with compressors, meters and valves); storage facilities such as tanks and underground reservoirs; treatment facilities
- Maritime transport of liquefied natural gas (LNG) and the necessary elements of the LNG supply chain (with liquefaction plants, ships, regasification plants, storage)
- Regional / local distribution (gate stations, meters, valves, odorising equipment, large and small diameter pipes mainly of steel or plastic).

The supply side together with the market side are represented in Figure 6 as a multi-layered model of the system.

Figure 6: Layered model of the gas supply infrastructure



Initially, the production and distribution of town gas was done at a local level. Today it has been replaced by natural gas and small distribution networks have been integrated into a large transcontinental network. Taking Europe as an example, natural gas is delivered from fields in Russia, the Caucasian region, the North Sea, Algeria and other countries and distributed all over the continent (see Figure 7). Gas constitutes 24% of Europe's primary energy consumption but increasing dependence on producing countries is raising concerns with regard to security of supply. The large pipelines in the Eastern Europe / Russia region are strongly East-West oriented with only few interconnections in the North-South direction.

Figure 7: Most important gas pipelines and LNG transportation routes in Europe [Erdgas 2006]

The use of gas varies from country to country. The Netherlands currently has the highest dependency in Europe at 46% of primary energy use. And, in many countries, demand continues to grow for various reasons; one reason is that gas plays an important role in fulfilling European obligations under the Kyoto protocol, as natural gas emits less carbon dioxide per kilogram burned than other fossil fuels.

Natural gas is used by residential and commercial customers for space and water heating and as cooking fuel, sometimes also as motor vehicle fuel, and by industrial customers for electricity production, for thermal uses and as feedstock for chemical production. Therefore, the gas supply system is a crucial infrastructure, and its interruption has a strong impact on the economy of a country and the well-being of society. Interruption can also have major impacts on other infrastructures, especially through the disruption of electricity supply. The degree of criticality may be quite high in scope and magnitude at a local or national level, but in most cases moderate to weak on a more global level. Widespread availability of storage leaves the system less vulnerable than electric power, but supply constraints such as those resulting on the US Gulf Coast after Hurricanes Katrina and Rita can have major impacts on availability and price.

Natural gas resources exist off-shore and on-shore, under pressures of up to 350 bar and in various qualities. The high pressure pipelines have diameters of up to 140 cm (trunk pipelines in Russia) and transport gas at pressures up to 80 bar. For transport over about 150 km, a gas-fuelled compressor station is usually required in order to maintain adequate pressure.

Gas can also be liquefied (-160°C) and then stored in insulated tanks or transported in special ships. This is, for instance, usually done to transport gas from Algeria to Europe.

For safety reasons, an odorant is added to the gas. Distribution is organised by dispatching centres (see e.g. Box 4). The gas transportation network is equipped with pressure and flow measures; values are monitored in a control room from where, in case of interruptions or any other operational needs, valves can be closed remotely. The valves are also used to limit the amount of natural gas that can escape if a pipe ruptures. While these valves require electricity to function, they also have battery back-up.

Most system status data and control signals are communicated via dedicated data lines installed along the pipelines; these data lines have built-in redundancy. However there is a slight trend to make use of the Internet. Examples have also been identified where the dispatcher can log in to the control computer from outside the dispatching centre via a dial-up line.

Box 4: Operation of Swiss gas supply – with relevance to other countries

The Swiss gas distribution network is basically honeycombed in shape, which makes it more robust against pipe ruptures, however there are minor exceptions. Most of Switzerland's gas comes from the transit pipeline that runs from the Netherlands to Italy. The pressure is high enough for local distribution without requiring additional compressor stations. Regional distribution is provided by five companies. Local distribution in towns is provided by a large number of small companies, most of which are owned publicly, often by municipalities.

Experienced operators run the gas supply system under defined conditions; changes in demand can be balanced using stored gas. Because the Swiss market has not been liberalised, it is possible to exchange gas between suppliers in cases of shortage.

Dispatching relies on a dedicated telecommunication network based on fibre optics, but independent radio communication equipment is available and cellular phones are also used. Gas pressure and flow are continuously measured. Such data are used for operational and emergency management purposes.

Both the one compressor station that is part of the transit pipeline, and smaller compressors used for storage facilities, are gas-fuelled. They can be operated in the event of a loss of electricity supply, but a large number of customers will not be able to use gas in such a situation (no electricity for furnace fans and pumps, factories not operating, etc.).

The gas supply system has experienced accidents, such as the following two examples:

- In January 2004, an explosion in a natural gas liquefaction plant in Skikda in Algeria killed 27 people and caused considerable damage to installations and buildings. The explosion was caused by a technical failure in a heat-exchanger [Saunalahti 2005]
- In 1982, an explosion occurred in the former Soviet Union, caused by a cyber attack. It was the largest non-nuclear explosion ever observed [NATO 2006].

Policy aims are similar to those of the electricity sector and focus on creating a large liberalised market. In the European Union, the 'gas Directive' [EC 2003a] of 26 June 2003 establishes common rules for the internal market in natural gas, repealing [EC 1998], and is combined with "notes for the implementation" and calls for national regulations.

Although the policy aims are similar, the liberalisation of the gas market is different from that for the electricity market in several ways:

- Gas can be stored and more readily substituted with other fuels; for example some gas turbines can also run on distillate
- Important gas producing countries for Europe are not EU Member States and are therefore not bound to apply EU Directives
- Access for third parties to high pressure gas pipelines has been possible for decades.

Although the political objective is that of a complete opening of the market, whereby industrial and private consumers can select their gas supplier, even gas industry representatives are ambiguous about how this should be implemented. Liberalisation of the gas market also raises new problems, as recent examples have shown:

- Long-term contracts are achieved by companies as a result of their high investment, but such contracts may be in conflict with anti-trust laws (for example, in Germany, the Federal Cartel Office has forbidden such long term contracts, but utilities have appealed to courts). In contrast, other contracts may make it possible to decouple gas prices from oil prices, which is understood to be an unwanted dependency
- Prices for customers may rise due to increased effort and cost in measuring gas flow.

Industry concentration is ongoing and promotes even tighter integration of the systems. Long-distance transport is dominated by a few large companies, either state-owned or private, while organisations involved in the final distribution to the end-user include both large and/or numerous small companies.

As a result of its large spatial extent and because many critical elements of the system are above ground, the gas transmission system is exposed to numerous hazards and vulnerable to potential attacks. Nevertheless, due to the design and physical properties of the system it is robust and safe. This is due in part to:

- Limited degrees of complexity and of highly dynamic behaviour
- Continuous overpressure of the gas network in order to avoid flashbacks and visual inspections of large gas pipelines in order to identify potential leaks and threats
- Inspection of the condition of the pipelines from inside, using a device travelling through the pipe
- Regular inspections of gas installations in residential houses and at industrial sites.

The following threats and system vulnerabilities have been identified:

- Countries which are net consumers of gas depend strongly on the gas producing countries. Gas shortages due to technological, geological or mainly political reasons may result in reduced delivery and affect social needs as storage is limited and costly, and limited interconnectedness of the network makes it very difficult to transfer supplies in unforeseen directions
- Gas pipelines are subject to interruptions by, for example, construction work. This is more likely to create impacts at a local distribution level but could also affect a trunk gas pipeline. However, gas companies are used to dealing with such interruptions by fast repair work. An example of a severe accident and the serious harm caused by such an interruption is given in Box 5
- Above-ground spherical tanks and gas pipelines can, in principal, be attacked easily; such attacks could cause widespread harm

- Natural events such as hurricanes, landslides or earthquakes may destroy large parts of the system[17]
- Both ships transporting LNG, which often pass through straits, and LNG terminals are regarded as attractive terrorist targets mainly due to their high explosive power.

Box 5: Gas pipeline explosion at Ghislenghien, Belgium

On July 30, 2004 a gas leak was observed on a high-pressure natural gas pipeline passing under a car park at Ghislenghien, Belgium. The leak was caused by the combination of a stop of the gas flow, which resulted in dynamic stresses, and a weakening of the pipeline due to construction work. A subsequent explosion caused 24 fatalities and more than 120 injuries, mostly among fire fighters and police. The crater at the explosion site was 10 metres in diameter. The high number of victims was also a result of a series of misunderstandings and an under-appreciation of the hazards [Saunalahti 2005].

The situation can be further improved by technical fixes and addressing political issues. Such improvements could include:

- Implementation of an easy-to-use information system on the location of gas pipelines for use by civil engineering workers and emergency response crews
- Reversing the trend toward using inherently insecure systems such as the Internet and dial-up modems
- Reshaping the conditions of market liberalisation with regard to supply security and lean processes, and assuring attractive conditions for long-term investment.

3.3 Urban Water

A water supply and wastewater system has to secure the supply of drinking and process water in sufficient quantity and quality (in terms of hygiene and chemical and physical properties) and provide water with sufficient pressure to consumers. Additionally, it has to assure the collection and treatment of wastewater and its safe discharge into the natural environment. A typical system comprises five interlocking components (see Figure 8):

1. Water collection (extraction from wells, rivers, ground-, lake- and seawater) and treatment (for example, disinfection, filtration or desalination)
2. Storage (to balance differences between water input and output)
3. Distribution: pumping stations and the network of pressure pipelines needed to provide water to consumers
4. Wastewater (sanitary sewage and rain water) collection and treatment
5. Operation (water treatment, distribution) and control (of, for example, water quality and pressure).

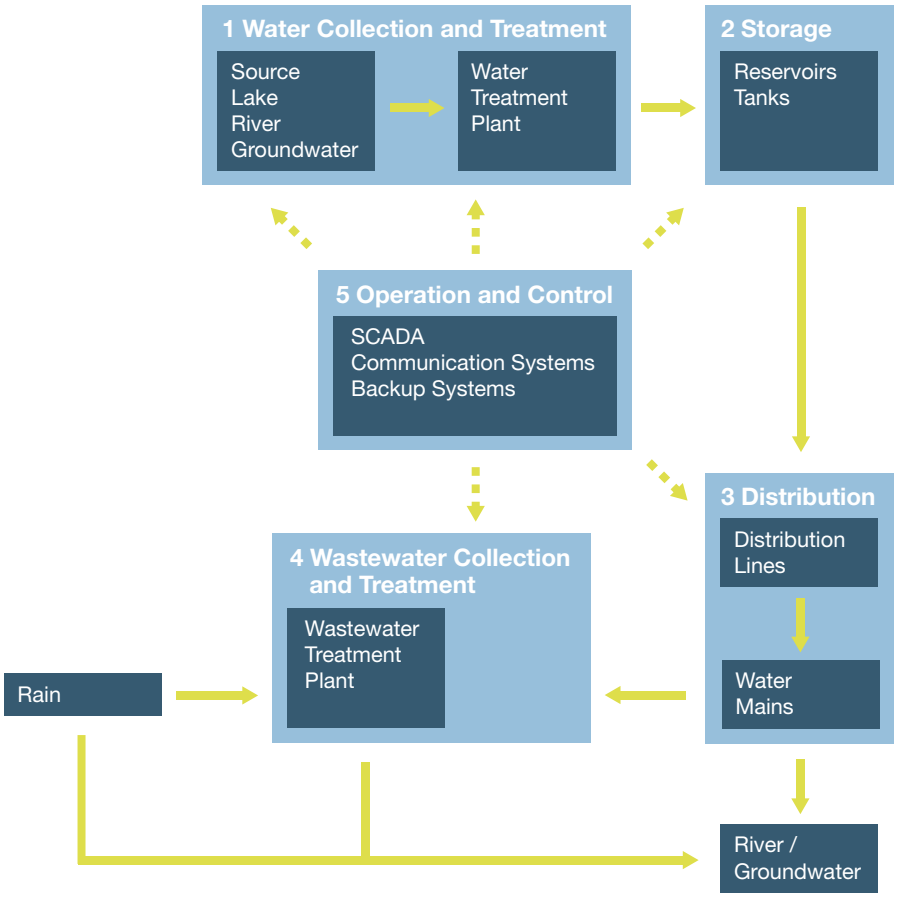
The individual, regionally-distributed water systems are highly diverse, ranging from simple systems that serve a few customers to complex metropolitan systems that serve millions, monitored by advanced computerised systems such as SCADA.

