Wolfgang Kröger · Enrico Zio

Vulnerable Systems

Springer

Vulnerable Systems

Wolfgang Kröger · Enrico Zio

with contributions of
Markus Schläpfer · Cen Nan · Konstantinos Trantopoulos
Giovanni Sansavini · Miltos Kyriakidis

Vulnerable Systems

Springer

Prof. Dr. Wolfgang Kröger
Mechanical and Process Engineering Department
ETH Zurich
Sonneggstrasse 3
8092 Zurich
Switzerland
e-mail: kroeger@mavt.ethz.ch

Prof. Dr. Enrico Zio
Laboratoire Génie Industriel
Ecole Central Paris and Supelec
Grande Voie des Vignes
92295 Chatenay-Malabry Cedex
France
e-mail: enrico.zio@ecp.fr,
enrico.zio@supelec.fr

Prof. Dr. Enrico Zio
Dipartimento di Energia
Politecnico di Milano
Via Ponzio 34/3
20133 Milano
Italy
e-mail: enrico.zio@polimi.it

Markus Schläpfer
Cen Nan
Konstantinos Trantopoulos
Swiss Federal Institute of Technology
Zürich (ETH)
Switzerland

Giovanni Sansavini
Polytechnic of Milan
Milan
Italy

Miltos Kyriakidis
Imperial College
London
UK

ISBN 978-0-85729-654-2 e-ISBN 978-0-85729-655-9
DOI 10.1007/978-0-85729-655-9
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Cover design: eStudio Calamar, Berlin/Figueres

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The attention on critical infrastructures is evolving from concerns about aging public works (in the 1980s) to redefinition in terms of national security as a result of increased international terrorism (after 11 September 2001) and susceptibility against natural hazards, to unprecedented failure combinations and malicious (cyber) attacks (during mid-2000s). Consequently, the view has broadened from local via national/regional to global while concerns about single failure mechanisms have developed into a full set of potential failures, hazards and threats. As a result, nowadays strategies to reduce and manage vulnerabilities in critical infrastructures and the provision of related analytical instruments have to follow an "all hazards approach".

Societies have always been dependent on services provided by infrastructures, but recently the systems involved have witnessed higher and tighter integration, e.g., by means of pervasive use of modern information and communication technology (ICT), changing operational environments, e.g., market liberalization, and growing mutual dependencies. At the same time the public has become even more dependent on the continuous service infrastructures offer (the Internet and consumption of electricity as a common good may serve as examples). Then today, we cannot allow many such systems to debilitate or collapse, as inconveniences and risks are unacceptable and financial losses are huge, e.g., the 14 August 2003 blackout in North America affected 50 million people and led to 3 billion USD insurance claims.

From the analysis point of view, it is commonly agreed that infrastructures have become more complex and their behavior is hard to understand or predict; research on complex networks has shown that some elements (nodes) evolve to become more important and some structures (topologies) are more susceptible against random failures or targeted attacks than others. Reduction of technological and social vulnerabilities calls for better system understanding and preventive analyses, efforts for which established frameworks and methods seem to be still missing or, if available, are not properly applied.

Infrastructures are of different types and dimensions and show different importance for our society, i.e. different degrees of criticality. This book will focus

on large, geographically-distributed, physical-engineered networks, and particularly on those of undoubted importance for at least highly industrialized countries, such as:

– energy supply (electricity, gas)
– urban freshwater supply and wastewater treatment
– information and communication
– transport (rail, road)
– control systems (SCADA).

Most of these systems are coupled and mutually dependent on different degree and order, difficult to understand and emulate. Very often "the system" consists of a "part being under control" and "the control part" itself, using the same technology as public information and communication systems or even those directly, i.e., the Internet for transport of data and commands. This book will reflect these structural conditions, where appropriate, when elaborating challenges to methods and assessing their quality/suitability.

