Chapter 5
Conceptual Frameworks for Vulnerability Assessment

Critical Infrastructures (CIs) have basic traits in common such as large-size, wide-area coverage, complexity and interconnectedness but show significant differences in detail, even when limited to physical-engineered CIs. The challenges for understanding, modeling and analyzing these systems with regard to vulnerability are immense and far away from being resolved. Approaches can be of two types, empirical and predictive, or a combination of both, as they complement each other (Johansson and Hassel 2010). By empirical investigations, previous events are studied in order to understand the behavior of CIs and the (inter)dependencies between them as well as to identify patterns, while predictive approaches aim to model the behavior of single or a group of CIs to find potential high consequence cases and non-obvious vulnerabilities.

5.1 General Outline

Applied methods, in particular for predictive analysis, have different view points, e.g., functional or structural, different levels of abstraction, different focus, objectives and metrics, different degrees of maturity and based on different levels of available information and knowledge, etc., None of the available methods alone is capable to address and tackle the variety of issues of vulnerability assessment including the impact of (inter)dependencies. It is commonly agreed that a universal, all-encompassing ("silver-bullet") approach or model which accounts for all issues does not exist (Eusgeld et al. 2009; Johansson and Hassel 2010).

Therefore, a conceptual framework is needed to bring all aspects, attributes and capabilities together and which goes beyond the pure analytical framework (architecture). Attempts have been made to develop conceptual frameworks with varying degrees of precision (see also Aven 2010) and focus, e.g., modeling interdependencies (Dudenhoeffer et al. 2006; Johansson and Hassel 2010), covering safety and security (Aven 2010) or cases of malevolence (Piwowar et al. 2009).

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_5,

Some proposals address single sectors like the Internet infrastructure (Qu et al. 2002), electric power grids and control systems (MIA 2010) or physical-engineered, (inter)dependent CIs in general (Eusgeld et al. 2009; Utne et al. 2009).

The goal of vulnerability analysis as outlined in Chap. 1 can be translated into a set of generic questions to be answered such as:

- What are the end states of interest for the given system(s) and how to define their boundaries?
- What are the threats and hazards of relevance that the system(s) under consideration might be exposed to?
- What is the sensitivity (susceptibility) and resilience of the system(s) experiencing them?
- What are resulting cascades and which (inter)dependencies can be identified? What is their impact and which are the high consequence scenarios?
- What are the uncertainties involved?

And finally:

- What are the obvious and non-obvious ("hidden") vulnerabilities and how can they be reduced and/or better managed?

Further specification of these questions is necessary when starting the vulnerability assessment of a specific system or a set of interconnected systems, and this can only be done in close cooperation between the analysts and the orderer ("problem owner") or recipient of the analysis, e.g., a public authority or private entity. The questions of what vulnerability/risk is and how it can be measured in the specific case, and at which level of accuracy, need to be answered precisely.

5.2 Outline of Stepwise Framework Approaches

It seems to be commonly agreed that a conceptual framework for vulnerability analysis should follow a stepwise, problem-driven approach tailored to the needs of the analysis. Two examples are given here, based on two different starting viewpoints.

5.2.1 Framework Tailored to Previously Defined, Undesired Events

The first example concerns a framework focused on the analysis of interdependency issues among CIs (Utne et al. 2009) and assumes that undesired events affecting several CIs can be derived from experience or gained by "brain power", and can be selected for further analysis. This so-called DECRIS conceptual framework for cross sector infrastructure vulnerability analysis starts with a

