Chapter 3
Challenges to Methods for the Vulnerability Analysis of Critical Infrastructures

As has been discussed in the previous section (see Table 2.1) critical infrastructures (CIs) exhibit a number of complex system characteristics which call for analyzing them as a whole and make their holistic study highly challenging. A comprehensive vulnerability analysis requires not only the consideration of a large number of spatially distributed, interacting elements with nonlinear behavior and feedback loops, but also a broad spectrum of hazards and threats including failures and threats. It comprises three main activities (Fig. 3.1):

- System analysis including system properties (e.g., physical and logical structures and operation modes)
- Quantification of system vulnerability indicators and identification of important elements
- Application to system improvements either technical or organizational

The challenges to methods for vulnerability analysis depend on the objectives of the assessment and on the system characteristics. More specifically, the following main challenges are to be tackled, while a look at how different methods basically respond to them is given in Chap. 4.

3.1 Emergent Behavior

The local interaction of a plethora of system components often results in global behavior, which is difficult or even counterintuitive to anticipate. In general, such hard-to-predict collective phenomena are referred to as "emergent behavior" (e.g., Bonabeau 2002). As a consequence, vulnerability analysis methods have to be developed and applied in such a way that emergent phenomena, potentially crucial for the overall robustness of critical infrastructures, are sufficiently captured.

According to Wolf and Holvoet (2005), the emergence properties include micro–macro effect, radical novelty, coherence, dynamics, interacting parts,

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_3,

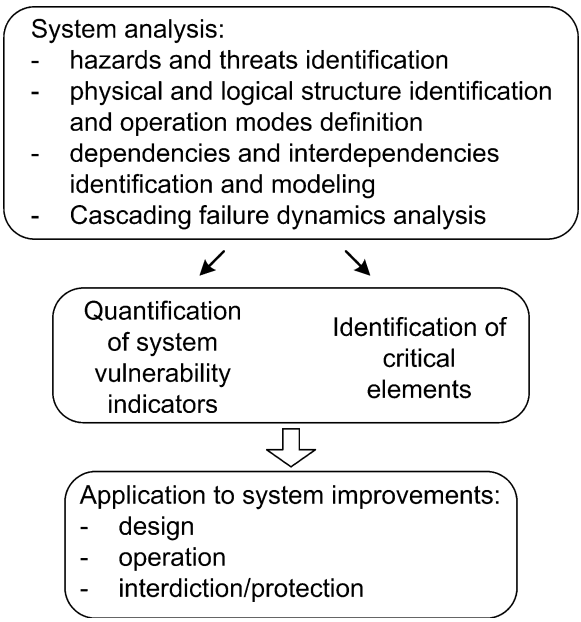

Fig. 3.1 Conceptualization of CI vulnerability assessment

decentralized control, two-way link and flexibility. For an individual infrastructure, the definition of the micro-level (lowest level of the modeling) depends on the level of detail, which has to be chosen carefully. Furthermore, a careful decision needs to be made with regard to the trade-off between two extreme viewpoints: so called non-reductionism, which means that the macro-level emergence is not reducible to the micro-level parts of the system, and the opposite opinion that emergent properties can be studied by taking a system apart and looking at the parts (so-called reductionism) and that the behavior of the system can be reduced to that of its elements (Kubik 2002).

3.2 Intricate Rules of Interaction

The required performance of critical infrastructures relies on intricate, often nonlinear interactions among a large number of interconnected and geographically distributed components of different types, including both technical and non-technical elements. Even their interaction with the regulatory, legal or institutional framework may eventually affect the overall vulnerability of infrastructure systems. Furthermore, the normal operation of these systems does not allow to detect 'hidden' interactions which might become crucial for the evolution of (cascading) failure events; the dynamic degradation of networks is sensitive to parameter variations and the system behavior cannot be described by linear equations.