The aim of the book is of collecting and capturing the state of knowledge in the evolving research field of vulnerability analysis of complex physical-engineered networks, by literature survey focused on "landmark" reports and making use of ongoing authors' work. The targeted audience encompasses students of natural and engineering sciences at MS or PhD level, researchers in the field, non-routine practitioners in industries and agencies as well as executives responsible for critical infrastructure design and protection.

The book is structured according to the course of a fictitious vulnerability analysis. At first the book introduces critical infrastructures in a top-down manner and defines the key terms including the concept of vulnerability followed by elaborations on characteristics of critical infrastructure such as complexity and dimensions of interdependencies, and on challenges to methods. Approaches for vulnerability assessment are categorized and outlined in more general terms before—in the focal chapter—some methods for screening analysis and in-depth analysis are presented in detail. The methods are selected according to their eligibility to meet the challenges posed by the basic characteristics of the types of infrastructures and the objectives of the analysis defined beforehand. Selected methods, e.g. complex network theory, probabilistic techniques, and object-oriented modeling, will be introduced in terms of basic approach, algorithm and measures, and explained by means of illustrative examples; strengths and weaknesses will be assessed separately and finally comparatively. Well-established and well-known methods, e.g., Petri nets, will be mentioned but not explained in detail; reference books will be referred to.

Acknowledgements

The authors wish to express their sincere gratitude to all those who have contributed to this book by participating in basic discussions, contributing to chapters and reviewing drafts, namely Giovanni Sansavini (basic discussions and contributions to Chap. 4, Sect. 6.2, 6.3 and 6.4), Irene Eusgeld (basic discussions, input to Chap. 3), Adrian Gheorghe (review Sect. 6.6), Lucia Roxana Golea (contribution to Sect. 6.3), Arnab Majumdar and Vinh Dang (supervision and review of Sect. 6.7), and Roberta Piccinelli (contribution to Sect. 6.4).

The authors would also like to express their high appreciation to Sabine Keller for typewriting of chapters and, in particular for providing Word files and Patrick Probst for general support and providing few image files.

Contents

Abbreviations

ABM	Agent-based modeling
ALMs	Accelerated lifetime models
ALSP	Aggregate level simulation protocol
ATHEANA	A technique for human error analysis
BNs	Bayesian networks
CARA	Controller action reliability assessment
CCDF	Complementary-cumulative distribution function
CDM	Communication data and management
CFP	Cognitive failure probability
CIs	Critical infrastructures
CREAM	Cognitive reliability and error analysis method
CTMC	Continuous-time Markov chain
DAWG	Data analysis working group
DISD	Distributed interactive simulation
DMSO	U.S. Defense modeling and simulation office
DOE	U.S. Department of energy
EHV	Extra-high voltage
ENTSO-E	European network of transmission system operators for electricity
EPOCHS	Electric power and communication synchronizing simulator
EPS	Electric power system
EPSS	Electric power supply system
ET	Event tree
FLSC	Swedish air force air combat simulation centre
FOM	Federate object model
FSM	Finite state machine
FMEA	Failure modes and effects analysis
FT	Fault tree
GLMs	Generalized linear models
GVW	Geographic valued worth
HAZOP	Hazard and operability

HEART	Human error assessment and reduction technique
HLA	High level architecture
HRA	Human reliability analysis
ICT	Information communication technology
IEEE	Institute of electrical and electronic engineers
IEs	Initiating events
IRRIS	Integrated risk reduction of information-based infrastructure systems
ISS	Interactive simulation systems
LAN	Local area network
LTI	Linear time invariant
MCs	Markov chains
MAUT	Multi-attitude utility theory
MCS	Minimal cut set
MLDs	Master logic diagrams
MPNs	Markov/Petri nets
MTTF	Mean-time-to-failure
NERC	North american electric reliability council
NET	Network event tree
NSF	National science foundation
OMT	Object model template
OPF	Optimal power flow
PHMs	Proportional hazard models
PI	Performance index
PRA	Probabilistic risk assessment
QRA	Quantitative risk assessment
RTI	Run time infrastructure
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SHERPA	Systematic human error reduction and prediction approach
SLIM/MAUD	Success likelihood index method/multi-attribute utility decomposition
SOC	Self-organized criticality
SOM	Simulate object model
SUB	Substation
THERP	Technique for human error rate prediction
TSO	Transmission systems operator
UCTE	Union for the coordination of transmission of electricity
UML	Unified modeling language
WAN	Wide area network