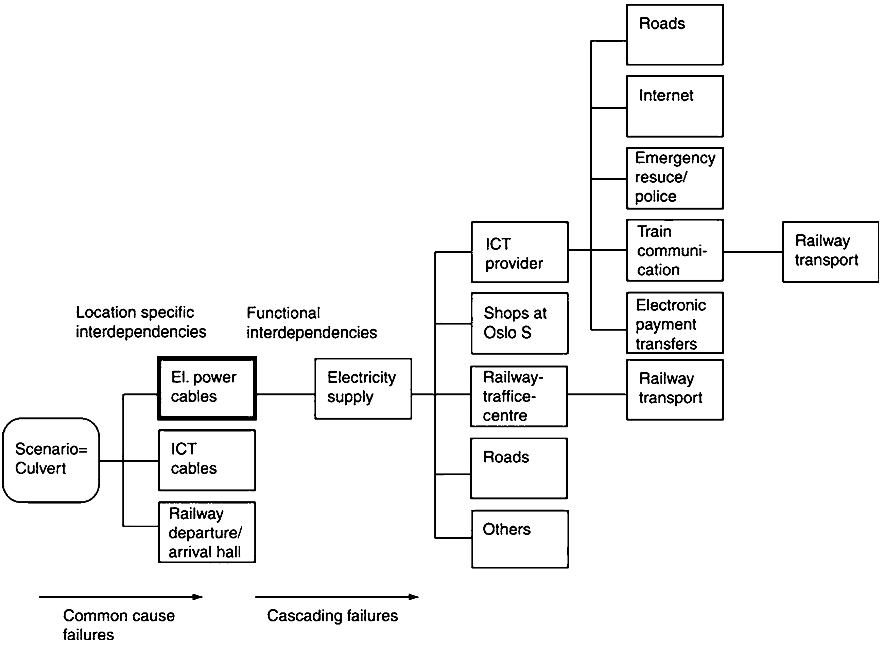

Fig. 5.1 First and second order functional interdependencies identified by applying the DECRIS framework (Utne et al. 2009). ("STOP" box indicates that we choose not to further analyze this object or function in detail)

screening analysis of experienced undesired events (phase 1) to select events, involving several infrastructures of interest, for further detailed analysis (phase 2). The first task of phase 2 aims at developing those selected, undesired events into accident scenarios and investigating interdependencies between the causes of undesired events and between infrastructures; the development of an adequate system understanding is regarded as an important pre-requisite (sub-task). The second task aims at identifying interdependencies of first or a higher order including location-specific (geo-spatial) and functional ones as main causes of cascading failures. The third task aims at analyzing the risks related to the interdependencies by means of qualitative or semi-quantitative methods using probability/frequency, extent and duration as quantitative measures of an accident scenario. If the semi-quantitative does not provide sufficient information, a quantitative analysis should be carried out (task 4) using network models and fault/ event trees. Finally (task 5), risk reducing measures have to be evaluated and the question to which extent the scenario could occur in other locations be answered.

The DECRIS framework has been applied to "damage to culvert/joint conduit of electric power, ICT, and water mains based on an undesired event that occurred in Oslo on November 27, 2007. Figure 5.1 shows first and second order identified functional interdependencies.

5.2.2 Framework Including Scenario Generation

The second example (Eusgeld and Kröger 2008; Eusgeld et al. 2009), includes scenario generation by simulation and, where appropriate, a holistic "system-of-system approach". The proposed framework distinguishes five steps, several decision points and feedback loops (see Fig. 5.2)

5.2.2.1 Preparatory Phase

The first step, the preparatory phase, integrates the task framing and definitions (step 1.1) into the process of familiarization with the system, so as to provide suitable information about the system design and operation conditions. Basically, the preparatory phase aims at reaching a clear definition of the terms involved in the assessment and mutual understanding of the objectives between all parties which have a stake in the analysis of the infrastructure and its operation. It is also important to decide on the spectrum of hazards and threats to be included into the analysis which can be of many-sided nature, including intentional malicious acts. Furthermore, it is necessary to deeply understand failure models and effects of/on each of the components of the CI. For a more effective screening of the system vulnerability (and to find obvious vulnerabilities as early and efficiently as possible) some reasonable simplifications should be made. For example the questions whether the interconnected systems can be "decoupled" and analyzed separately, whether it is acceptable to focus on some weak points first, etc., have to be pre-assessed. These assumptions need re-visiting in a later phase of the assessment (step 3.2).

After key information is collected and pre-assessment is done, the knowledge base should be checked with respect to the availability of methods suitable for the defined tasks. To build adequate capability of analysis, interaction with the scientific community needs to be established where appropriate (*double arrow* in Fig. 5.2).