Different components of the system, such as reservoirs and pumps, are monitored and controlled centrally using sensors, measuring devices and signal transmission lines to a control room from which, in turn, signals are sent to the actuating elements (pumps, gates).

17 In case of earthquakes, the gas supply system is tolerably robust against shaking, but not against shear forces.

Most of the world's water supply systems are run by municipalities, although the participation of private companies in the financing, construction and management of water supply and wastewater systems has significantly increased during the last 10 years[18]. There are also significant differences in industry structure between countries: a European comparison published in 2005 showed that in Italy there were at that time about 10000 water suppliers, in Germany about 6000, in Belgium and Spain 139 and 129 respectively, while in Britain only 26 [Aquamedia 2005].

Figure 8: Typical components of the water supply and treatment system



Four typical forms of ownership and management can generally be found in the water sector: public management, public limited company, delegated and direct private management (Table 2).

Water is vital to society's well-being, but the interruption of water supply has only a minor immediate impact on the population when compared to interruptions to other critical infrastructures. The scope of loss of water supply is generally local or regional, but health-related risks can increase significantly with the duration of the interruption and be perceived as more serious than physical events or the loss of energy supply. On the other hand, the intentional or inadvertent introduction of some contaminants can have major consequences for public health.

In most countries there is a body of legislation focussing rather more on water quality issues than on market organisation, such as the EU Water Framework Directive [EC 2000] governing the acceptable

18 The internationalisation of the ownership structure ('horizontal integration') can also be observed in the water sector, albeit on a more limited scale, e.g. compared to the electric power sector.

amounts of contaminants, measured in parts per million, in a Member State's drinking water. In the US, "the Environmental Protection Agency (EPA) began working with other government agencies and water suppliers to ensure that the nation's water supply continues to be safe, even against terrorist attacks. EPA is providing local water utilities with the best scientific information as well as technical training on conducting vulnerability assessments and enhancing emergency response plans should an attack occur" [Geer 2005]. The Canadian Water and Wastewater Association (CWWA) developed template-based guidelines for owners and operators of municipal water and wastewater utilities to conduct vulnerability assessments. Similarly, the Swiss Gas and Water Association prepared a guidance document for the planning and realisation of water supply in emergency situations [SVGW 1995].

Table 2: Different water utility management models in selected countries and the EU (percentages) [Bakker 2005]

	Public	Public limited company	Delegated private	Direct private
US	86		14	
EU	48	15.5	20.5	16
Germany	55	30	15	
France	23	2	75	
UK	12			88
Netherlands	15	85		

In order to ensure a secure and affordable supply of water in sufficient quality for the domestic sector, no changes (such as further privatisation) or alignments of the different, country-specific ownership models are currently being considered at the EU level [OECD 2005]. Instead, the diversity of industry structures is retained by keeping the regulations at the country level. In the UK, for example, the Water Act 2003 established a Water Service Regulation Authority, which oversees economic regulation and also has responsibility for consulting with the independent Consumer Council for Water with the power to investigate matters that relate to consumers' interests [Water Act 2003]. Also in the UK, the Water Industry Act (1991) established a requirement for water companies to reach arrangements with other water companies in order to secure the supply of water in an emergency [Water Industry Act 1991]. To sum up, the UK's privatisation led to the development of complex regulation and control in order to protect customers, to guarantee an acceptable water quality and to protect the environment – this last as a reaction to serious shortcomings in the environmental performance of the UK water companies.

Water supply and wastewater management systems operate as open systems and are subject to multiple threats and vulnerabilities. They are highly sensitive to environmental impacts such as, for example, pollution of the source water in the aftermath of natural disasters or through sewage treatment overflow during heavy rain conditions. The consequences of such events often do not occur immediately and allow timely countermeasures, such as the activation of emergency response plans. Metropolitan water systems are highly vulnerable to the disruption of certain important nodes, such as treatment plants and reservoirs. In the US the metropolitan water systems contain a few large plants supplying some 75% of the population, and failures of these could have severe impacts [OECD 2005].

Box 6: The Maroochy Shire sewage spill

"In March 2001 Vitek Boden parked his car near a water treatment works at Pacific Paradise in Queensland, Australia. He switched on his laptop, typed a few commands and watched as 4.5 million litres of raw sewage spilt out into the waterways beside a nearby holiday resort. It turned the water black, poisoned marine life and created an overpowering stench." "Boden was an engineer formerly employed by the company that installed the computer system that controlled the water works. Bitter at missing out on a job at the local council, he exacted his revenge on the community by exploiting his knowledge of the works' control systems – with a little help from his wireless laptop connection" [Graham-Rowe 2004].

"To sabotage the system, he set the software on his laptop to identify itself as 'pumping station 4', then suppressed all alarms. Like thousands of utilities around the world, Maroochy Shire allowed technicians operating remotely to manipulate its digital controls. Boden learned how to use those controls as an insider, but the software he used conforms to international standards and the manuals are available on the Web. Nearly identical systems run oil and gas utilities and many manufacturing plants" [Washington Post 2002].

Almost all urban water services in developed countries – whether public or private – are heavily subsidised[19]. As a consequence, water utilities are strongly dependent on unpredictable and ad hoc political decisions regarding water-related expenditures. Such decisions often result in price increases which are significantly below the amount needed to cover maintenance, infrastructure upgrading, and the replacement of aging assets [OECD 2005]. The result of this under-investment is a degraded infrastructure with leakages in distribution systems. These leakages are becoming a serious problem, endangering the security of supply[20].

In some countries there are increasing concerns about terrorism and other deliberate attacks on the water infrastructure. In the US, budgetary provisions to 'harden' the water infrastructure against acts of terrorism and sabotage are in the range of US$ 1.2 billion [OECD 2005]. The EU will include water in its programme on critical infrastructure protection [EC 2005b].

Attacks on the water infrastructure can take two main forms: contamination from biological or chemical agents or disruption of processing and distribution.

Unintended or intended contamination can be caused by:
- Accidents in the transport of dangerous goods
- Fertilisation with sewage or chemical products
- Contamination with chemical, biological or radiological materials.

Disruption can be provoked by:
- Technical and human failures, industrial accidents and fires
- Physical damage such as pump outages or loss of pressure
- Natural hazards such as floods, drought, earthquake, mudslides
- Cyber attack on the monitoring or control systems. (The importance of security measures against cyber attack is illustrated by a malicious spill in Australia (see Box 6).)

19 In Greece and Spain, for example, water tariffs are at some 25-30% of the true costs and in UK at about 90% [Lee 2001].

20 In the US, for example, current leakage rates from the mains are up to 50% in the case of older systems and a threefold increase of the repair costs is expected by the year 2030 [USHR 2004]. In the UK leakage decreased by around 20 million litres a day for the period of 2005/2006 [OFWAT 2006a]. It is worth mentioning that the UK regulator of the water and sewerage industry has the power to set leakage targets and to impose fines in the case of non-compliance [OFWAT 2006b].

Contamination of a reservoir would be unlikely to produce a large risk to public health because of its high visibility, consistent monitoring and dilution effects. Large reservoirs contain hundreds of thousands litres of water, and a massive amount of contaminant would be required for a successful attack. If agents were to be introduced at a reservoir point it is also likely that they would be detected. However, the likelihood of success is much greater if the point of contamination is at a stage in the system after treatment and storage facilities, such as in the water distribution system where monitoring, filters, chlorination and other preventative measures would no longer be effective, and where water quality is not monitored. Experts have identified the water distribution system ('the open end') as the most vulnerable element of the water supply and treatment system [GAO 2004]. It would, for example, not require a great effort to reverse the direction of the flow of water into the end-user installations, and the resulting backflow could be used to discharge contaminations into the distribution system. Here again, the dilution effect could reduce the severity of such a 'backflow attack' meaning that it would need to take place near to the targeted area in order to produce casualties. However, the fact that there are limited current capabilities to detect the large number of available agents makes timely countermeasures difficult or even impossible.

Box 7: Water system disruptions following the 2003 power blackout in the US and Canada [DHS 2003]

Cleveland experienced its worst water crisis in history as the blackout shut down all major pumping stations, which serve more than 1 million residents. The National Guard had to tank in thousands of litres of drinking water until taps flowed again. In Detroit five days after the outage tap water was still undrinkable. In major cities (e.g. New York) streams of raw sewage began to flow into surrounding waterways posing health and environmental hazards.

The most common accidental cause of contamination in distribution systems is a cross-connection to the wastewater system [Halliday 2003]. Unintentional backflow from end-user installations can also be responsible for epidemics, as can contamination by cryptosporidium after heavy rain. The psychological effect on the population of a possible contamination can be as, or more, important than that of other threats. Because much contamination cannot be detected visually, humans feel very vulnerable to a possible attack.

Impeding the ability of the water supply to reach the population can have far-reaching consequences. For example, businesses would not be able to conduct operations, manufacturing would be halted and daily routines would be interrupted. Without adequate water supply most fire department capabilities would be dramatically reduced.

Failures of wastewater treatment systems can lead to wastewater overflows into the environment, which result in public health issues.

Illegal electronic or physical access to operation and control systems may result in partial or total malfunction of the infrastructure system and may also disturb the water industry's role in emergency situations. Furthermore, economic pressure, such as price controls, may squeeze out back-up and reserve components such as redundant pumps or force reductions in the volumes of stored water.

Interruptions of the electric power supply can endanger water and sewage systems by, for example, putting pumping stations and water treatment plants out of commission (see Box 7). Failure of the road or rail transportation system may limit the supply of treatment chemicals. Furthermore, water systems rely heavily on the IT infrastructure for monitoring and control, particularly to regulate pressure.

The vulnerability of urban water systems, their dependence on other infrastructures, in particular on regular electricity supply, and the consequences resulting from failures were dramatically demonstrated in the US by Hurricane Katrina and its aftermath in August 2005 (see Box 8).

There are both technological and political-organisational measures that can reduce the vulnerability and the attractiveness for terrorist and cyber attacks of water systems. On the technological side new systems could be better designed by, for example:

- Reducing the vulnerability of water distribution structures
- Clearly separating water distribution channels and wastewater systems at critical interfaces (for example, at the end-user site).

Box 8: Hurricane Katrina – impacts on the New Orleans urban water system [Wikipedia 2005]

The New Orleans urban water supply could survive the storm itself – which was not the case of the regular electricity supply – despite a high number of broken pipes. But it totally collapsed as the flooding due to the destroyed dams of Lake Pontchartrain caused the failure of its back-up power plant.

Water purification and wastewater treatment plants failed and, as the pressure in the distribution system was lost, the supply became exposed to contaminants, such as untreated sewage leaking from broken wastewater collection systems. Consequently, the population was ordered by the state authorities to boil the tap water before using it. A shortage of potable water and its contamination became a serious health issue for people who remained in the most severely affected areas. According to the US Centers for Disease Control and Prevention, five people died from drinking water contaminated with bacteria.

The purification plants were back in service within a few days. However, the restoration of the distribution system in order to supply drinking water took weeks, as repairs to the countless and massive leaks were delayed due to the tons of debris like cars, houses and fallen trees. The costs associated with the damage to all public water supply systems affected by the hurricane are estimated at more than US$ 2 billion.

Older systems could be improved by:

- Using power backup facilities and redundant pumps (to overcome pump outages and power cuts)
- Restricting human access to critical water system components
- Monitoring and detection of, for example, pressure, water levels and, using fish/mussels/algae as indicator species, of water quality
- Adopting SCADA systems that do not use inadequately secured public telecommunications networks or the Internet to transmit control commands
- Using back-flow preventers.