Chapter 1
Introduction and Definition of Key Terms

The welfare and security of each nation rely on the continuous flow of essential goods (such as energy and data) and services (such as banking and health care). A large-scale array of wide area, man-made systems and assets, mostly privately owned or operated, that function collaboratively and synergistically to produce and distribute such a flow, are called infrastructures. Those infrastructures so vital to any country that their incapacity or destruction would have a debilitating impact on the health, safety, security, economics, and social well-being, including the effective functioning of governments[1] are called critical. A failure within one of these infrastructures, or the loss of its continuous service, may be damaging enough to a society and its economy, while that which cascades across boundaries has the potential for multi-infrastructural collapse and unprecedented consequences.

Critical infrastructures (CIs) are various by nature, e.g., physical-engineered, cybernetic or organizational systems, and by environment (geographical, natural) and operational context (political/legal/institutional, economic, etc.).

In principle, a system can be defined as a group of interacting elements (or subsystems) having an internal structure and comprising a unified whole. The boundary of a system is either given or obvious or needs to be defined. Autonomy, coherence, permanence, and organization are essential properties of systems (Dupuy 1985).

Engineered physically networked CIs, often called lifeline systems, is the focus of this book; examples are those providing:

- Energy (electricity, oil, and gas supply)
- Transportation (by rail, road, air, and sea)
- Information and telecommunication (such as the Internet)
- Drinking water, including wastewater treatment

[1] Definition refers to President's Commission on Critical Infrastructure Protection (1997), USA Patriot Act (2001) and European Commission (2004) but was slightly modified by the authors.

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_1,

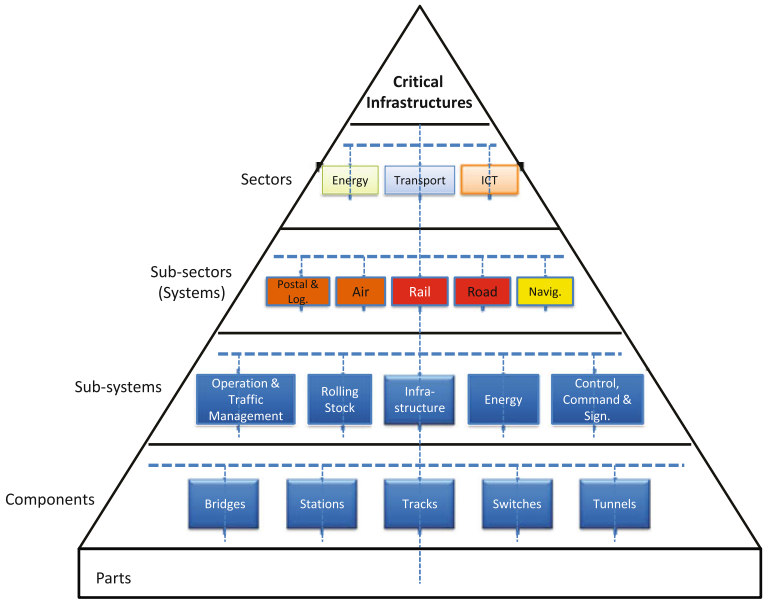

Fig. 1.1 Hierarchical representation of the rail system

The system of CIs can be represented by hierarchical layers which are linked through physical and logical relations (see Fig. 1.1 for the rail transport system).