5.2.2.2 Development of System Understanding

In general, the analyst should have basic know-how about the system (design/layout and related standards, functionality, support and control subsystems, operating modes and conditions, etc.) and about the modeling and analysis methods (including limitations/simplifications). Collection and pre-processing statistical data, in particular about system failures, breakdowns, and near-misses to infer preliminary knowledge should be an essential part of the preparatory phase. This also helps to check whether the system is sufficiently well understood and to sharpen the view on vulnerabilities and (inter)dependencies in particular. Cooperation with and support of system owners/operators must be established to

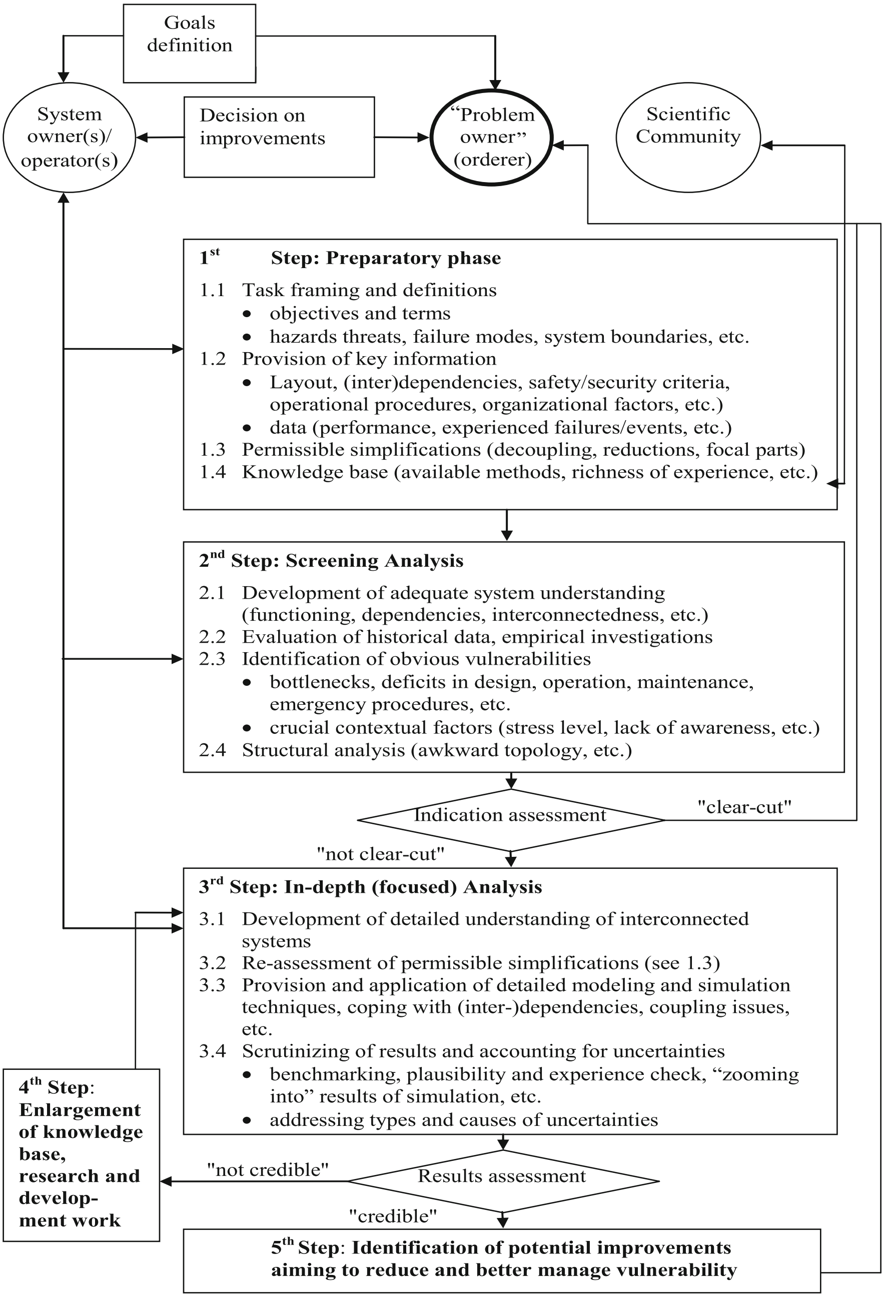
Goals definition
System owner(s)/ operator(s)
Decision on improvements
"Problem owner" (orderer)
Scientific Community
1st Step: Preparatory phase
1.1 Task framing and definitions
• objectives and terms
• hazards threats, failure modes, system boundaries, etc.
1.2 Provision of key information
• Layout, (inter)dependencies, safety/security criteria, operational procedures, organizational factors, etc.)
• data (performance, experienced failures/events, etc.)
1.3 Permissible simplifications (decoupling, reductions, focal parts)
1.4 Knowledge base (available methods, richness of experience, etc.)
2nd Step: Screening Analysis
2.1 Development of adequate system understanding (functioning, dependencies, interconnectedness, etc.)
2.2 Evaluation of historical data, empirical investigations
2.3 Identification of obvious vulnerabilities
• bottlenecks, deficits in design, operation, maintenance, emergency procedures, etc.
• crucial contextual factors (stress level, lack of awareness, etc.)
2.4 Structural analysis (awkward topology, etc.)
Indication assessment
"clear-cut"
"not clear-cut"
3rd Step: In-depth (focused) Analysis
3.1 Development of detailed understanding of interconnected systems
3.2 Re-assessment of permissible simplifications (see 1.3)
3.3 Provision and application of detailed modeling and simulation techniques, coping with (inter-)dependencies, coupling issues, etc.
3.4 Scrutinizing of results and accounting for uncertainties
• benchmarking, plausibility and experience check, "zooming into" results of simulation, etc.
• addressing types and causes of uncertainties
4th Step: Enlargement of knowledge base, research and development work
"not credible"
Results assessment
"credible"
5th Step: Identification of potential improvements aiming to reduce and better manage vulnerability

