Chapter 7
Concluding Considerations

In this book, the subject of vulnerable systems has been addressed in depth. The focus has been on engineered physical critical infrastructures (CIs) such as the networks for energy supply, transportation, information and telecommunication. These are large-scale arrays of systems and assets that function systematically to produce and distribute services vital for modern economy and social welfare.

One main motif underlying the viewpoints presented in the book is that of the complexity of these systems and the related emergent behaviors which may arise in collective ways, difficult to predict from the superposition of the behavior of the individual elements of the system. This complex, emergent behavior has been demonstrated by system breakdowns often triggered by small perturbations followed by accelerating cascades and large-scale, border-crossing consequences, stressing the importance of (inter)dependencies (see Table 2.4 for details). As a conclusion, the analysis of these systems cannot be carried out with classical analytical methods of system decomposition and logic analysis; a framework of analysis is needed to integrate a number of methods capable of viewing the problem from different perspectives (topological and functional, static and dynamic, etc.).

Another relevant complexity attribute that has been stressed throughout relates to the increased integration of CIs, e.g., driven by the pervasive use of computer-based communication and control systems, which is beneficial in many respects but on the other hand it introduces additional vulnerabilities due to the increased (inter)dependence which can lead to surprising behaviors in response to perturbations. The electric power supply system, for instance, is undergoing a design re-conceptualization to allow for the integration of large shares of electricity produced by harvesting solar and wind energies at the most suitable sites (e.g., desert solar and offshore wind farms). The grids will become "smarter" by decentralized generation, smart metering, new devices for increased controllability, etc., which will "convert the existing power grid from a static infrastructure to be operated as designed into a flexible, adaptive infrastructure operated proactively" (IEC 10). These types of developments can be expected to be shared

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_7,

among CIs, but the final states and related challenges may be different. For instance, the extended use of traffic control systems may increase the complexity of our road transport systems at a first glance, but may in the end turn them into less dynamic systems upon transferring important influencing factors such as speed, distance keeping, performance, etc., from individual drivers to computer-based systems.

Another important aspect that has underpinned a number of considerations in this book, relates to the fact that the types of CIs considered are subject to a broader spectrum of hazards and threats, including malicious attacks; this has led to the conclusion that an all-hazards approach is required for the understanding of the failure behavior of such systems, for their consequent protection.

The above considerations have led to the structuring of the analysis of vulnerable CI systems in the book into five levels:

- The *problem definition level*, at which the concepts of CI and vulnerability have been unambiguously introduced, together with and in reference to other key terms.
- The *issues level*, at which the peculiar characteristic features of such intra- and inter-connected systems have been described, the related challenges with respect to their analysis have been identified and the methods have been critically addressed.
- The *approaches level*, at which approaches to meeting the challenges have been discussed.
- The *methods level*, at which the methods currently under consideration for the analysis of vulnerable CIs have been illustrated to a level of detail sufficient for their implementation and use, and with a careful analysis of their respective strengths, limitations, and degrees of maturity for practical application.
- The *framework level*, at which an integrated view of the procedure for vulnerability analysis has been offered, coherent with the relevant aspects and features of intra- and inter-dependent CI systems highlighted above.

As unidirectional and bidirectional relationships within and among CIs are expected to continue standing as a real-world issue and representing a major challenge for analysis methods, the evaluation of the vulnerability of CIs becomes central for their future efficient and safe development and operation. As a contribution to this, the present book introduces an operational definition of vulnerability in terms of weaknesses that render the CI susceptible to destruction or incapacitation when exposed to a set of hazards or threats (see Fig. 1.3).

Furthermore, in practice CIs are considered critical with regard to some criteria, possibly varying from country to country and from one perspective to another, e.g., corporate, societal, system or user's view. In the book, an attempt has been made to distinguish the degrees of criticality, because this is considered to help guiding the vulnerability analysis.