These CIs are subject to a set of multiple hazards and potentially asymmetrical threats (Table 1.1) disclosing weaknesses and vulnerabilities, respectively; furthermore, they may pose risks themselves during normal operation (e.g., electromagnetic fields—EMF) or accidents (e.g., rupture of gas pipelines). Also, most CIs have a dynamic structure, are undergoing far-reaching changes, both technological and organizational, and incorporating technologies soon after they are (commercially) available.

As shown by experienced events, CIs are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communication technologies, the so-called cyber-based systems (Rinaldi et al. 2001). Identifying, understanding and analyzing these features are still major challenges, magnified by the breadth and complexity[2] of most infrastructures.

According to Rinaldi et al. (2001), *dependency* is defined as a unidirectional relationship between two infrastructures, that is infrastructure i depends on j through the link, but j does not depend on i through the same link, while *interdependency* defines a bidirectional relationship, that is infrastructure i depends on j through some links, and j likewise depends on i through the same and/or other links.

[2] See Chap. 2 for definition.

Table 1.1 Set of multiple hazards and threats disclosing vulnerabilities of CI

Natural events such as earthquakes, hurricanes/typhoons, tornados, severe flooding, landslides or other (increasingly) extreme weather conditions
Accidents or technical factors such as components' failure/rupture leading to the debilitation of plants, networks and operations
Market factors such as instability associated with major producer groups, or economic pressure trading off security factors
Policy factors such as artificial supply limitations or negative pricing outcomes or misusing "energy" for political purposes
Human factors such as unintended failures of omission or commission, e.g., of system operator, intended errors or even targeted malicious attacks, either physical or cyber

Infrastructures are not only complex but most of them show adaptive behavior; that is, all components and the system as a whole are influenced by past experience, e.g., degradation from overuse, aging over time, by trials to improve performance, e.g., of the personnel, and by adjustment to new conditions or disturbances, e.g., automatic variation of generator output to meet actual power loads or load-shedding (Rinaldi et al. 2001).

Infrastructure interdependencies[3] have often been illustrated by a dependency matrix (IRGC 2005; Luiijf 2008) or by representing infrastructure networks as interconnected single planes or layers as shown in Fig. 1.2. In Fig. 1.2, parallel lines represent individual sectors or subjects within a particular infrastructure; solid lines connect nodes and cross-sectors in internal dependencies while dashed lines mark interdependencies. A meaningful representation of such web of dependencies must relate to a specific scenario; here, the flooding event and subsequent response during Hurricane Katarina have been selected.

The *vulnerability* of CIs must be theoretically analyzed and assessed. While the concept of risk is fairly mature and consensually agreed, the *concept of vulnerability* is still evolving and not yet established. In general terms, *risk* refers to a combination of the probability of occurrence (frequency F) of a specific (mostly undesired/adverse) event leading to loss, damage or injury and its extent (consequence indicators c_j)[4]. These quantities and their associated uncertainties are regarded as being numerically quantifiable. Besides this quantitative side of risk, there is a non-technical dimension accounting for the aspects of societal and psychological risk experience and perception which are subject to changes and contextual in nature.[5] For CIs, the term risk may include the frequency of loss of service with its resulting consequences for the people concerned.

[3] See Chap. 2 for further explanation.

[4] See also ISO/IEC Guide 73 (ISO/IEC 2002).

[5] See also German Advisory Council for Global Change (WBGU 1999) and IRGC White Paper 1 (IRGC 2005, p 141) for further details.