In addition to technological improvements, governance principles for water management should be reviewed. We offer the following recommendations:

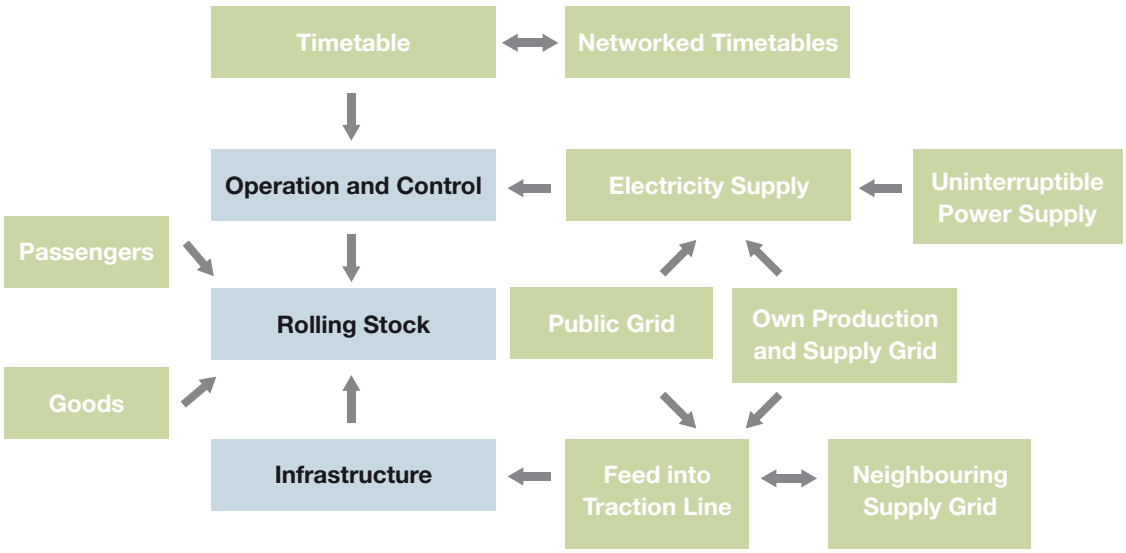
- In order to overcome the inherent problem of under-investment in infrastructure assets, the full economic costs of water services should be passed on to the stakeholders (end-users)
- There should be greater emphasis on “public accountability for decisions relating to the water system, effective exercise of the owner’s oversight responsibilities” [O’Connor 2002] and assurance of full transparency in decision-making
- Monitoring of the competence and effectiveness of system management and operation.

3.4 Transport by Rail

Railway systems provide transportation services for passengers and goods (including dangerous substances) in almost all countries and across borders. They consist of (see Figure 9):

- Operation and control (control centres, related computers and data lines)
- Rolling stock (locomotives and the wagons for passengers and goods)
- Infrastructure (tracks, signals, overhead traction line and electricity supply or diesel fuel stock, stations, etc.).

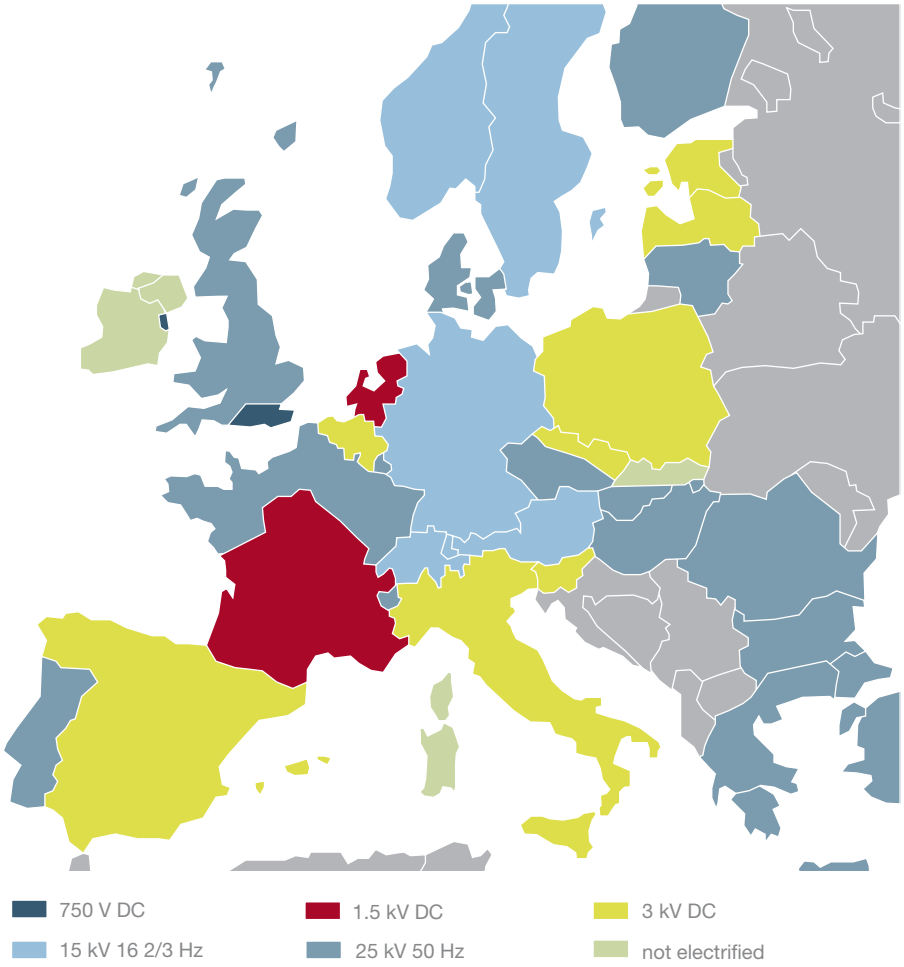
Figure 9: System diagram of a typical electric traction rail system



The railway system is part of the set of critical infrastructures, and interruption can have immediate and far-reaching consequences on society and on the economy of a country, as it is used by people to go to work and to move essential goods for industry (often just-in-time). In countries with high population density or metropolitan areas, substitution of railways is extremely difficult. Nevertheless the degree of criticality is moderate, as impacts of failures, losses and unavailabilities will in most cases be limited in scope (local to regional), magnitude (minimal to moderate) and effects of time. The rail transport infrastructure depends on other infrastructures, in particular energy supply and ICT systems to different degrees, whilst the energy sector may depend on fuel transported by rail and the ICT systems may use data transmission lines that are often routed along rail rights-of-way.

Networks are formed geographically at local, regional and long-distance level. Traditionally, these networks are largely separate and, in Europe, each is owned and operated by one – often state-owned – company. Nowadays, larger networks have been formed by linking networks physically (same infrastructure) and organisationally (timetables, ticketing). Older railway systems have been built at local, regional and state level in a fairly uncoordinated and inconsistent manner. For example, the main railway companies in Europe make use of four different electricity systems (see Figure 10) and different track gauges.

Figure 10: Railway electricity systems in Europe, electric traction is dominating in most regions [ISL 2005]



At a national level and in a liberalised market environment:

- Infrastructure companies provide construction, maintenance, and refitting (including electricity production and supply), often sub-contracted to other companies
- Transportation companies provide the purchase or leasing, maintenance and operation of rolling stock (including diesel fuel supply[21])
- Regulatory authorities provide basic conditions (guidelines, standards, etc.) and authorise and supervise the infrastructure and transportation companies.

Electric traction is widely used in Europe and in a few parts of the US. Diesel traction is widespread in many other regions. Many large rail companies have their own power plants to cover a part or all of their electricity needs, obtaining the rest from the public electricity grid. The signals and the control centres are normally powered by the public supply and backed-up by the railway grid. Additionally there is very often an uninterruptible power supply (UPS) for a few hours provided by batteries. In case of a total loss of electricity supply, signals fall into a 'fail-safe' state.

In the past, the primary political goal in the European rail system was to assure security of transport ('mobility') by rail at a level that is competitive with other carriers (road, air). In the meantime, elements

21 In case of unbundled state-owned railway companies, infrastructure and transportation services can be represented by divisions of the company.

of market liberalisation have been introduced in many countries, leading to privatisation and the unbundling of former national monopolistic companies. The UK serves as a prominent example of these developments. Subsequent problems have included under-investment in maintaining and renewing the system[22].

In Europe, at trans-national level, the EU Council Directive of 29 July 1991 on the development of the European Community's railways states that "the efficiency of the railway system should be improved, in order to integrate it into a competitive market, while taking account of the special features of the railways" [EC 1991]. As a result, the European rail system has witnessed a move towards harmonisation at the technical and organisational levels, promoting competitiveness with road transportation.

The following two organisations currently play a mayor role in railway governance, but they will have to show their relevance in the future liberalised market:

- The Intergovernmental Organisation for International Carriage by Rail (OTIF) has been established encompassing 42 countries and 25 organisations. The goal of this incorporated organisation is the harmonisation of regulation and of regulatory standards
- The International Union of Railways (UIC) has the goals of improving cooperation and harmonisation at a technical level, and of running projects, e.g. on harmonisation in training programmes for railway staff.

Railway systems are subject to various threats[23]:

- Sudden interruption of services due to loss of energy supply or communication and control
- Technical and human failures leading to accidents with losses or fatalities due to direct impacts (e.g. from the release of dangerous goods)
- Natural forces and other events or attacks, particularly those which impact on bottlenecks within the railway network or on important sections such as tunnels, with subsequent closure of affected sections and loss of services
- Malicious cyber attacks on control systems.

The railway system has a high degree of interaction and complexity. It is an open access system with a positive image in many countries and it is relatively reliable and safe. The N-1 criterion is applied in crucial parts of the system and data transfer and electricity supply systems are mostly, but not always, independent of the public grid.

In order to demonstrate the importance of compliance with rules and standards, the impact of poor information exchange, and the ability of single failures to cascade and affect wider society, we refer to two events that occurred recently in Switzerland: a failure of a railway control and communication system (see Box 9) and a complete loss of electricity supply (below).

On June 22, 2005 a complete blackout of the Swiss railway system was triggered by the shutdown of two of the three power lines due to nearby construction work (a violation of N-1 criterion) and the subsequent automatic shutdown of the remaining power line due to a short-circuit. As a result, the

22 In contrast, various organisations and a series of Acts of Parliament relate to railway safety in the UK. Under the Railways Act 2005, Network Rail, which owns the railway infrastructure, has direct responsibility and is accountable for ensuring the performance of the rail network. The Railway Group Standard gives detailed instructions and operability standards, while the National Railway Security Programme gives both mandatory and best practice standards for the industry. The Railway Safety and Standards Board provides a forum for stakeholders to keep up-to-date with safety standards and all rail industry parties must be a member of it. Although five severe accidents occurred since privatisation, the accident rate did not increase and is still in the range of the EU average [Hope 2002].

23 In addition, strikes by staff may be also be a threat to train transportation.

system's own power stations and power lines were shut down causing a total loss of electricity supply and stoppage of all trains 40 minutes later. It was not possible to connect the rail network in order to receive electricity supply from the public grid. More than three hours later the network was restored, and the trains started to resume regular operation.

Box 9: Failure of the railway control and communication system in the greater Zurich area (February 7, 2005)

Origin and mechanisms:

- Planned cable works on the data network in the central railway control centre of Zurich main station; a redundant line was out of order
- Movements inspectors were not informed about this work. They thought it to be a technical disturbance and tried to repair it; mismanipulation then led to an overloading of the network communication capacity
- Cascading failure of most computers in the railway control centre, resulting in the collapse of the whole system.

Consequences:

- Breakdown of the railway system for over 4 hours in greater Zurich area
- 300 trains were cancelled, 1250 passenger trains were delayed for a total time of approx. 180 hours, 250 freight trains of approx. 90 hours
- Passenger trains were misrouted due to the manual train operation
- Breakdown of the train information system for ten thousands passengers, nearly 100 missed flights at the nearby airport
- Railway control and communication system recovered only over 12 hours later.

[SER 2005], [NZZ 2005]

Trains are parked in open-access areas. They also stop in, or pass through, crowded and sensitive areas such as stations, hazardous facilities and protected areas. They must therefore be regarded as highly attractive targets for terrorist attacks, as has been demonstrated in, for example, Tokyo (underground station sarin gas attack, 1995), Madrid (commuter train bombs, 2004) and London (underground train bombs, 2005).