Fig. 5.2 Conceptual framework for the vulnerability analysis of interconnected infrastructures (flow chart-type of illustration; *double arrows* represent two-way interactions)

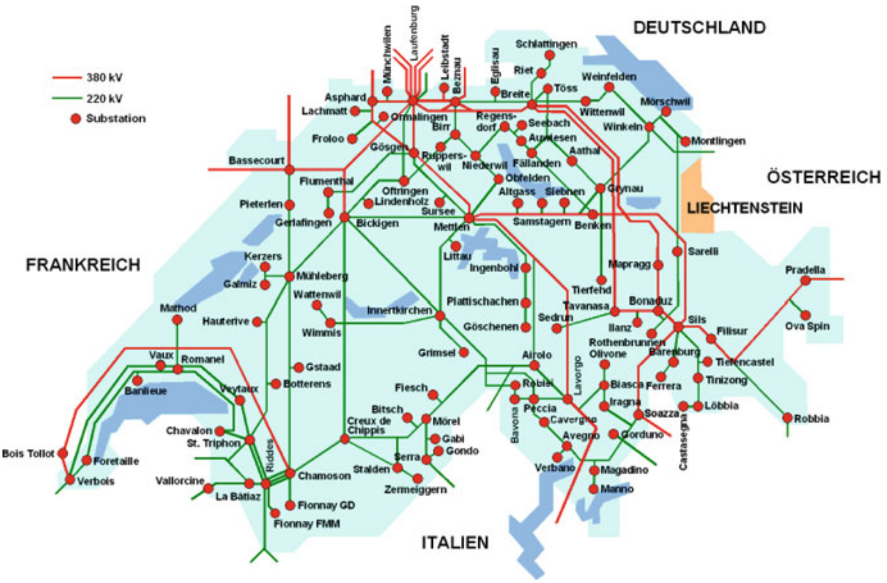

Fig. 5.3 Swiss high voltage electric power transmission system (www.swissgrid.ch)

allocate the information needs and to make sure that the system model is in accordance with reality. System visits ("walk through", "talk through") may be essential.

To which degree the rich and complex properties of the CI being assessed, including (inter)dependencies and cascading failures, need to be understood and how system boundaries should be fixed depends on the purpose and goals of the analysis. Let us take the domestic electric power transmission system as the example for illustration. If you are asked to assess the robustness of the system against random failures or targeted attacks, i.e., to investigate the topology, as part of a "screening analysis", the system boundary is narrow and topological unweighted network analysis seems appropriate; if you want to learn about inhomogeneities, the approach should be extended to weighted network analysis. The information necessary for such analysis is limited and can be procured from open sources, e.g., the Internet (see Fig. 5.3).