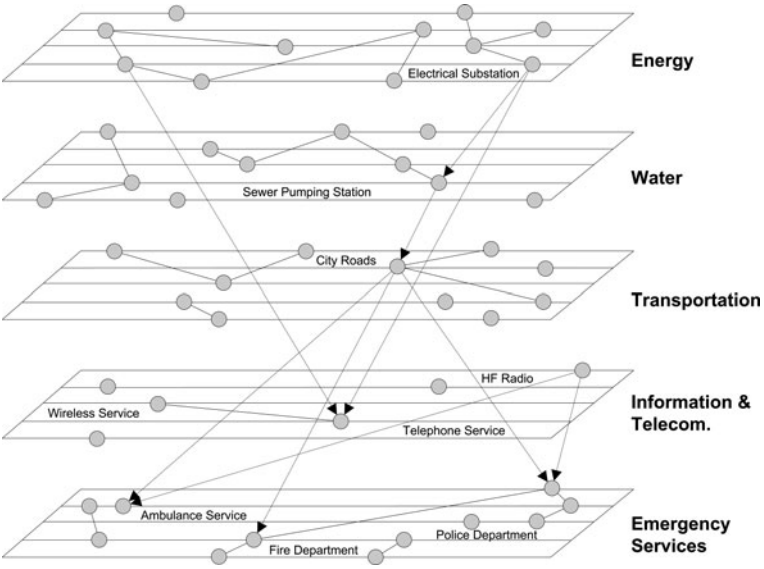

Fig. 1.2 Infrastructure interdependencies, illustrated for the flooding event and subsequent response during Hurricane Katrina, USA (Pederson et al. 2006)

The term *vulnerability* has been introduced as the hazard[6]-centric perception of disasters that is revealed as being too limited to understand in terms of risks. A hazard of low intensity could have severe consequences, while a hazard of high intensity could have negligible consequences: the level of *vulnerability* is making the difference (White 1974).

The *concept of vulnerability* seen as a global system property focuses on three elements[7]:

- Degree of loss and damages due to the impact of a hazard (technical dimension)
- Degree of exposure to the hazards, i.e., likelihood of being exposed to hazards of a certain degree and susceptibility of an element at the risk of suffering loss and damages (the element at risk could be a technical system)
- Degree of resilience,[8] i.e., the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a hazard (technical) or disaster (social).

[6] "A potentially damaging physical event, phenomenon and/or human activity, which may cause loss of life or injury, property damage, social and economic disruption or environmental degradation. Hazards can be single, sequential or combined in their origin and effects" (UN/ISDR 2004).

[7] See Bouchon (2006) for further detailed explanations.

[8] Resilience generally means the ability to recover from some shock, insult, or disturbance, the quality or state of being flexible. In *physics and engineering*, it is defined as the physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit, i.e., as its capacity to absorb energy when it is deformed and then, upon

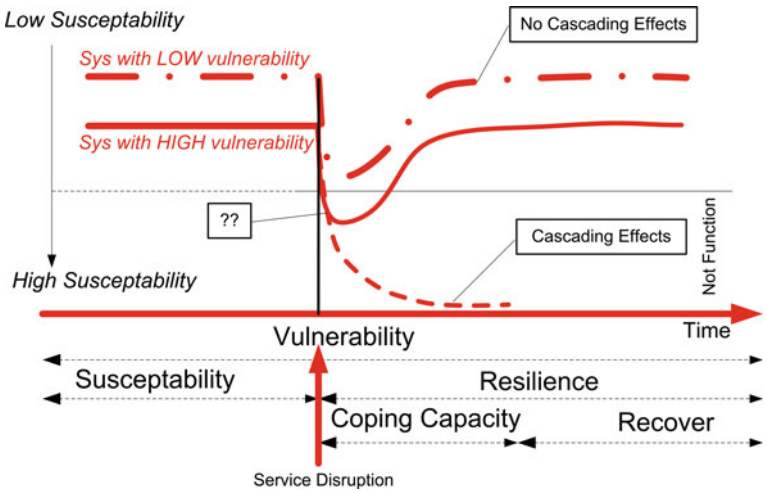

Fig. 1.3 Vulnerability elements and associated response scenarios (Bouchon 2006)

Figure 1.3 brings these elements together with the scenarios which may develop depending on the system characteristics; cascading effects are shown to possibly lead to a complete system breakdown.