The following measures and principles are proposed as options for consideration to make the rail transport system more robust:

- Better balancing of economic pressures against broader societal needs, particularly in countries that have privatised all or parts of the system
- Setting of intergovernmental standards on security, quality assurance, education and training, etc., in order to cope with the increasing challenges faced by the railway system (e.g. higher density of timetables; tighter safety margins) as well as threats which derive from recent additions to what the system is required for, such as the long-distance trans-border transport of dangerous goods and devices, including nuclear waste
- Replacing dedicated ICT systems for operation and control by off-the-shelf and / or open access systems only in situations in which security and quality can be assured
- Performing comprehensive analysis and assessment of risks and of emergency management plans in order to identify weaknesses, bottlenecks and vulnerabilities, as well as to support the development and implementation of adequate countermeasures
- Particular consideration should be given to adopting effective measures against malicious attacks;

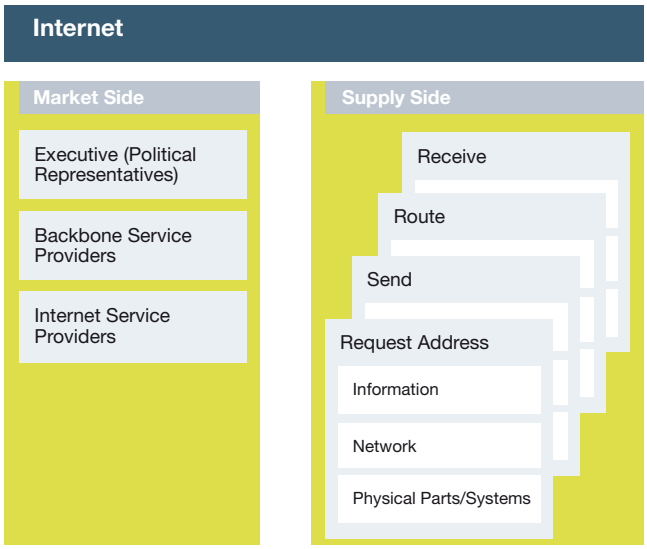
such measures will need to be balanced against societal values such as privacy, open society and passenger comfort:

- Technical: enhanced video surveillance of the most sensitive areas such as stations (both above and below ground), sidings and tunnels; extended personnel access control; monitoring of containers and freight wagons
- Operational: avoid trains with hazardous goods passing through densely populated areas (selecting alternative routes) or assign specific time slots which avoid hours of the day when the facilities are crowded
- Socio-political: raising the general awareness of the vulnerabilities and risks of the system; include rail transport in critical infrastructure protection programmes.

3.5 Information and Communication

The information and communication sector includes broadcasting systems, telecommunications (telephone, fax, cable and satellite), computer software and hardware as well as networks such as the Internet, which we take as an example for this report. The Internet connects computers and computer networks to enable, inter alia, the exchange of data, voice and multimedia content (see also Figure 11).

Figure 11: Simplified layered model of the Internet, comprising a network of world-wide interconnected computers and computer networks



The Internet is a "publicly accessible worldwide system of interconnected computer networks that transmit data by packet switching using a standardised Internet Protocol (IP). It is made up of thousands of smaller commercial, academic, domestic, and government networks. It carries various information and services, such as e-mail, online chat, and the interlinked Web pages and other documents of the World Wide Web" [Wikipedia 2006]. The Internet consists of the following functional components:

- Physical components: physical cable (fibre, copper), satellite links, servers, bridges and hubs (links between networks), routers (for data transmission through networks), personal computers (home user, network computers)
- Network components (such as Domain Name Servers[24] and Internet Exchange Points[25])
- Information components (operating systems, network software, databases, web servers and browsers).

24 Public accessible server containing a database with the capability of translating domain names to IP addresses.
25 A physical infrastructure connecting networks of different Internet Service Providers.

Governance of the Internet is difficult and relies strongly on international co-operation. Since the Internet is an open network of networks, many organisations build, maintain and secure parts of it. The main actors in its governance include:

- The Internet Corporation for Assigned Names and Numbers (ICANN), responsible for "managing and coordinating the Domain Name System (DNS)[26] to ensure that every address is unique and that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique IP addresses and domain names. It also ensures that each domain name maps to the correct IP address" [ICANN 2006]
- The Internet Engineering Task Force (IETF), responsible for the technological development of the Internet and for the support of standardisation efforts
- Registrars, responsible for the management of Internet Domain Names within a certain Top Level Domain (the last part of an Internet domain name, e.g. .org)
- Backbone[27] Service Providers, responsible for the operation of the fast and high-bandwidth network connections of the Internet core
- Internet Service Providers (ISP), responsible for user access to the Internet and for managing access networks.

The Internet is vital to modern economies and the degree of criticality is high. Apart from e-businesses relying on the Internet as their only sales channel, IP-based networks used to transport data and voice services (Voice over Internet Protocol (VoIP)) have experienced exponential growth over the past decade. Although there are major exceptions, particularly in electricity supply, many organisations rely on the Internet and on computer networks for daily operations both within their own organisation and in collaboration with partners, suppliers and customers. These operations include on-site and remote data management. This makes it rather difficult to separate the information and communication sector from all other sectors, including other critical infrastructures. Thus, one of the keys to robust critical infrastructures is the protection of information and communication systems including the Internet.

Numerous trends are influencing the development of the Internet. Amongst these are increased network speeds, the need for more bandwidth, the growing proportion of wireless network connections, ubiquitous computing, the convergence of formerly separate voice, TV, data and Internet access networks, and an increased number of available Internet addresses with the introduction of new protocols (IPv6: Internet protocol version 6 and others).

Box 10: Internet worm Code Red

"On June 18th 2001, a serious Windows IIS vulnerability was discovered. After almost one month, the first version of Code Red worm that exploited this vulnerability emerged on July 13th, 2001…The truly virulent strain of the worm (Code Red version2) began to spread around 10:00 UTC of July 19th, 2001" [Zhang 2006].

"More than 359,000 computers were infected with the Code-Red (CRv2) worm in less than 14 hours. At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute. 43% of all infected hosts were in the United States, while 11% originated in Korea followed by 5% in China and 4% in Taiwan. The .NET Top Level Domain (TLD) accounted for 19% of all compromised machines, followed by .COM with 14% and .EDU with 2%" [Moore 2001].

26 A distributed system of databases for translating domain names to IP addresses, e.g. irgc.org to 217.197.216.6.

27 Basic network infrastructure consisting mainly of routers and cables with high capacities and long distance connections.

Threats to the Internet may be grouped into two categories: (1) threats against the Internet infrastructure and (2) threats using the Internet as a platform or vector. The first category comprises threats such as:

- Intentional attacks against specific Internet routers, servers (e.g. a specific or targeted group of DNS), access networks[28] or minor backbone networks using Distributed Denial-of-Service attacks (see Glossary for a variety of cyber threats)
- Intentional cascade-based attacks on important Internet nodes
- Physical attacks or natural hazards hitting key Internet communication links, exchange points and/or DNS root servers.

Under the second category fall threats such as:

- 'Denial-of-Service' attacks including those in which so much traffic is introduced that the system becomes unusable
- 'Phishing', which solicits "confidential information from an individual, group, or organisation, often for illicit financial gain or other fraudulent purposes. These attempts are often conducted through a Web browser and involve social engineering. A 'Phisher' often uses spoofed e-mail, malicious Web sites, or Trojans delivered surreptitiously through a Web browser to trick users into disclosing sensitive data, such as credit card numbers, online banking information and other confidential information" [Symantec 2005]
- The propagation of malicious software programmes such as worms (an example is outlined in Box 10), viruses, Trojan horses and packet sniffers. For such threats the time from the discovery of a vulnerability to the development of early exploit scripts and to the widespread availability of automated attack tools that exploit the vulnerability has been dramatically shortened
- "Spam, usually defined as junk or unsolicited e-mail from a third party, made up over 60% of all e-mail traffic during Symantec's security threat reporting period" [Symantec 2005]. While it is certainly an annoyance to users and administrators, spam is also regarded a serious security concern as it can be used to deliver Trojans, viruses, and phishing attempts. Recent developments have shown an increasing proportion of spam being sent via the VoIP-channels.

Further information on Internet shortcomings can be found in [Lipson 2002].

The main vulnerabilities of the Internet in its present form are:

- The Domain Name System "comprises one of the few (logical) single points of failure within the Internet. More specifically, the root of the Internet namespace is held in 13 geographically distributed root name servers operated by nine independent organisations. In a worst case scenario, loss of all 13 of the root name servers would result in significant disruption to Internet operation as name-to-address translation (and vice versa) would no longer function" [Conrad 1999]. One example of a Distributed Denial-of-Service attack against the DNS happened on a global scale on October 21, 2002 although the impact was very low due to the high redundancy of 13 root name servers [Vixie 2002]
- The routing system represents a further vulnerability. This concerns mainly the inter-domain routing between the approximately 20,000 autonomous systems (AS). With a partial or total shutdown of AS due to power failure or physical destruction (an example is outlined in Box 11) there may be problems in recovering and restoring the functionality of the network as most inter-domain routing is based on complex contracts and requires manual configuration
- Mono-cultures of routers, switches, individual and networked computers, applications and operating systems increase the effects of any threat: a single vulnerability can exist and be exploited in millions of identical copies of the same software

28 Part of a communication network which connects clients to their ISP network, either by physical or wireless connection.

- „The Web browser is a critical and ubiquitous application that has increasingly created security headlines over the past few years. Typically, Web application vulnerabilities are targeted by attacks that take advantage of input validation errors and the improper handling of submitted requests. This could allow an attacker to execute malicious code on the target system“ [Symantec 2005]. A key issue in the vulnerability of the Web browser is the widespread use of ‘active content’ that is downloaded to a user‘s machine and run with little or no awareness of the code‘s actions.

Box 11: Internet crash in Pakistan

On June 21, 2005 an undersea cable carrying data between Pakistan and surrounding countries developed a serious fault, virtually crippling data feeds including the Internet and telecommunications. The fault was detected South of Karachi on the Sea-Me-We 3 (South East Asia Middle East Western Europe 3) submarine cable, the only cable link to Pakistan. The system was down for more than 12 days. Many offices across the country ground to a halt as people realised this was not one of Pakistan’s regular, but usually brief, technical hitches.

For the entire time the Sea-Me-We 3 link was down, Pakistan had to rely on bandwidth of 100 Mbps (mega-bits-per-second) available via satellite. Even this was achieved only through some ad hoc provisioning with carriers in the region by Pakistan Telecommunication Co. Ltd which increased the satellite bandwidth from about 34 Mbps before the mishap; before the cable fault, Pakistan was using bandwidth of about 775 Mbps.

Pakistan was not the only country affected. While the cable was being fixed, Internet users in India, the United Arab Emirates, Oman, and Djibouti also experienced disruptions for several hours as all data transport in the cable was shut down. The cable is owned by a consortium of 90 countries, and has end points in 36 countries, including Pakistan.

In contrast to Pakistan and a number of other developing countries, there are large numbers of cable links connecting most developed countries.

[Reuters 2005], [The News International 2005], [IDG News Service 2005]

The increased use of IP-based communication, and the subsequent non-investment in and non-replacement of alternative communication channels, especially by network operators such as Internet and Backbone Service Providers, will increase the vulnerability of critical infrastructure operators in cases of partial Internet failures.

The functioning of the Internet relies heavily on the public telephone network. More specifically, although the public telephone network and the Internet are for the most part logically distinct, they are closely tied physically because both depend on the same fibre-optic infrastructure and, more recently, the same wireless connections. Besides these intra-system dependencies the Internet depends on a number of other infrastructures and/or is an integral part of them. Examples of this dependency include:

- Dependence on sufficient power supply for the operation of DNS, Internet Exchange Points, and Internet Service Providers
- “Active Worms, autonomous programmes that spread through networks by searching, attacking, and infecting remote machines” [Weaver 2002] automatically have an increasing effect on other critical infrastructures.

Measures to reduce the Internet's vulnerabilities involve the sharing of responsibilities amongst owners, operators and users. Options include:

Organisational measures:

- Current Internet governance arrangements should be improved, especially with regard to the administration of the Domain Name Service, interconnection costs, Internet stability, security and cyber crime, spam, data protection and privacy rights, and IP addressing, amongst other issues. The United Nations Working Group on Internet Governance (WGIG) has recently recommended such improvements to Internet Governance mechanisms [WGIG 2005]
- Better partnerships need to be built with ISPs to promote the adoption of best practices and codes of conduct. This is of paramount importance since computers or computer networks "operated by home users or small businesses (less likely to be maintained by a professional system administrator) are integral to the robustness of the global Internet" [Moore 2001]
- The effective mitigation of Internet vulnerabilities may not be possible without also addressing the issue of the prevailing product monoculture
- Raising awareness of the increasing dependence on the Internet of businesses and economies.