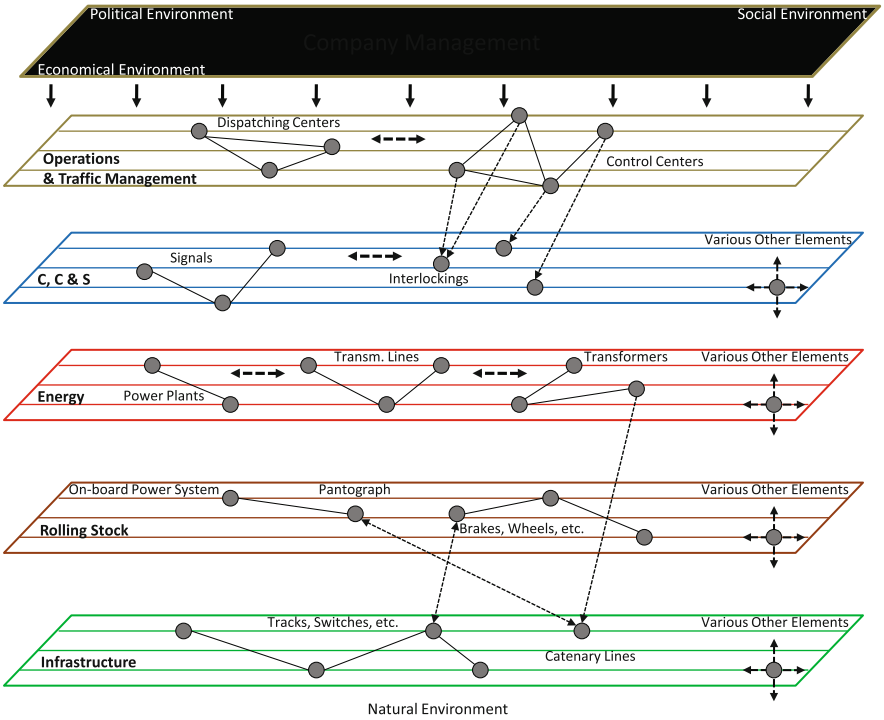

Fig. 3.2 Illustration of railway system as a multi-layer infrastructure network

Most CI are open systems, i.e., they exchange with the environment very intensively. Each CI needs input in terms of energy, resources, information, etc.; the services provided are the system outputs. The interactions between the system and its environment have to be taken into account carefully and the undergoing exchanges to be established adequately via interfaces.

3.3 Single System Features and "Systems-of-Systems"

3.3.1 Multi-Layered Systems

Single critical infrastructures can be viewed as large-scale systems built up from various co-existing techno-socio-economic layers. For instance, transportation systems or electric power supply infrastructures consist of physical networks, communication and control layers, among others, all embedded within a market-driven organizational framework. Figure 3.2 shows one way of illustrating the different layers making up the overall railway system (see also Fig. 1.2 for further explanations).

Tackling the system fragility induced by these layered (inter)dependencies, even when only within one CI, remains one of the main challenges of today's modeling and simulation capabilities.

3.3.2 State Changes

Modeling and simulation of dynamical processes emulate changes of the system/components states over time which can be either discrete or continuous (Borshchev et al., 2002):

1. *Discrete processes:* State variables change "jumping" from one value to another. Typical examples are break-down failures, factory operations or shipping facilities, in which the material or information being simulated can be described as moving in discrete steps or packets, etc.
2. *Continuous processes:* State variables are changing continuously, rather than in discrete steps or packets. Typical examples of continuous dynamic behavior are wear-out processes, water movement through reservoirs and pipes, etc.

Besides the typical discrete systems (clocked transport systems, telecommunication) and continuous systems (electric power supply, gas and water supply) there are so called hybrid systems, e.g., *continuous systems controlled by discrete events,* which include time-dependent changes and jumping events. An example is the continuous electricity supply provided by the electric power system affected by a shutdown event initiated by the SCADA-system in the case of line overload.

In the case of discrete state changes, models must treat entities (e.g., units of traffic), resources (elements that service entities), and control elements (elements that determine the states of the entities and resources). In the case of continuous processes, the model has to include differential or integral equations that describe the evolution of the system. For hybrid systems, a separation of the underlying discrete and continuous processes into two different layers is typically required.

When modeling these changes we have also to be aware of multiple time scales. For example, within the electric power transmission system switching-over voltages happen within microseconds whereas, e.g., some maintenance actions may be scheduled once a year and take hours to days.

3.3.3 Evolving Systems

Modern societies have become embedded in an increasingly dense web of interconnected infrastructures which are subject to a continuous and fairly rapid evolution over time characterized by, for instance, geographic expansions, integration of new technologies, coexistence of old and new technologies or changing market conditions. This evolution at different time and spatial scales brings about

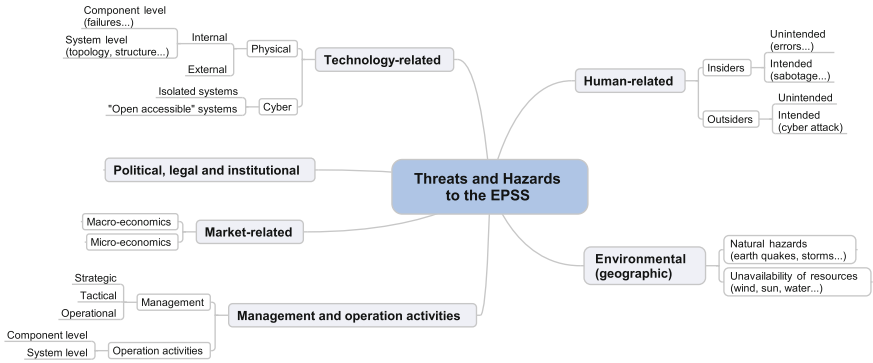

Fig. 3.3 Spectrum of multiple hazards and threats to CI (Kröger 2008)

the need to continuously adapt and update vulnerability assessments. Such a process, however, might become a prohibitive task.

