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,

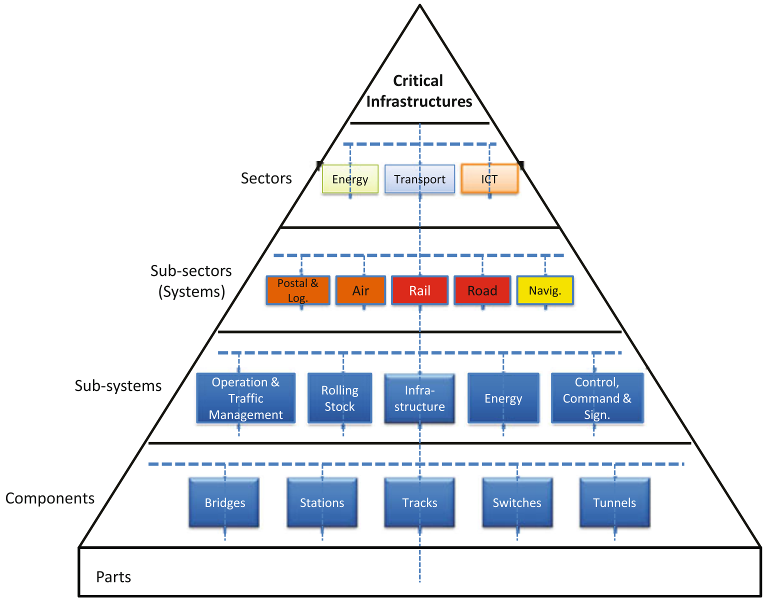

Fig. 1.1 Hierarchical representation of the rail system

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.

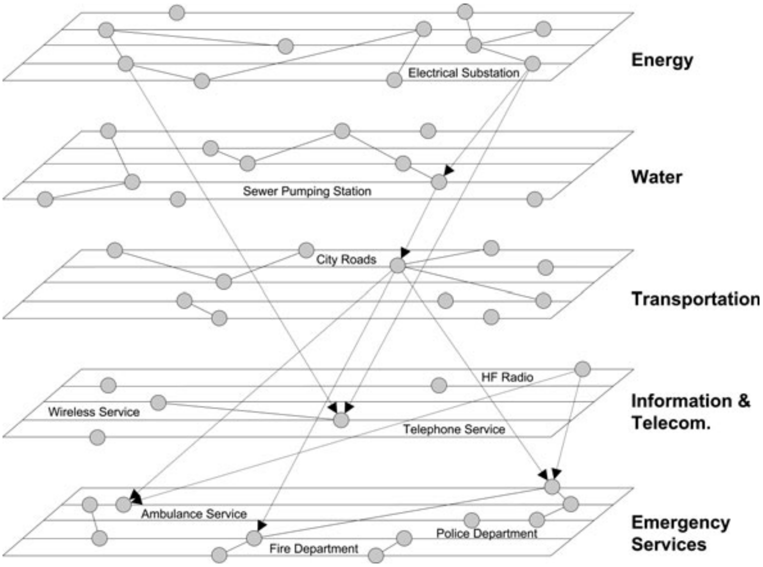

Fig. 1.2 Infrastructure interdependencies, illustrated for the flooding event and subsequent response during Hurricane Katrina, USA (Pederson et al. 2006)

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

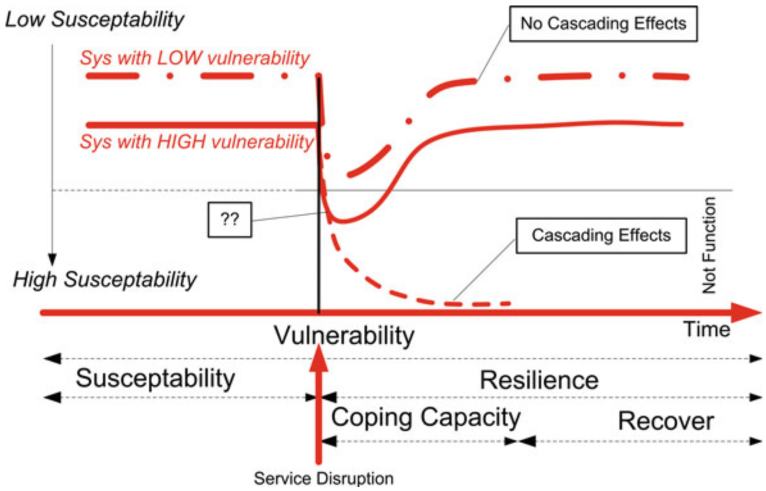

Fig. 1.3 Vulnerability elements and associated response scenarios (Bouchon 2006)

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).

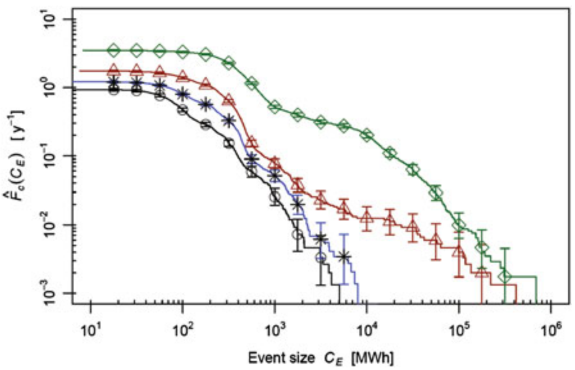

Fig. 1.4 Complementary cumulative blackout frequencies for four different grid load levels L-100% (*circles*), 110% (*stars*), 120% (*triangles*) and 137% (*diamonds*) (Schläpfer et al. 2008)

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