Technological measures:

- Enhancing the security protocols on which the Internet is based. The primary focus should be on the improvement of the Internet Protocol (e.g. updating IPv4 to IPv6), the Border Gateway Protocol as well as the Domain Name System. An example of added security to the DNS are the DNS Security Extensions (DNSSEC), which provide „a) origin authentication of DNS data, b) data integrity, and c) authenticated denial of existence" [DNSSEC 2006]
- Promoting improved routing technologies including source address verification
- "Key businesses and services that must continue to operate in a disaster should examine their dependence on Internet connections and plan accordingly" [NAP 2003]. This applies specifically to critical infrastructure operators that increasingly rely on IP-based communication, since they may face serious problems due to the lack of alternate communication channels in an instance of partial Internet failure
- "Network operators and telecommunications interconnection facility operators should review their emergency power procedures" [NAO 2003]
- Develop new mechanisms to be able to provide security within the Internet that spans multiple autonomous systems.

Even with all these improvements, there are limits to how secure the Internet can be made. Critical communication and control functions should not, therefore, use or be accessible via the Internet.

Many infrastructures make use of ICT services[29] for operation and control and have integrated ICT into their systems while coping with increased demand and escalating interconnections and transactions among local and regional systems and owners/operators. While commercially valuable, these developments also create vulnerabilities, partly due to their connectedness and openness – both of which facilitate malicious attacks. This trend will continue and consolidate in the future with the electric power/energy infrastructure the most likely to serve as both driver and pathfinder and, therefore, as a kind of reference point. Furthermore, equipment maintenance, whether electromechanical or cyber-digital, is already heavily dependent on remote access to the facilities and the local use of portable ICT-devices.

29 Services are characterised by fundamental properties such as functionality, performance, cost, security, usability, manageability, and adaptability.

In the past, several of the European infrastructure operators deployed their own dedicated networks mainly based on fibre optics. This was seen as a natural extension of the company's resources. In the last few years, many of these lines increased in economic value and were sold to telecommunication companies. These infrastructure operators were therefore demonstrating that they could find it more convenient to pay for a communication service when needed, rather than have to design, run and maintain their own system. Generally, these communication lines are open ones – meaning that they are open to universal access, paving the way to logic bombs, viruses, and exposure to a full range of Internet attacks and all kinds of software designed to harm a computer system (malware).

As a general rule, ICT has not been developed with industrial applications in mind. This is even more the case in its use within other critical infrastructures. This appears to be because of the need for lower costs and does not adequately account for either longer-term risks or the added vulnerability it leads to. We have found only limited evidence that ICT assurance and security have been the subject of intensive discussions by infrastructure owners and operators, or considered in standards [EC 2005], [Gheorghe 2006], [WFS 2003].

The ubiquitous intensified use of ICT introduces a broad set of potential failures:

- Each system component might include faults deriving from its incorrect design or development, or from improper application
- Its deployment in a certain operational medium might cause physical deterioration of the hardware, e.g. due to extreme temperatures or intense EMF
- The combination of various systems might bring about interaction faults
- The interaction with human operators is prone to accidental errors, such as input mistakes, and offers the potential for malicious intrusion attempts.

Some mechanisms for coping with these failures have been introduced, but currently they are only used for industries considered to be safety-critical. And even in these industries, the availability and application of such mechanisms seem to be hardly sufficient.

The following measures are proposed to cope with the situation described in this section on industrial ICT and the Internet (mostly based on [EC 2005], [GAO 2005], [Gheorghe 2006], [WFS 2003]):

- Carry out a more comprehensive risk assessment and proper security assessment; in particular, include risks arising from 'classical' system failures and industrial ICT operation and control in combination, integrate cyber attacks and increase the use of probabilistic methods within such assessments
- Make security a top objective and apply security standards and countermeasures to ICT and open access communication systems such as the Internet, distinguish between the immediate effect of threats on ICT, and secondary impacts on the interconnected infrastructures
- Involve all stakeholders in the assessment of and protection against risks and security threats; stimulate stakeholders to build trust among each other in order to improve information exchange and collaboration.

4 TECHNICAL, MANAGEMENT AND ORGANISATIONAL STRATEGIES

Strategies to reduce the probability of disruption to services provided by the five infrastructures examined here, as well as the social vulnerabilities associated with them, should encompass technical, management, and organisational measures. Adequate strategies and policy options (see chapter 5) must consider the different characteristics of the various infrastructures such as their complexity, dependencies and interconnectedness, as well as such important contextual factors as the market environment. Infrastructures can be vulnerable to a variety of events including failures of system components, human errors, natural hazards such as extreme weather conditions or earthquakes, and malicious attacks. Furthermore, critical infrastructures have been, remain and will probably always be subject to changes of different degrees and speed, with technological development and market liberalisation as the current drivers. Some infrastructures, the electric power system in particular, have been designed for conditions other than those under which they now operate.

Based on the summary of each infrastructure given in the previous chapter, Table 3 provides a template for an initial assessment of the characteristics of the five infrastructures studied. It also addresses certain of the different dependencies between the infrastructures. For example, transport by electrified rail systems relies on continuous electricity supply and ICT support, so these cells are marked red. The importance of electricity to other infrastructures and the associated dependencies are more moderate and thus are marked yellow. The matrix also estimates and cross-compares the degree of criticality – from an admittedly Western societal perspective – using factors such as the scope of the geographical area affected, the magnitude of impact or losses and the effects of time of a service interruption or degradation. This assessment matrix[30] may provide initial guidance (in the absence of more detailed assessment and analysis) on where to put emphasis on risk governance strategies and how to tailor the measures that are outlined, below. The results may differ for another societal context, or from an individual perspective.

Critical infrastructures are vulnerable to a variety of disruptions. The first step in guarding against such events is an adequate assessment of the range of possible accidental and intentional disruption scenarios as well as of possible weaknesses, including 'bottlenecks'. In the case of many infrastructures, this has either not been done with the necessary degree of breadth and depth, or the appropriate analytical methods or capabilities have not been developed or used. Sometimes those who have done such analysis have not been able to accomplish adequate communication with the public and decision makers in order to motivate appropriate corrective actions in response to their findings.

Having analysed the events that might give rise to system failure, the next step is to perform contingency and failure analysis appropriate to meeting pre-agreed societal needs and objectives (e.g. appropriate levels of security; balanced degree of redundancy; alignment of the criteria for automatic protective devices with those needs; etc.). However, in many important areas, there is as yet no agreement on such needs and objectives, especially in an international context. Simple safety criteria (N-1, N-2) and failure consequence methods are widely used in assessing and in shaping the design of many infrastructures. In many of today's complex systems, more sophisticated approaches are needed.

30 This evaluation should be backed by more detailed analyses, possibly to be done in future infrastructure projects by IRGC and by other organisations with capability to carry out the more sophisticated investigation and analysis needed for more precise guidance on system weaknesses and needs for improvement.

One major source of difficulties, which has been a factor in a number of cascading power outages in both the US and Europe, is the absence, inadequacy or inappropriate implementation of agreed and mandatory procedures and rules[31] to govern the operation and control of separate parts of the larger system. In the creating or modifying of such rules, consideration must be given to balancing conflicting social objectives. Market mechanisms may play a role in this process, but we believe that much of the need is for improved and more explicit political objectives and enabling frameworks, especially at the international level.

Table 3: Assessment matrix for the five infrastructures selected for this study. Colours are used for our initial judgement: red corresponds to high, green to low, yellow to in-between; transitions from one colour to another indicate changes/trends.

			Electricity	Gas	Railways	ICT	Urban Water
Infrastructure characteristics	Complexity	Physical					
		Organisational					
		Speed of change					
	Dependence (interconnected-ness)	On other infrastructures					
		For other infrastructures					
		Intra-infrastructure					
		ICT control					
	Vulnerability	External impact*					
		Technical/human failure					
		Cyber attacks					
		Terrorist target					
	Market environment	Degree of liberalisation					
		Adequacy of control					
		Speed of change					
Criticality	Degree of criticality – factors	Scope**					
		Magnitude					
		Effects of time					
	Overall degree of criticality						
Governance	Elements of risk governance – inadequacy of	Awareness					
		Goal setting					
		Process/means***					
	Inadequacy of current risk governance						

* *Natural hazards, construction work, etc.*

** *Potential of cascading transnational effects*

*** *Including actors' participation; responsibility and liability issues*

Of course, rules alone are not sufficient. System operators must also know what is happening so that they can take informed actions. This means that, for safe and reliable system operation, one must have

31 In the meantime, the UCTE has made such procedures and rules [UCTE 2005b] mandatory and the US NERC is going to do so.

real-time situational awareness and emergency preparedness along with adequate system-wide scope based on improved instrumentation and communications. The need is perhaps greatest in the case of electric power and rail transport. However, in a world in which terrorism is a growing threat, improvements are also needed in a number of other settings, such as urban water distribution systems.

Many critical infrastructures are susceptible to common-cause or causal failure. For example, suppose that status and control channels for a power system, communication circuits for rail signalling, and telephone cables all go through the same tunnel or corridor. In such a circumstance, a fire or other 'common-cause initiation' events could cause all of them to fail simultaneously.

Before one can address the risks posed by such potential common-cause or causal failures, they must first be identified. That is often not easy to do and requires careful and extended data collection and analysis informed by real-world experience. One solution is to add independence, redundancy or spatial separation, but these can also add unintended complications. The performance of large complex interconnected systems is not easy to predict. In some cases, such as the electric power system and many ICT systems, the complexity can be so great that complete analysis is simply not possible. Nevertheless, more comprehensive and holistic approaches need to be undertaken and, for many areas, more sophisticated methods developed.

ICT systems present a range of challenges for all of the infrastructures considered in this report. Many key systems for situational awareness and control are still highly vulnerable to accidental or intentional disruption or spoofing. Such systems should not make use of, or be interconnected to, the public Internet, which is inherently insecure and will remain so for the foreseeable future. However, at present, a number of such systems are connected to the Internet and are thus vulnerable to accidental disruption or intentional cyber attack. Further investigation and actions to reduce such vulnerabilities are urgently needed. Adequate physical system maintenance and support are also vitally important.

A number of critical infrastructures suffer from the fact that they have grown in a rather unplanned and unstructured way, sometimes without basic changes in operation and control. Often, decentralised control areas are maintained while the system has expanded spatially, hence requiring better coordination and data exchange. Coherent expansion planning and associated capacity expansion is critically important if these systems are to evolve in ways that are consistent with the interests and needs of all affected parties. However, such systematic planning can run counter to market competition objectives and privatisation. Gradually, strategies are being evolved to reconcile these tensions but, in the case of several infrastructure systems, much additional attention is needed.

New technology, such as more capable SCADA systems, can sometimes play an important role in relieving previous technical or institutional constraints, as well as in providing new functionality. But this may also introduce new vulnerabilities.

Even the best-designed systems will fail occasionally. When this happens, operators may never have experienced such circumstances before and may not know how to react. Several strategies can reduce the risks in such circumstances:

- Strategies and designs that support 'graceful' degradation of capabilities ('island solutions' in power systems' control and grid structure and reduced bandwidth and traffic priority in ICT, to give two examples)
- Demand management, including priority setting
- The incorporation of rapid-acting, cooperating, distributed autonomous computer control agents
- Careful contingency preparation, including operator training conducted in realistic simulators.

While it is tempting to focus exclusively on the importance of critical infrastructures, one should remember that it is the social services they provide, not the systems themselves, that are most valued by society. This insight implies that, in addition to doing what can reasonably be done to assure the continued operation of the system, attention should also be directed at enabling critical social services to continue to operate in the face of primary system failure. Thus, for example, if new gas turbine peaking plants are installed near large pumps for water and sewer systems, and appropriate wiring and controls are installed, water and sewer service can be maintained even if the electrical grid suffers a cascading failure. However, if the natural gas system also fails or is degraded, storage of fuel near the gas turbine may be needed to assure that the pumps can continue to run in the event that both the electrical grid and the natural gas systems are unavailable. Failures affecting the electrical grid and the natural gas distribution system occurred in Georgia in January 2006 as a consequence of terrorist attacks on both systems. Similarly, if traffic lights are converted to low power Light Emitting Diodes (LEDs) and backed up with solid state controls and trickle-charged batteries, traffic can continue to flow in urban cores, even when the power goes out.