Turning the attention to vulnerability analysis, the book embraces the classical characterization of CIs as systems made of a large number of elements interacting in different complex ways which make system behaviors emerge (sometimes in

unexpected ways). The differentiation from complicated systems is clearly pointed out (see also Table 2.1), together with the resulting fact that decomposition may not help in identifying and analyzing the (emergent) system behaviors, so that the CI system itself must be looked at as a whole with all its intra- and inter-dependencies.

In the book, the procedure of vulnerability analysis offered comprises three tasks (on top of the analysis of the system structure, properties and (all) hazards): the quantification of vulnerability indicators, the identification of critical elements and the application of the analysis results for system improvements (see Fig. 3.1). Correspondingly, the challenges to the methods used within the vulnerability analysis procedure depend on the specific objectives of the analysis and on the system characteristics; a common challenge comes from the large number of parameters needed to characterize the model of the system and the paucity of reliable data in support. Other specific challenges come from the need to capture the emergent behaviors and intricate rules of interaction, various system features like multi-layering, state changes, adaptation to new developments, "system-of-systems" characteristics, the susceptibility to a broad spectrum of hazards and threats (see Fig. 3.3). All these features need to be tackled by the methods for vulnerability assessment. A number of these have been compiled, characterized, and critically evaluated against the assessment steps, the desired outputs and practical objectives (Table 4.1). Methods of statistical analysis, probabilistic modeling techniques (e.g., Bayesian networks), and tabular methods for hazard studies and risk analysis (HAZOP, FMEA, pure expert judgment) used in isolation have been concluded to show limited chances of success against the challenges posed; on the contrary, integration of elements of probabilistic risk assessment (e.g., adapted logic trees), complex network theory and agent-based modeling and simulation techniques, including high-level architecture (HLA), appear most promising.

In the end, it is concluded that a universal, all encompassing modeling approach capable of addressing by itself the assessment of vulnerable systems does not exist. Rather, a conceptual framework is proposed (Fig. 5.1) to systematically tackle the problem in a step-wise and integrated fashion which stands on a preparatory phase, a screening analysis and an in-depth analysis of major critical areas of the system. Integration is intended to refer also to the multitude of perspectives of the different "players" (users/operators) involved, their different logics, and even potential confidentiality issues.

The book points at methods of network theory, probabilistic risk analysis, cascading failure dynamics for the screening analysis, which although performed at a relatively high level of abstraction is capable of providing generic insights into the topology and phenomena involved which can serve as guidance for the successive in-depth vulnerability analysis phase. For this latter more detailed phase, the combination of agent-based modeling with Monte Carlo simulation techniques and, where appropriate, with physical models (e.g., for mass or power flows) has been pointed at in the book as the most promising approach.

For (inter)dependency analysis HLA standard might be attractive as the modeling of the interconnected systems in a super-model with adequate granularity

might be impossible due to further exacerbated computer time/resources issues and overall model complexities.

In the book, the above mentioned methods of screening and in-depth analysis have been illustrated by a detailed description of their functioning and evaluated as to how/to what extent they succeed in the analysis of vulnerable systems and in meeting the related challenges, and to how mature they are for practical application. The considerations that have merged in the book (see Table 7.1) show in general terms differing levels of capabilities; some of the methods have been developed in other fields of technical risk assessment, e.g., PRA for nuclear power plants, or other sectors, e.g., network theory and agent-based modeling in social systems, and applied/adapted to the vulnerability assessment of engineered CIs. The results gained and the way to illustrate them also differ (e.g., metrics of robustness of network topology, curves depicting frequency, and size of potential blackouts) and are, therefore, differently qualified as input for decision making. Although some of the concepts and results have been proved against statistical data (e.g., statistical data on blackouts) and benchmarked against other methods, the analysis provided in the book shows that there is still general lack of validation, there are still contradictions between (limited) empirical investigations and theoretical analysis.