3.3.4 "System-of-Systems"

Modern infrastructure networks are strongly coupled to each other by different types of (inter)dependencies (see Sect. 2.3) of different degrees. Therefore, they should preferably be modeled as interconnected "system-of-systems".[1] A fundamental property of interdependent networks is that failures within one network may cascade through dependent nodes in other networks (Buldyrev 2010). Powerful methods are needed to describe the behavior of such a system as a whole (not as a sum of single systems).

3.4 Broad Spectrum of Hazards and Threats

In principle, the model of interconnected or single CI must consider all relevant hazards and threats. The risks or vulnerabilities related to critical infrastructures often refer to being *systemic* by nature. "Investigating systemic risks or vulnerabilities goes beyond the usual agent-consequence analysis and focuses on interdependencies and spill-over risk clusters" (IRGC 2005). Hence, approaches are required to capture this holistic view.

[1] No universally accepted definition of the term exists; we focus on the following one (DeLaurentis 2007): "A system-of-systems consists of multiple, heterogeneous, operationally distributed, occasionally independently operating systems embedded in networks at multiple levels that evolve over time.

Depending on the goal of the analysis a decision has to be taken about the spectrum of hazards and threats to be included which can be of many-sided nature, either technology- or human-related, natural and operational as well as contextual (see Fig. 3.3 for illustration).

Technology-related hazards and threats include physical failures at component and system level as well as cyber-induced problems depending on the openness of the system. Challenges are to distil the most important technology-related hazards and threats and related failure modes, and to model their occurrence and the potential consequences adequately.

The spectrum of *human-related* threats ranges from unintended errors, e.g., of operators (a) of not-performing the required task ("errors of omission") or (b) doing something else instead ("errors of commission") to (c) intended "errors" (sabotage) made by insiders or outsiders to (d) targeted malicious attacks, either physical (e.g., explosive devices) or cyber. While challenges resulting from (a) are well known and call for models to deal with human reliability, (b) to (d) call for even more sophisticated models capable of describing a complex human behavior under abnormal conditions, together with systems response models to predict a potential damage to the system analyzed.

The wide-area, large-scale nature of critical infrastructures makes them highly susceptible to *natural* hazards, such as earthquakes, flooding, extreme weather conditions including heat, cold, storms, etc. Special models are necessary to quantify hazards (e.g., seismic hazard curves) and to capture the impact on exposed systems. Other environmental hazards relate to, e.g., geographic proximity of various components and systems, challenging models to deal with interdependencies and cascading effects.

Inadequate *management and operational* activities can threaten infrastructures, in particular errors in instructions and norms can lead to service interruptions or even cause the complete failure of a system; it is a non-trivial task to find out such weaknesses in the documentation and integrate them into the dynamic model of a system.

Further hazards and threats relate to factors which are often called *contextual* such as market-related as well as political, legal or institutional. There is evidence that liberalization of the market and associated political decisions have cut off reliability factors such as reserves and redundancies and slowed down investments while integration of the systems has been further increased (IRGC 2005). Therefore, contextual factors clearly affect system vulnerability in complex ways. They add challenges to system modeling and analysis (simulation). There is a clear need to take increased economic pressure into account when assessing human response behavior, to modify maintenance strategies and spare-parts managing, to focus on the search for entry points for hacker attacks after the industrial control systems have become more open and less dedicated, etc.

The consideration of a broad spectrum of hazards and threats, often called "all hazards approach", including failures and failure combinations of highly reliable elements, and the occurrence of rare natural hazardous events may cause specific modeling difficulties. The simulation of such events, of low probability of

occurrence, brings issues related to the time frame of the analysis and to the number of simulation runs needed to observe the effects of a statistically significant number of rare events (very low by nature).

References

Bonabeau E (2002) Predicting the unpredictable. Harvard Bus Rev 80(3):5–11

Borshchev A, Karpov Y, Kharitonov V (2002) Distributed simulation of hybrid systems with AnyLogic and HLA. Future Gener Comp Sy 18(6):829–839

Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464:1025–1028

DeLaurentis D (2007) Role of humans in complexity of a system-of-systems. In: Duffy VG (ed) Digital human modeling, LNCS 4561. Springer-Verlag, Berlin, Heidelberg, pp 363–371

IRGC (2005) Risk governance: towards an integrative approach. White Paper No. 1, IRGC, Geneva

Kröger W (2008) Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. Reliab Eng Syst Safe 93:1781–1787

Kubik A (2002) Towards a formalization of emergence. Artif Life 9(1):41–65

Wolf TD, Holvoet T (2005) Emergence versus self-organization: different concepts but promising when combined. In: Proceedings of the second international workshop on engineering self-organizing applications (July 2004), Springer-Verlag, Berlin, Heidelberg, pp. 96–110