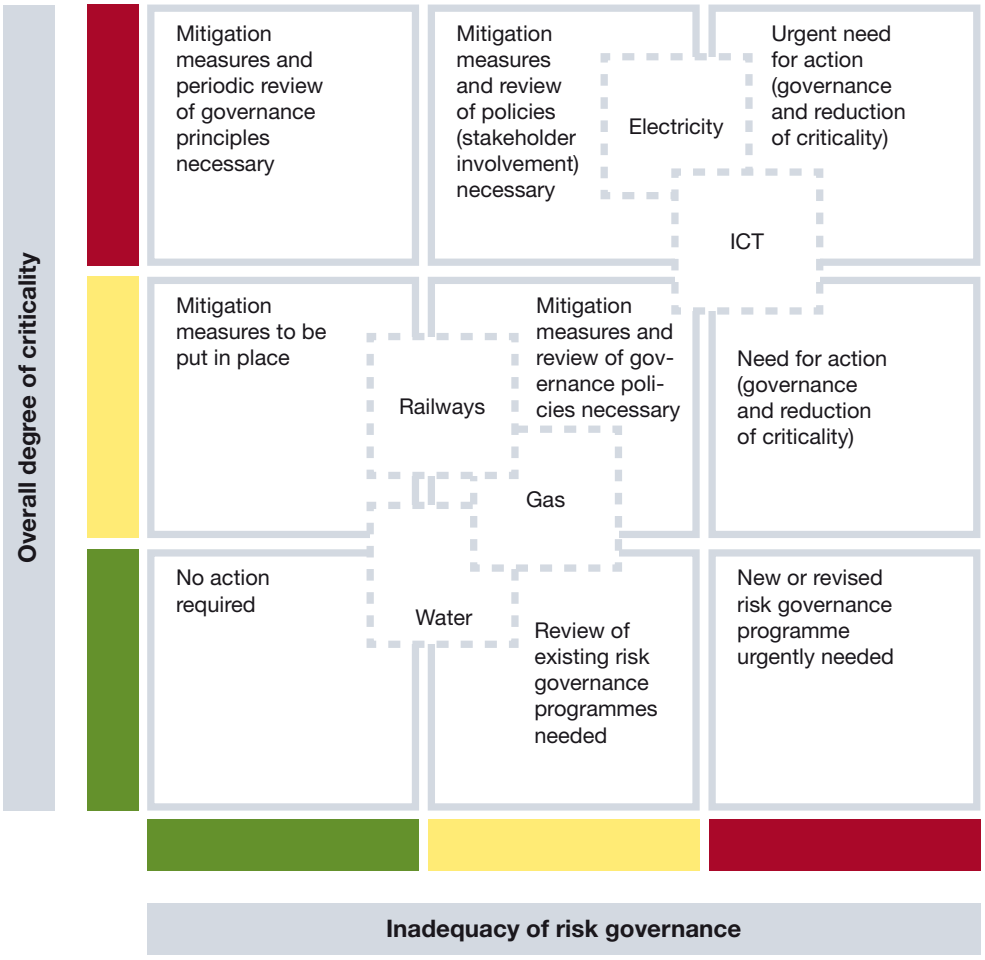
Since occasional service outages are unavoidable in a world with storms, floods, earthquakes, and terrorism, it is important that system operators maintain equipment and prepare effective plans for the rapid restoration of services. This deceptively simple observation carries some very profound implications in terms of stockpiling critical components and sharing resources among different system operators, as well as training and preparing work crews.

5 POLICY OPTIONS

The five infrastructures discussed in this report are embedded in a multifaceted context, which is continuously changing and becoming more and more instable. Risk factors (see Box 2) are increasing while the spectrum of threats has broadened, particularly in relation to cyber and physical terrorist attacks. The infrastructures are highly complex and interconnected, challenging our abilities and willingness to assess and understand their vulnerabilities and to take appropriate actions to reduce these vulnerabilities. Typically, these actions involve increased costs, which must be paid for through increased service prices or from other sources such as government subsidy. The systems are all subject to increased stress, to different degrees, and are also dependent on the different market environments and operational contexts. All of these factors raise questions concerning conflicting objectives and the adequacy of risk governance.

For the electric power and information and communication systems in particular, a gap has been identified between the dependence of Western societies on those systems and the adequacy of the approach taken to addressing security of supply issues (see preceding chapters). We conclude that further efforts are needed to understand these complex issues, to share that understanding with decision makers and the public, and to increase cooperation among the parties responsible for risk management of these systems. These parties include the system owners and operators, and governmental departments, agencies and regulators at levels extending from local to regional, national, and international.

Figure 12: Degree of criticality vs. adequacy of risk governance for five critical infrastructures (simple schematic)



Given the high societal importance, members of the public and non-governmental organisations will have a strong interest in observing the process and participating in dialogue regarding the decisions to be taken, especially when there are important financial or supply consequences for them. It is especially important that goals and paradigms be examined in the process of improving risk governance for these systems (see lower part of the assessment matrix in Table 3). Recent emphasis and evolution toward more open competitive markets in the US, the EU, and also in Russia and elsewhere, needs further investigation, particularly of the implications of such changes to system vulnerability. In order to achieve agreement on system goals, processes for dialogue and stakeholder participation should be reviewed and perhaps improved. Figure 12 provides a highly simplified overview of the kinds of actions needed and indicates their importance and urgency.

In many parts of the world, programmes to identify and protect critical infrastructures against malicious attacks have been undertaken (as in the US) or are going to be established (e.g. the EU [EC 2005b]). All five infrastructures addressed in this IRGC report should be included in such programmes.

Table 4: Policy options to improve the protection of critical infrastructures (depending on their degree of criticality and their respective environment)

The creation of institutions and governance processes that involve all relevant players and that consider and balance conflicting social objectives such as economic efficiency, security and privacy and that aim at establishing an overall framework for improved risk governance.
A legal mandate for specific system structures and capabilities, such as redundancies, SCADA, and binding operational rules such as security criteria and contingency management procedures; independent monitoring of compliance with these requirements.
Improved public reporting of service performance, particularly of service disruptions and their causes.
Investigation of system failures by technically qualified and independent organisations.
Clear delineation of responsibility and liability in the event of system failures.
Creation of institutions to identify and promote the adoption of 'best practices' by all participants.
Promotion of service level agreements between service providers and customers with financial and other guarantees and penalties.
The creation of insurance mechanisms to compensate losses.
Tax incentives to create desired behaviours, and a range of incentives to assure adequate long term planning and investments.
Government subsidies to support socially desirable functions that cannot be supported by market-based or other means, such as protection against terrorist attacks.
The creation of institutions that identify, codify and promulgate voluntary standards and best professional design practice, especially in the context of ICT systems.
Procurement strategies that promote voluntary standards and best professional design practice in the acquisition of new systems; monitoring and public reporting of compliance.
Creation of a legal/regulatory environment that at least allows (and, when needed, promotes) multiple service routes and providers.
Mandated basic technology research, funded at least in part as a cost of doing business by all players.

A number of policy options have been identified and are listed in Table 4. These options can be used to promote the adoption of socially desirable technical, management, and organisational strategies to protect critical infrastructures. When our analysis allows us to make specific recommendations relating to one of the five infrastructures we have discussed, we do so. These are highlighted in Box 12. However, the more general contribution of this IRGC report is to highlight issues for further investigation, analysis and dialogue with stakeholders. This process should provide increased understanding of system vulnerability and lead to a more detailed set of strategies for improved risk governance and reduced system vulnerability. Our recommendations reflect our opinion, and should be regarded as provisional and subject to possible change based on further investigation, analysis, and stakeholder dialogue.

Some critical infrastructure systems (or elements of them) are owned and operated by private parties, some by local or national governments[32]. Clearly, governance options differ in these two cases. Yet, even if in private ownership, if the system is truly critical, other parties who depend upon the services it provides (end-users) must be given a role in developing the policies and practices that govern its operation and in overseeing their effective implementation. Classical decision-making and risk management processes should be revisited and, where necessary, supplemented or even replaced by more participative governance strategies.

32 There is no single owner of coupled infrastructures.

Box 12: Some specific policy recommendations

IRGC has not been able to systematically review all important critical infrastructures, nor have we been able to study the five that are discussed in this report in sufficient depth to make comprehensive policy recommendations about all of them. Nevertheless, we have learned enough in our examination of these five infrastructures to make a few specific recommendations which we summarise below:

The Electric Power Supply System

Directives and goals (e.g. the EU electricity market Directives and Regulations), national legal and regulatory institutions as well as policy provisions are still all market-focused. Reliability criteria are often traded-off against other important factors in liberalised markets. Therefore:

- Security of continuous supply should be addressed more explicitly and become a new overarching principle. Strategies to ensure an appropriate level of protection and resilience need to be promoted.
- Top-down political decision- and rule-making processes should be revisited to include an appropriate level of technical analysis and dialogue with stakeholders. Different governance approaches are needed that not only embrace all major players (including end-user groups) but also address key challenges (for example tariff structures to ensure adequate investments and to establish financial risk transfer mechanisms).

The Gas Supply System

- There is a need to establish and make available an easy-to-use information system covering the location of gas pipelines, mainly to be used by civil engineering workers and emergency forces.

Water

- Proceeding from studies determining their effectiveness, systems and measures should be considered to improve the monitoring of water and sewage systems.
- Restricting human access to critical water system components, including water works and end-of-distribution systems.
- In particular, dams should be adequately protected against terrorist attacks.

Transport by Rail

- Upgrading and revision of intergovernmental standards is needed on security, quality assurance, education, and training, etc., in order to cope with the more challenging use of the railway system (higher density of timetables, tighter safety margins) and new threats (trans-border transport of dangerous goods and devices).
- More effective technical, organisational and socio-political measures against malicious attacks should be carefully considered and balanced against social values such as privacy, open society and comfort.

Communication and Information (Internet)

- System owners, operators and users should strive for, and share the undertaking of, the organisational and technological measures needed to reduce the Internet's vulnerabilities.
- The current public Internet is not secure. Until efforts to develop much more secure Internets in the future are successful, the public Internet should not be used for any function which is vital to the supervision, operation, or control of any critical infrastructure. Instead, dedicated communication systems should be employed that involve no logical link to publicly accessible computer systems and networks.

The management of almost all critical infrastructures requires trade-offs between a variety of legitimate private and public objectives. These include: economic efficiency, profit, systems security and continuity in service delivery, security of sensitive data and the privacy of the individuals being served. In the case of most of the infrastructures we have studied, there are no legitimate institutions, or governance processes, which involve all relevant players, and which have as their objective the identification, consideration and balancing of conflicting social considerations. In other cases, infrastructures that were previously operated by vertically structured, state-owned monopolies under supervision provided by a public regulatory authority or some similar entity have now been unbundled and privatised, causing institutional fragmentation (see Figure 4). Where institutions and governance processes to provide the necessary supervision have not been created, governments should move to create this capability, while guarding against any tendency to over-regulate. In some cases, the necessary levels of protection could be achieved through legal mandates for specific system structures and capabilities, and by introducing and enforcing binding operational rules. In such cases, it is important that there are independent institutions which have the technical capability and legal authority to assure that the rules are being met, and can impose sanctions when they are not. In all cases, provisions should be included for stakeholders to observe and participate in the process.

Even in the best of circumstances, problems may develop and failures may occur. In these events, accident analysis and reporting should be performed by an independent entity, and not by the same organisation which is responsible for the design, operation and maintenance of the infrastructure system. The best example of this in operation is aircraft accident investigation which, for example, is performed in the US by the National Transportation Safety Board, and not by the airlines themselves. Further, such investigation is undertaken completely separately from legal arguments about responsibility and liability. At the same time, delineation of responsibility and assignment of liability is another mechanism to assure that responsible operating parties take failure seriously. Insurance solutions can provide protection for affected parties, and to the extent that premiums reflect risks, can also provide appropriate incentives to system operators for safe and reliable operation.