It is worth mentioning that the specific advantages and limitations of a framework of analysis laying over two levels of system abstraction (high-level for screening and detailed for in-depth analysis) eventually lay the groundwork for their specific and separate application to particular areas as well as for their interplay within a comprehensive analysis of CI networks. Highly detailed modeling approaches with close adherence to reality may also serve for quantifying the reliability of a specific system under given operational conditions. In complementation, minimal, highly abstract models allow for a qualitative identification of basic underlying mechanisms and generic key factors, which are not restricted to specific systems. Such insights may again serve as valuable clues on where to put the focus with highly detailed modeling approaches. On the other way around, quantitative results from specific systems may also be checked with regard to their generality by using minimal models.

Finally, uncertainty analysis is much needed for inclusion into the picture, although still rarely an element of an overall vulnerability assessment; in this respect, computational tools for uncertainty propagation and sensitivity analysis in large scale applications, with reasonable computing times are missing. The same holds for the need of including the interactions and influences of the human operators, a cross-cutting issue into vulnerability analysis which has been addressed in other than CI sectors, mainly in the framework of PRA for nuclear power plants, but is now starting to arise also in the field of vulnerable CIs analysis.

In conclusion, the writing of the book has served the authors to build the confirmation that there is still a gap between the ability to design and operate complex networked CI systems and the ability to understand, model and simulate them for identifying and reducing vulnerabilities. In this view, intensive research, development and application work must be continued and many other books can be expected in future.

Table 7.1 Summary of the various methods for the vulnerability analysis of CIs

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
Complex network theory	Mainly for capturing topological features of the networked CI; addition of "weights" can account for physical attributes of the CI components, to a certain extent	Simple and fast analysis, which provides quantitative indicators of the topological characteristics of the network of connections underpinning a CI. Allows to identify topologically-critical areas of the system	If used in isolation, it can provide only indications on the topology of the system, potentially failing to represent the other features related to the flow-driving characteristics	In the weighted scheme of analysis, the possibility of accounting for uncertainties on the weighting parameters seems straightforward and it does not pose particular computational challenges given that the evaluation of the underlying (topological) model is very fast	A number of validation proofs have been offered with regard to the topological characterization of real networked infrastructures	Very limited efforts have been made in providing user friendly tools to carry out complex network analyses	The results are typically synthesized in distributions and point-value metrics which summarize topological features of the network connection Web

(continued)

Table 7.1 (continued)

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
Risk analysis	Mainly for parts of a CI. Extended application to an entire CI would typically require excessive resources	Allows a systematic and logic analysis of vulnerability scenarios which may affect a CI, while at the same time allowing for their quantification of likelihood of occurrence and consequence, and for the identification of the critical CI components	The efforts in logic modeling and quantification are significant. The capability of providing an exhaustive analysis is limited, particularly in view of the unexpected emergent behaviors and of the many (inter) dependencies	The quantification part of the analysis is typically based on probabilistic modeling, which is naturally suited for uncertainty analysis. The computational burden depends on the extent of the modeling upon which uncertainty analysis is to be mounted, with its additional computational burden	Validation of such analyses is quite difficult to obtain. Quality assurance is needed in support, but this is far from trivial	A number of tools have been developed, but not specific for CI vulnerability analysis. Adaptation would be needed, whose effort and degree of success is difficult to foresee	Results are provided in terms of logic scenario trees, risk matrices and distributions. These are quite familiar representations for risk analysts

(continued)

Table 7.1 (continued)