In the context of the material presented in this book, we define *vulnerability* as a flaw or weakness (inherent characteristic, including resilience capacity) in the design, implementation, operation, and/or management of an infrastructure system, or its elements, that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume new stable conditions. The latter can be provided with a likelihood (frequency) while a measurand for destruction or incapacitation (loss or damage, respectively) needs specific elaborations depending on the value placed on the asset by its owner/operator or the customer/government. For example, the *vulnerability* of the electric power system might be specified in terms of changes in network characteristics following attacks on nodes and the scale (e.g., number of nodes/lines lost) or the duration of the associated loss. More sophistically, it can be expressed in terms of the frequency of major blackouts (number per year) and the associated severity, measured either in power lost or energy unserved (MW or MWh) as illustrated by Fig. 1.4.

Therefore, this interpretation of *vulnerability* is closely related to the definition of risk while another interpretation is used to describe a system component or an aspect of a system, i.e., a component is said to be a *vulnerability* of a system if its

(Footnote 8 continued)
unloading, to have this energy recovered. Regarding systems resilience basically it is the potential to remain in a particular configuration and to maintain its feedback and functions, and involves the ability of the system to reorganize following disturbance-driven changes (Bouchon 2006).

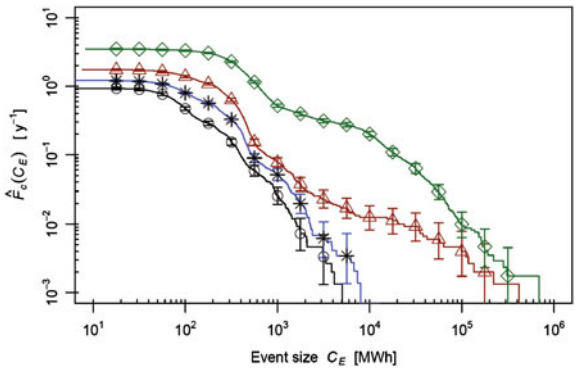

Fig. 1.4 Complementary cumulative blackout frequencies for four different grid load levels L-100% (*circles*), 110% (*stars*), 120% (*triangles*) and 137% (*diamonds*) (Schläpfer et al. 2008)

failure causes large negative consequences to that system (Jönsson et al. 2008). The measure could be a ranking of components a system depends upon.

Reliability of an infrastructure of interest and availability of a service or goods it provides are also attributes useful to subscribe the quality of infrastructure systems. These terms are defined as follows:

- *Reliability* is the ability of a system or component to perform its required functions under stated conditions for a specified period of time (mission without maintenance). Reliability is quantitatively expressed as a probability.
- *Availability* is the probability of a unit to be in working state at a given time t (includes maintenance).

The term "safety" is defined as the absence of a specified damage on users, the public and the environment taking unintentional (random) triggering acts/events, failures or faults into account while "security" includes threats of intentional origin such as sabotage, cyber attacks and terrorism. The traditional security attributes such as availability, confidentiality and integrity are often applied, together with attributes such as privacy and accountability (see also Aven 2007).

Given the realm of single infrastructures and interdependencies, the*goals of vulnerability analysis*, and the associated modeling and simulation efforts, could be:

1. Given a system and the end state of interest, identify the set of events and event sequences that can cause damages and loss effects.
2. Identify the relevant set of "initiating events" and evaluate their cascading impact on a subset of elements, or the system as a whole.
3. Given a system and the end state of interest, identify the set of events or respective event sequences that would cause this effect.
4. Given the set of initiating events and observed outcomes, determine and elaborate on (inter)dependencies (within the system and among systems) and on coupling of different orders.