If an infrastructure is operated under classical rate-of-return regulation in which all capital investments are assured of earning a specified income, then the regulator can order the installation of system features or operational procedures that serve some broader public good, such as system security or even national security, and allow the service provider to recover costs by passing them on the end-users in the price charged for the service. However, as services are privatised, and competition is instituted, such solutions become difficult, particularly when some providers of critical services are subject to regulation by more than one regulator with different objectives. Tax incentives or subsidy programmes can be used to achieve similar socially-desirable objectives, but also need to be aligned with the actions of regulators. In many newly privatised systems, such steps have not yet been taken.

Information technology is evolving so rapidly that in many cases mandatory standards can be counter-productive, seriously impeding innovation or otherwise causing problems. While a few basic rules, such as no use of the Internet for system-critical control functions, make sense, in general a more flexible approach will be more appropriate.

Morgan et al. [Morgan 2004] suggest a number of strategies to promote the growth of effective system design standards without resorting to inflexible government regulation. These suggestions include:

- Best professional practice
- Certification
- Acquisition specification

- Legal frameworks
- Tort and liability
- Insurance
- Taxes or fees on uncertified systems.

In their opinion, the combined effects of such actions could prove far reaching and widespread adoption of best professional practice and certification standards should, over time, help to create a culture in which system designers routinely think about issues of anonymity and security as they develop systems.

One way to assure continuity of the services that critical infrastructures provide is to find ways to allow, or perhaps even promote, multiple service routes and providers. This is most easily achieved in telecommunications. It is also possible in electric power through the use of distributed controls, distributed generation, micro-grids, and intelligent distribution system management. But what is possible is not always allowed[33].

Finally, research can often create new options which can better meet and balance private and social interests. While R&D investments in ICT are substantial (8-10% of sales), too few are focused on addressing issues of security and reliability. In electric power R&D investments are much too low to meet societal needs (<0.5% of sales). The industry has not had a strong research tradition and restructuring has complicated matters, focusing many players on short-term bottom line issues and creating a 'free rider' problem. Unless R&D investments are mandated[34] for all players as a 'cost of doing business' it is difficult to see how this situation can be expected to change.

6 LIMITATIONS, OUTLOOK

This initial study examined five critical infrastructures, issues of interdependencies between them, and a number of socio-economic, contextual and physical factors which impact on them. We acknowledge that there are other important infrastructures that have not been considered such as air, road, water and multi-modal transport, other aspects of ICT, food delivery, financial services systems, health care, and government services.

We followed an infrastructure-by-infrastructure approach focusing on Europe and the US. Further study, involving a region-by-region approach that looks across several infrastructures simultaneously, could provide additional insights, especially if it is expanded to more regions and explores the influence of different cultures, regulatory environments and legal frameworks[35]. It would also be important to consider issues in the context of industrialising countries and regions.

We focussed mainly on reducing social vulnerabilities by increasing the reliability and robustness of the systems. There is a need for additional work which focuses on identifying social vulnerabilities and developing strategies to maintain critical services when the main infrastructures on which they depend fail or malfunction.

33 For example, in many parts of the US, laws granting traditional electric power companies 'exclusive service territories' preclude the operation of micro-grids, which serve more than a single customer.

34 This could be done by specifying that some proportion of value added (e.g. 1%) must be invested in R&D. Firms that do not want to bother to manage such research could be required to support a government R&D programme.

35 For example, it would be useful to examine several European countries, including Russia, to cross-compare the US and the EU 25, examine large Asian countries, small island states threatened by sea level rise, etc.

While this study defined 'critical' from a Western societal perspective, it would also be desirable to explore criticality (a) within another socio-economic-cultural context and (b) from the perspective of different stakeholders and individuals. While our analysis considered criticality in terms of scope, magnitude and effects of time, other factors may be more important for specific individuals or other contexts and infrastructures.

There is a need to develop and refine appropriate risk and vulnerability assessment methods. This should facilitate more effective assessment of the relative criticality of different infrastructures and related services.

This study gave some consideration to the duration of disruptions, although the principal focus has been on short-term impacts. Some of our conclusions could be different if, for example, we looked at long-term impacts – a long-term loss of water supply would certainly have enormous criticality. Nor have we given full consideration to the risks and vulnerabilities of the inputs to the five critical infrastructures. Future studies should give greater consideration both to more extended disruptions[36] and delayed effects arising from initial disruption, which may persist even after the original service has been restored, and to input supply issues, particularly the security of their supply[37].

Although we addressed a broad spectrum of threats including natural events, human failures and malicious attacks, more work needs to be done on:

- Natural disasters of large spatial extent and duration such as strong earthquakes, hurricanes, ice storms and floods
- Occurrence of multiple failures or attacks on a system, or simultaneous attacks on several systems, which may amplify total impacts
- Strikes and other labour actions
- Epidemics, pandemics, mass evacuation, etc.
- Longer-term developments such as migration or the impacts of climate change.

We have not emphasised the importance of stable social and political conditions, although their importance has been clearly demonstrated by instances of political sabotage and destabilising activities affecting key industries and infrastructures. Besides direct consequences such as loss of production, the unavailability of ICT support may seriously worsen the situation. More investigations are needed to better understand such complex situations and to propose clear, adequate governance strategies.

As even the best-designed systems will occasionally fail, we outlined strategies to reduce the risks in such circumstances. However, our analysis did not consider crisis preparedness and management, nor did we explore the importance of learning from major events such as Hurricanes Katrina and Rita, the European heatwave of 2003, etc. To better understand their impact on critical infrastructures, such events should be carefully examined. Such studies could provide input to the development of learning strategies to better cope with surprises in the future.

This report is targeted towards senior private and public sector decision makers and other stakeholders, and is intended to provide ideas for policy options. Therefore, it may not provide as much detail as some technical experts might like. However, we hope it will trigger additional work in specific areas, such as:

36 For example, damage to a critical high-voltage transformer may disrupt the grid for months.

37 For example, by functional and geographical extension of the energy infrastructures to include gas and oil, above-ground and maritime transport from exporting to consuming countries, etc.

- Impact of extreme weather conditions (heat, cold, storms, rain / droughts) on electric power and water supply systems
- Potential for common-cause or causal failure (geographic bundling of parts of ICT as well as energy and transportation systems)
- Conditions for the use of ICT (Internet) within secured industrial control systems (e.g. SCADA)
- Requirements for adequate spatial extension and forecast planning
- Detailed analysis of gas and oil supply systems, including driving contextual factors
- State-of-the-art assessment of modelling techniques.

We intend that this White Paper should raise wider awareness and act as a solid basis for a trans-regional political dialogue and cross-sectoral exchange of information. We encourage the active distribution of its recommendations and recognise that full consideration of some of our policy recommendations requires communication across an extensive network. For example, establishing an agreed set of system objectives for the European electric power system and interconnected ICT system and an implementation strategy for achieving them may involve a high level stakeholder workshop including representatives from the EU, national governments and regulators, industry / system owners and operators and end-user groups as just the first step.

IRGC will continue to explore the risks and vulnerabilities of critical infrastructures and will support the efforts of others working in this important area. We anticipate that our contributions will include applying the IRGC's framework for risk characterisation and risk governance [IRGC 2005] to critical infrastructure(s). In addition, we will also make efforts to communicate relevant information to developing countries as they plan and construct their own infrastructure systems.

7 REFERENCES

[Apt 2004] Apt, J., Morgan, G., et al., Critical Electric Power Issues in Pennsylvania: Transmission, Distributed Generation, and Continuing Services when the Grid Fails, Carnegie Mellon Electricity Industry Centre, July 2004, Draft

[Aquamedia 2005] New Ways in Water Supply, Aquamedia, International Water Website, www.aquamedia.at/templates/index.cfm/id/967, page visited in 2005

[Bakker 2005] Bakker, K., Global Trends in Private Sector Participation, www.geog.ubc.ca/~bakker/globaltrends.htm, page visited in 2005

[Bialek 2004] Bialek J.W., Recent Blackouts in US and Continental Europe: Is Liberalisation to Blame? Cambridge Working Papers in Economics CWPE 0407

[Carreras 2001] Carreras, B.A., Newman, D.E., et al., Evidence for Self-Organized Criticality in Electric Power System Blackouts, presented at the 34th Hawaii International Conference on System Sciences, Maui, Hawaii, 2001

[Cleveland 2005] Cleveland, F., IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption, 2005

[Conrad 1999] Conrad, D., Kato, A., Manning, B., Root Nameserver Year 2000 Status, www.icann.org/committees/dns-root/y2k-statement.htm, page visited in 2005

[DHS 2003] Department of Homeland Security, Daily Open Source Infrastructure Reports, www.dhs.gov/dhspublic/display?content=5580, page visited in 2003

[DNSSEC 2006] (short for DNS Security Extensions) www.dnssec.net, page visited in 2006

[EC 1991] COUNCIL DIRECTIVE 91/440/EEC of 29 July 1991 on the development of the Community's railways

[EC 1996] 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

[EC 1998] DIRECTIVE 98/30/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 June 1998 concerning common rules for the internal market in natural gas

[EC 2000] DIRECTIVE 2000/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2000 establishing a framework for Community action in the field of water policy

[EC 2003a] DIRECTIVE 2003/55/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2003 concerning common rules for the internal market in natural gas and repealing Directive 98/30/EC

[EC 2003b] 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

[EC 2003c] 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

[EC 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

[EC 2004] EU Document COM (2004) 702 final concerning Critical Infrastructure Protection in the fight against terrorism

[EC 2005a] The future of ICT for power systems: emerging security challenges, report on the workshop held in Brussels, 3-4 February 2005

[EC 2005b] Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, Brussels, 17.11.2005

[EC 2006] Green Paper, A European Strategy for Sustainable, Competitive and Secure Energy, COM(2006) 105 final, Brussels, 8.3.2006

[Erdgas 2006] Das Erdgastransportnetz in Europa, http://www.erdgas.ch/71.html#, page visited in 2006

[Ericsson 2004] Ericsson, G., Managing information security in an electric utility, ELECTRA (journal of CIGRE members), no. 212, February 2004, p. 20 ff

[Eurelectric 2004] Statistics and Prospects for the European Electricity Sector (1980-1990, 2000-2020), Brussels, Eurelectric, 2004

[GAO 2004] Stephenson, J. B., Drinking Water, Experts' Views on How Federal Funding Can Best Be Spent To Improve Security, GAO Testimony Before the Subcommittee on Environment and Hazardous Materials, Committee on Energy and Commerce, House of Representatives, United States Government Accountability Office, GAO-04-1098T, September 2004

[GAO 2005] Critical Infrastructure Protection, Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, GAO Report to Congressional Requesters, United States Government Accountability Office, GAO-05-434, May 2005

[Gheorghe 2006] Gheorghe, A.V., Masera, M., Weijnen, M., de Vries, L., Critical Infrastructure at Risk, Securing the European Electric Power System, Springer, 2006

[Graham-Rowe 2004] Graham-Rowe, D., Power Play, The New Scientist, Issue 2447, 15 May 2004

[Greer 2005] Greer Commission of Public Works (CPW), 'Facility Security', public information communication by the Greer CPW, www.greercpw.com/info_security.htm, page visited in 2005

[Halliday 2003] Halliday, R.A., Water, Critical Infrastructure Protection and Emergency Management, Public Safety and Emergency Preparedness Canada, Ottawa, 2003

[Hope 2002] Hope, R., Accidents Raise Fears about Britain's Fragmented Railway, Japan Railway & Transport Review, 33, Dec. 2002, p. 32 ff

[ICANN 2006] The Internet Corporation for Assigned Names and Numbers (ICANN), www.icann.org/faq/#WhatisICANN, page visited in 2006

[IEEE 1990] IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, Institute of Electrical and Electronics Engineers, New York, NY, 1990

[IEEE / CIGRE 2004] IEEE / CIGRE Joint Task Force on Stability Terms and Definitions, Definition and Classification of Power System Stability, IEEE Transactions on Power Systems, Vol. 19, No. 2

[IDG News Service 2005] IDG News Service, Bangalore Bureau, 5 July 2005

[IEA 2004] Electricity Information, 2004, International Energy Agency, Paris, 2004