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
Probabilistic modeling of cascades dynamics	Allows superposing the cascade dynamic process onto the topology of the system, within a relatively high-level of abstraction. In this sense, it is suitable for comple-menting the topological analysis with dynamic features representative of the cascade phenomena which may occur	The high-level of abstraction leads to a modeling which is still sufficiently slim to allow running what-if scenarios at reasonable computational expenses. The results of this add to the topological analysis by confirming or not certain network connectivity characteristics and critical points, in light of also the dynamic patterns of cascade evolution	Although dynamics is added to complement the topological analysis, it may still fail to capture physical aspects of the cascade dynamics related to the flow-driven processes actually occurring	Uncertainties on the development of the cascade scenarios can be added in a quite straightforward manner, with no particular additional burden of computations	A number of validation tests have been presented with regard to the capability of modeling the main characteristics of real cascading processes, e.g., electrical blackouts	Very limited efforts have been made to provide user-friendly tools	Results are usually provided in terms of network connectivity characteristics and cascade sizes, as a function of key system parameters. From these, phase transitions are sought which testify the emergence of new behaviors and allow dimensioning protections and preventions with respect to the escalation of uncontrolled cascades

(continued)

Table 7.1 (continued)

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
Agent-based modeling	Allows simulation of complex systems, comprising a large number of heterogeneous components interacting with each other	Close adherence to reality; capable to capture highly non-linear dynamics and emergent phenomena; integration of non-technical system elements	Usually requires a large number of model parameters and may imply long computational times	The level of modeling details allows to quantify a multitude of time-dependent reliability and vulnerability aspects, and thus potentially provides essential insights into the diverse sources of uncertainties	While it has been widely validated in fields like social sciences, it still lacks comprehensive feasibility studies in the field of CIs	A number of user friendly tools are available	Due to its high flexibility, it offers a broad range of quantitative result representations. Examples include disruption times or "frequency–consequence (F–C)" diagrams

(continued)

Table 7.1 (continued)

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
High-level architecture	A simulation standard mainly for representing multiple interacting systems such as CIs in one simulation tool, which is not suitable to all simulation developments. A "pre-investigation" is recommended before adopting this standard	As a promising approach for integrating different modeling methods, the distribution of simulation components improves the flexibility/reusability of the simulation tool and decreases its overall complexity	It is not a "plug-and-play" standard. Resources and time required to implement an HLA-compliant simulation tool could be significant	Synchronization issues between distributed simulation components, which means that one component could process events forwarded by other components in non-increasing time stamp order, can account for uncertainties on overall simulation	Validation of such approach is difficult. Extra validation experiments need to be developed and conducted, which should include the validation experiments regarding the decomposition of simulation components	Several commercial and free ready-to-use software tools have been developed and are available to users who try to adopt HLA standard	Results are usually representations of the integration of model outputs from each distributed simulation components and corresponding systematic analyses

(continued)

Table 7.1 (continued)

Technique	Capabilities			Accountancy of uncertainties	Maturity for practical applications		
	Suitability	Advantage	Disadvantage		Degree of validation[a]	User friendly tools	Presentation of results
Human reliability and performance modeling	Methods are used to assess human performance during the execution of a task in a qualitative matter and to estimate the corresponding human error probability	With a relatively simple and straightforward manner allows analysts to estimate human contribution to the risk, to calculate the possibility of the occurrence of a human error and to identify the factors that compromise human performance. In addition suggestions either to improve safety or to deal with the unpleasant consequences are provided	Lack of data and biased experts judgment can compromise the validity of the analysis. Findings may vary based on analysts experience, background and training. Complex techniques can only be used by experienced and trained analysts. The analysis can be both time-consuming and exhaustive	Uncertainty analysis was not included in the first stages of human performance modeling. Both interactions between employees and interdepen-dencies between factors that compromise human performance were not taken into account, Only recently, new approaches are trying to incorporate uncertainty analysis into the overall human performance modeling frame	A number of HRA techniques have been applied to several domains, such as nuclear power plants, chemical plants, medicine and transportation. However, the lack of data may compromise the validity of the methods	Despite the large number of existing HRA techniques only few tools have been developed to facilitate their use. Nevertheless, most of the methods can be implemented by using pen and paper	Results are usually a combination of quantitative and qualitative outcomes. In the first case the human error probability is estimated. Qualitative results provide to analysts a detailed illustration of the possible errors

[a] Including proof of concepts, benchmarking against other methods, validation