On the other hand, if the vulnerability of the electric power transmission system against "major blackouts", i.e., the unavailability of electricity for a large part of the population over a longer period of time, is to be assessed, methods of functional analysis, including modeling the dynamics of physical quantities of the real network (e.g., load flows), need to be applied (e.g., a two layers object-oriented modeling approach). For this "in-depth analysis (step 3 according to the framework), information about the system goes beyond open sources and must be provided by the system operator, with the usual care of the

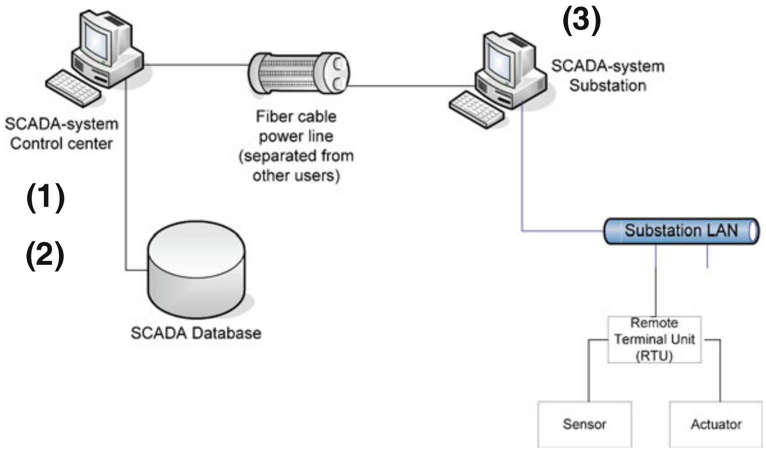
(3)
SCADA-system Substation
SCADA-system Control center
Fiber cable power line (separated from other users)
(1)
(2)
SCADA Database
Substation LAN
Remote Terminal Unit (RTU)
Sensor
Actuator

Fig. 5.4 Supervisory control and data acquisition (SCADA) system (simplified Swiss system) (1) Dedicated data exchange between power stations and network operator via PIA (system for exchange among partners) (2) Trading/office systems separated from SCADA (3) Substations have their own guidance systems and can, if needed, be operated by telephone lines; protection systems work independently from SCADA system

confidentiality issues involved; initial load flow conditions are an example of information needed from the system operation. The narrow domestic border cutting-off neighboring countries within the synchronized grid needs to be revisited.

Going one step further and making the disclosure of "hidden" vulnerabilities within the system, or of respective elements, calls for further details. The SCADA systems using modern information and communication technology (ICT) may introduce risks of cyber attacks or common cause failures. The search for potential entry points for potential "outside hackers" requires very detailed information about the layout and operation of this important industrial data acquisition and control system, which can only be provided by the transmission system operator (TSO) and calls for an excellent partnership and trust. Figure 5.4 attempts to illustrate the level of information needed in this case.

5.2.2.3 Screening and In-Depth Analysis

It is assumed that the vulnerability analysis should evolve in two steps where appropriate. A screening-type of analysis might be efficient and sufficient to identify eye-catching, obvious weak points vulnerabilities, e.g., awkward topology, spatial proximity of interconnected systems or bottlenecks, and further actions should focus on eliminating or reducing them. The screening analysis could also prepare the ground for and give steer to the in-depth analysis which may turn out necessary.

The *screening analysis* leads off with development of adequate system understanding (see also previous section); we assume that information provided from system owners/operators (step 1.2) allows for general understanding of main functionalities, states of relevance, interfaces, inter-dependencies, etc. In this phase, the main emphasis is placed on experts' opinions, brainstorming, etc., rather than on application of detailed models. Nevertheless, topology-driven analysis of vulnerabilities may provide an essential support to the screening analysis aiming at identifying the system connection patterns, shortest connection paths, local and global specifics, etc. The techniques used are typically based on complex network theory (see Sect. 6.2).