The ultimate goal is to identify obvious and, most importantly, hidden vulnerabilities in infrastructure systems, to be able to act for managing and reducing

them. The achievement of these goals rely on the analysis of the system, its parts and their interactions within the system; the analysis must account for the environment which the system lives in and operates, and finally for the objectives the system is expected to achieve. During the development of such basic system understanding, first vulnerabilities may have already been emerged.

References

Aven T (2007) A unified framework for risk and vulnerability analysis covering both safety and security. Reliab Eng Syst Safe 92(6):745–754

Bouchon S (2006) The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art (EU report). EU Commission, Joint Research Centre, Ispra, Italy

Dupuy G (1985) Systèmes, réseaux et territoires. Presse de L'Ecole nationale des Ponts et Chaussées, Paris

European Commission (2004) Critical infrastructure protection in the fight against terrorism, COM (2004) 702 final. Bruxelles, 20 October 2004

IRGC (2005) Risk governance: towards an integrative approach. White Paper No. 1, written by O Renn with an annex by P Graham. Geneva

ISO/IEC (2002) ISO/IEC Guide 73: risk management: vocabulary: guidelines for use in standards. ISO Technical Management Board Working Group 2

Pederson P, Dudenhoeffer D, Hartley S, Permann M (2006) Critical infrastructure interdependency modeling: a survey of U.S. and international research. Technical report INL/EXT-06-11464. Idaho National Laboratory, Idaho, USA

President's Commission on Critical Infrastructure Protection (1997) Critical foundations: protecting America's infrastructures. The report of the President's Commission on Critical Infrastructure Protection, Washington, DC

Rinaldi SM, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Contr Syst Mag 21(6):11–25

Schläpfer M, Kessler T, Kröger W (2008) Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. In: Proceedings of the 16th power systems computation conference, Glasgow, 14–18 July 2008

UN/ISDR (2004) Terminology: basic terms of disaster risk reduction: glossary. UN/ISDR, New York, USA

USA Patriot Act (2001) Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001. H.R. 3162, in the Senate of the United States

White GF (1974) Natural hazards: local, national and global. Oxford University Press, New York p 288

Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen (1999) Welt im Wandel: strategien zur Bewältigung Globaler Umweltrisiken/WBGU. Springer, Berlin, Heidelberg

Chapter 2
Properties of Critical Infrastructures

Physical-engineered critical infrastructures (CIs) are characterized as large scale, spatially distributed, complex networks—either open or closed. According to Dueñas-Osorio and Vemuru (2009), these systems are made of "a large number of interacting components (real or virtual), show emergent properties difficult to anticipate from the knowledge of single components, are characterized by a large degree of adaptability to absorb random disruptions and are highly vulnerable to widespread failure under adverse conditions." Indeed, small perturbations can trigger cascades and large-scale consequences in CIs; furthermore, disruptions may also be caused by targeted malicious attacks.

2.1 Complexity

A recent National Science Foundation (NSF) workshop report (Guckenheimer and Ottino 2008) points at the fact that a complex system is characterized by an internal structure which may consist, besides many interacting components, of "a network that describes which components of the system interact, multiple scales of space and/or time, or symmetry. The components of many complex systems are heterogeneous and form a hierarchy of subsystems." Furthermore, uncertainty is regarded as pervasive in complex systems, and its characterization and propagation through the system as key aspects for the reliable prediction of the system behavior and its effect and safe control.

The above attributes draw the boundary between simple and complex systems. Less trivial is to draw a boundary between complicated and complex systems. Table 2.1 attempts to do so by highlighting the very essence of a complex system, which is believed to lie in the degree and modality the parts interact and the overall behavior of the system that emerges from these. "The system must be analyzed as a whole; decomposing the system and analyzing subsystems does not necessarily give a clue as to the behavior of the whole" (Guckenheimer and Ottino 2008).