[IRGC 2005] IRGC White Paper No. 1, Risk Governance – Towards an Integrative Approach, Geneva, 2005

[ISL 2005] Institut für Städtebau und Landesplanung, Universität Karlsruhe, www.isl.uni-karlsruhe.de/fallmodule/nord_sued_trans/Karte%20der%20wichtigsten%20Stromsysteme%20des%20europ%E4ischen%20Eisenbahnnetzes.jpg, page visited in 2005

[Kirschen 2005] Kirschen D., Why do we get blackouts? Presentation given at the EC Workshop on The Future of ICT for Power Systems: Emerging Security Challenges, February 2005, Brussels

[Knops 2004] Knops, H.P.A., De Vries, L.J., and Correljé, A.F., Energiekeuze(s) belicht Beleidskeuzes voor de inrichting van de elektriciteits- en de gassector in Nederland, The Hague, Wetenschappelijk Instituut voor het CDA, 2004

[Lee 2001] Lee, T., Oliver, J.-L., Teniere-Buchot, P.-F., Travers, L., Valiron, F., Economic and financial aspects, in: Frontiers in Urban Water Management – Deadlock or Hope. Ed. Maksimovic, C., Tejada-Guibert, J. A., IWA pub., 2001

[Lipson 2002] Lipson, H.F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, SEI Special Report, CMU/SEI-2002-SR-009, Carnegie Mellon Software Engineering Institute, Pittsburgh, November 2002

[Madani 2005] Madani, V., Taming the Power Grid, IEEE Spectrum online, 2005

[Moore 2001] Moore, D., Shannon, C., The Spread of the Code-Red Worm (CRv2), Cooperative Association for Internet Data Analysis (CAIDA), http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml, page visited in 2006

[Morgan 2004] Morgan, M.G., and Newton, E.M., Protecting Public Anonymity, in: Issues in Science and Technology, 2004

[Moteff 2003] Moteff, J., Copeland, C., and Fischer, J., Critical Infrastructure: What Makes an Infrastructure Critical? Report for Congress, Order Code RL31556, Congressional Research Service – The Library of Congress, January 2003

[NAP 2003] The Internet Under Crisis Conditions: Learning from September 11, National Academy Press, Washington D.C., 2003

[NATO 2006] NATO Energy Security Forum, February 24, 2006, Prague, Westby, J., CEO Global Cyber Risk LLC, Cyber Security, 2006

[NERC 2006] North American Electric Reliability Council, www.nerc.com, page visited in 2006

[NZZ 2005] Neue Züricher Zeitung, 9.2.2005, Zürich, 2005, p. 47

[O'Connor 2002] O'Connor, D., Report of the Walkerton Inquiry, Part II, A Strategy for Safe Drinking Water, Queen's Printer for Ontario, Toronto, 2002

[OECD 2005] OECD Futures Project on Global Infrastructure Needs: Prospects and Implications for Public and Private Actors, Second Meeting of the Steering Group, Discussion Paper, December 2005

[OFWAT 2006a] Leakage slightly down – companies warned against complacency (press notice). The Water Services Regulation Authority (ofwat), http://www.ofwat.gov.uk/aptrix/ofwat/publish.nsf/Content/pn2206, page visited in 2006

[OFWAT 2006b] What is Ofwat's role in leakage? The Water Services Regulation Authority (Ofwat), www.ofwat.gov.uk/, page visited in 2006

[PCCIP 1997] Critical Foundations: Protecting America's Infrastructures, Report of the President's Commission on Critical Infrastructure Protection, Washington D.C., 1997

[Public Citizen 2003] Public Citizen, Water Privatization Fiascos: Broken Promises and Social Turmoil, Public Citizen, Washington D.C., 2003

[Reuters 2005] Reuters, 28 June 2005

[RFC-2828 2000] Internet Security Glossary, Request for Comments, R. Shirey, Network Working Group, 2002

[Rinaldi 2001] Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., Critical Infrastructure Interdependencies, IEEE Control Systems Magazine 21, 2001

[Saunalathi 2005] Saunalahti Group Oyj, Espoo, www.saunalahti.fi/ility/index.html, page visited in 2005

[SER 2005] Schweizer Eisenbahn-Revue, 4/2005, Luzern, Minirex, 2005

[Shea 2003] Shea, D., Critical Infrastructure: Control Systems and the Terrorist Threat, Report for Congress, Order Code RL31534, Congressional Research Service – The Library of Congress, 2003

[SVGW 1995] SVGW, Wegleitung für die Planung und Realisierung der Trinkwasserversorgung in Notlagen (TWN), 1995

[Symantec 2005] Symantec, Symantec Internet Security Threat Report, Trends for July 04 – December 04, Volume VII, 2005

[The News International 2005] The News International, 4 July 2005

[UCTE 2004a] Union for the Co-ordination of Transmission of Electricity, Operational Handbook, www.ucte.org, page visited in 2005

[UCTE 2004b] Union for the Co-ordination of Transmission of Electricity, Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, www.ucte.org, page visited in 2005

[UCTE 2006] Union for the Co-ordination of Transmission of Electricity, www.ucte.org, page visited in 2006

[USHR 2004] USHR, Ageing Water Supply Infrastructure, Subcommittee on Water Resources and Environment, US House of Representatives 2004

[US Patriot Act 2001] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (US PATRIOT ACT), Act of 2001

[Vixie 2002] Vixie, P., Sneeringer, G., and Schleifer, M. Events of 21-Oct-2002, Internet Software Consortium, 2002

[Washington Post 2002] Washington Post, June 27, 2002

[Water Act 2003] Water Act 2003, Her Majesty's Stationery Office, London, 2003

[Water Industry Act 1991] Water Industry Act 1991, Her Majesty's Stationery Office, London, 1991

[Weaver 2002] Weaver, N., Potential Strategies for High Speed Active Worms: A Worst Case Analysis, U.C. Berkeley BRASS group, 2002

[WFS 2003] Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar, Document WSIS-03/GENEVA/CONTR/6-E, World Federation of Scientists, Permanent Monitoring Panel on Information Security, August 2003

[WGIG 2005] Report of the Working Group on Internet Governance, Château de Bossey, 2005, www.wgig.org/, page visited in 2005

[Wikipedia 2005] WIKIPEDIA, the free encyclopedia, www.en.wikipedia.org/wiki/Hurricane_Katrina, page visited in 2005

[Wikipedia 2006] WIKIPEDIA, the free encyclopedia, www.en.wikipedia.org/wiki/Internet, page visited in 2006

[Yeager 2004] Yeager, Kurt E., and Gellings, Clark W., A Bold Vision for T&D, Carnegie Mellon University Conference on Electricity Transmission in Deregulated Markets, December 15-16, 2004

[Zhang 2006] Zhang, G., Decentralized Information Sharing for Detection and Protection against Network Attacks, PhD Thesis, The State University of New Jersey, New Brunswick, 2006

8 GLOSSARY

Cyber threats:

Adware: An acronym of 'advertising' and 'software' and describes the kind of software that automatically starts downloading or displaying advertising material.

Computer virus: "A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting, i.e. inserting a copy of itself into, and becoming part of another program. A virus requires that its host program be run to make the virus active" [RFC-2828 2000].

Denial-of-Service attack: An attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, the attack aiming to cause the hosted web pages to be unavailable on the Internet.

Logic bomb: "Malicious logic that activates when specified conditions are met. Usually intended to cause Denial-of-Service or otherwise damage system resources" [RFC-2828 2000].

Malware: Is an umbrella term for all kinds of software designed to harm a computer system. The term is an acronym of 'malicious' and 'software'. It commonly includes computer viruses, worms, Trojan horses, spyware and some adware.

Packet sniffer: Software which enables the operator to observe and watch the content of data transferred trough a network.

Trojan horse: "A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program" [RFC-2828 2000].

Worm: "A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively" [RFC-2828 2000].

Distributed control systems (DCS) are "process control systems where hardware and software components are often provided by a single vendor. These process control systems are commonly deployed in a single manufacturing or production complex, and perform a higher level of internal data processing. DCS generally provide processed information to or a series of commands from a control center" [Shea 2003]. DCS typically are used within a single processing or generating plant or over a small geographic area. "An example might occur within a chemical plant, where a DCS might simultaneously monitor the temperature of a series of reactors and control the rate at which reactants were mixed together, while performing real time process optimisation and reporting the progress of the reaction. An attack targeting DCS might cause extensive damage at a single facility, but would be unlikely to affect more than a single site" [Shea 2003].

Programmable logic controllers (PLCs) are "devices used to automate monitoring and control of industrial plants, and are generally used within a manufacturing facility. They tend to provide little external information, and do the majority of their data processing internally. Programmable logic controllers can control as little as a single machine to as much as an entire manufacturing facility. An automated assembly line can be comprised of a series of PLCs, with each machine on the assembly line performing a distinct job. An attack targeting PLCs might cause significant turmoil at a single location, but the extent of the damage would depend on both the PLC's size and connectivity" [Shea 2003].

Reliability refers to the ability (probability) of satisfactory operation (design function) over the long run (within a given time interval under specified operational conditions) [IEEE 1990]. It denotes the ability to supply adequate (correct) service on a nearly continuous basis, with only a few interruptions over an extended time period.
While reliability denotes the continuity of correct service, availability refers to the readiness of correct service.

Risk[38] refers – in general terms – to the possibility (frequency) of loss, damage or injury and their extent (impact indicators) [EC 2005b]. These variables and associated uncertainties are regarded as being quantifiable. Besides this, there is a non-technical dimension focussing on aspects of societal and psychological risk experience and perception which are subject to changes and contextual in nature.
With regard to critical infrastructures the level of risk depends on the value placed on the asset by its owner / operator and the impact of loss or change (1) to the asset and (2) the likelihood that specific vulnerability will be exploited by a particular threat [EC 2005b].

Risk governance[39] in the context of critical infrastructures includes the totality of players, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken.

38 See also [IRGC 2005].
39 See also [IRGC 2005].

Encompassing the risk-relevant decisions and actions, risk governance is of particular importance in, but not restricted to, situations where instead of a single authority to take a binding decision the nature of the risk requires the collaboration and co-ordination between various stakeholders. Risk governance also calls for the consideration of contextual factors such as institutional arrangements (e.g. the regulatory and legal framework that determines the relationship, roles and responsibilities of the actors and co-ordination mechanisms such as markets, incentives or self-imposed norms) and socio-political culture.

SCADA systems are "primarily software toolkits for building industrial control systems. These systems are often used for remote monitoring and sending commands to valves and switches. For example, they can be found in water utilities and oil pipelines, where they monitor flow rates and pressures. Based on the data that these systems provide, computer programs or operators at a central control centre balance the flow of material using industrial control systems to activate valves and regulators. Generally, SCADA systems process little data internally, instead performing analysis in a more central location, but are the primary conduits for raw data in and commands out of a control centre. They are vulnerable to implantation of faulty data and to remote access through dial-up modems used for maintenance" [Shea 2003].

Security of an infrastructure refers to the degree of risk in its ability to survive imminent disturbances without interruption of customer service. It relates to robustness of the system and, hence, depends on the system operation condition as well as the contingent probability of disturbances [IEEE / CIGRE 2004].

Security of supply: For example, electricity supply is assured when at any time the required service, e.g. amount of electricity of satisfactory quality, is available at an affordable price within the whole network.

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 joint task force of the IEEE / CIGRE, reliability is the overall objective in power system design and operation. To be reliable the system itself must be secure most of the time. To be secure the system must be stable but also be secure against other contingencies that would not be classified as stability problems [IEEE / CIGRE 2004].

Threat: Any event or circumstance that has the potential to adversely impact on an infrastructure, or any element thereof, through accidents, natural hazards, unauthorized access, capacity overloads as well as deliberate attacks (cyber, terrorism), etc. [EC 2005].

Vulnerability: A flaw or weakness (characteristic) in the design, implementation, operation and/or management of an infrastructure or its elements that renders it susceptible to destruction or incapacitation by a threat [EC 2005].

international risk governance council
7-9 Chemin de Balexert, Châtelaine
CH-1219 Geneva, Switzerland
tel +41 (0)22 795 1730
fax +41 (0)22 795 1739
www.irgc.org