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_2,

Table 2.1 Characteristics of complicated versus complex systems, both entailing a large number of highly connected components

Complicated systems (mechanical watches, aircraft, power plants, etc.)	Complex systems (stock market, www, power grid, etc.)
Components have well-defined roles and are governed by prescribed interactions	Rules of interaction between the components may change over time and may not be well understood
Structure remains stable over the time. Low dynamics	Connectivity of the components may be quite plastic and roles may be fluid. Interactions are not always obvious
No adaptation. One key defect may bring system to a halt	System responds to external conditions and evolves
Limited range of responses to changes in their environment	Display organization without a central organizing principle (self-organization/ emergence)
Decomposing the system and analyzing sub-parts can give us an understanding of the behavior of the whole, i.e., the whole can be reassembled from its parts	Respond to and interact with their environment
Problems can be solved through analytical thinking and diligence work	Inadequate information about the state of the influencing variables, nonlinearities
	Overall behavior cannot be simplified in terms of their building blocks. The whole is much more than the sum of its parts

2.2 Learning from Experience

Despite Cassandra, CIs have proved highly reliable in and beneficial for Western societies. Nevertheless major breakdowns have occurred, illustrating the complexity of system behavior and of the event sequences which may generate, and showing the negative consequences of dependencies leading to cascading effects.

In the electrical transmission CIs, for example, the analysis of recent major blackouts from 2003 to 2006 (Table 2.2) leads to drawing some conclusions on the main underlying causes and to carving some patterns of common behavior:

- Technical failures (Denmark/Sweden, two independent failures), external impacts (Tokyo, construction work; Brazil, extreme weather conditions) and adverse behavior of protective devices (London) are important triggering events, when not protected by the N-1 security criterion[1] and/or in combination with high-load conditions (Moscow).

[1] Definition of 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." (Union for the Coordination of Transmission of Electricity 2008).

Table 2.2 Recent major blackouts of electric power supply systems

Blackout		Load loss (GW)	Duration (h)	People affected	Main causes
Aug 14, 2003	Great Lakes, NYC	~60	~16	50 million	Inadequate right-of-way maintenance, EMS failure, poor coordination among neighboring TSOs
Aug 28, 2003	London	0.72	1	500,000	Incorrect line protection device setting
Sept 23, 2003	Denmark/Sweden	6.4	~7	4.2 million	Two independent component failures (not covered by N-1 rule)
Sept 28, 2003	Italy	~30	up to 18	56 million	High load flow CH-I, line flashovers, poor coordination among neighboring TSOs
July 12, 2004	Athens	~9	~3	5 million	Voltage collapse
May 25, 2005	Moscow	2.5	~4	4 million	Transformer fire, high demand leading to overload conditions
June 22, 2005	Switzerland (railway supply)	0.2	~3	200,000 passengers	Non-fulfillment of the N-1 rule, wrong documentation of line protection settings, inadequate alarm processing
Aug 14, 2006	Tokyo	?	−5	0.8 million households	Damage of a main line due to construction work
Nov 4, 2006	Western Europe ("controlled" line cut off)	~14	~2	15 million households	High load flow D-NL, violation of the N-1 rule, poor inter TSO–coordination
Nov 10, 2009	Brazil, Paraguay	~14	~4	60 million	Short circuit on key power line due to bad weather, Itaipu hydro plant (18 GW) shut down

- Organizational factors such as market liberalization and short-term contracting causing operation of the system beyond original design parameters (e.g., Great Lakes, Italy), and stressing operation conditions such as weakening maintenance work and/or inadequate integration of intermittent power generation (e.g., Western Europe) have proven to be outstanding causes.
- As the transmission system operators (TSOs) play a decisive role with regard to contingency management, lack of situational awareness and short-term preparedness, as well as limited real-time monitoring beyond control areas and poorly timed cross-border coordination (e.g., Great Lakes, Italy, Switzerland (rail)) build up as aggravating factors.
- The inadequacy of the N-1 security criterion and, even more importantly, of its inadequate evaluation/implementation in various cases have enforced attempts to make it more stringent and legally binding.