If the results and insights (indication assessment in Fig. 5.2) gained by screening analysis are not satisfying (not "clear-cut") and major hidden vulnerabilities are still feared, a more sophisticated *in-depth analysis* (step 3) has to be launched.

To achieve a higher degree of accuracy in the vulnerability evaluation, system understanding has to be further developed on the basis of additional information about the system and its operating environment (arrow to and from the owners/operators). Special attention should be placed on (inter)dependencies within or among systems. The re-assessment of simplifications made earlier (including bringing together "decoupled" systems) may call for more sophisticated methods of analysis, e.g., following a system or even a system-of-systems approach. In order to integrate a comprehensive spectrum of different phenomena, stochastic, time-dependent event chains and agent-based modeling approaches combined with Monte Carlo simulation and, where necessary, physical models may be considered (see Sect. 6.5).

Other frameworks exist for this part of the vulnerability analysis, proposing different architectures of analysis for specific types of infrastructure, e.g., for the Internet (see Fig. 5.5 for illustration).

The last but not least step of the in-depth analysis should focus on scrutinizing the results obtained and accounting for the uncertainties of both aleatory (stochastic) and epistemic (lack of knowledge including data and modeling) nature. While full validation and verification of models and methods, as well as of results, seem infeasible, benchmarking against other similar analyses, plausibility checks and checks against experienced events, if available, may help to support the credibility of the vulnerability assessment and build confidence in the decision making which follows.

The results of simulations typically represented by plots will need to undergo an appropriate process of "zooming" for the necessary deep understanding of the underlying scenarios and the examination of the main influencing parameters/factors. This would be helpful for finding relevant failure combinations and potential artifacts, respectively.

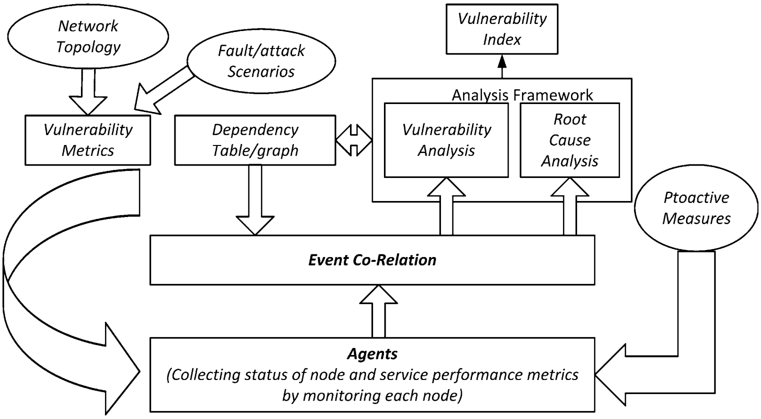

Fig. 5.5 Agent-based vulnerability analysis architecture for the Internet (Qu et al. 2002)

5.2.2.4 Results Assessment and Suggestions for Improvements

The final results of the vulnerability analysis should be assessed regarding their overall credibility. If a distinct need arises to further develop the knowledge base and/or the modeling and simulation techniques, R&D work should be triggered (step 4, Fig. 5.2) and the whole analysis might be delayed.

Depending on the results regarded credible and the related feedbacks from the ordering entity and system owner(s)/operator(s), system improvements (step 5) may be proposed to further reduce and better manage vulnerabilities by all means of provisions. The may include—besides "soft factors"—improved structural and functional design of the system(s), including redundancy and spatial separation, lowered stress level by increased safety margins and modified operational conditions, increased investment into new capacities and/or replacement of old equipment, increased cyber security, adapted emergency, etc.

The final decision about actually implementing the proposals of improvement is left to the "problem owner", possibly after iterating the vulnerability analysis in order to take changes into account and to assess the effectiveness of the proposed improvements and avoid negative feedbacks.

References

Aven T (2010) A unified framework for risk and vulnerability analysis covering both safety and security. Reliab Eng Syst Safe. doi:10.1016/j.ress2006.03.008

Dudenhoeffer DD, Permann MR, Manic M (2006) CIMS: A framework for infrastructure interdependency modeling and analysis. In Proceedings of the 38th conference on winter simulation, Monterey, California, 2006

Eusgeld I, Kröger W (2008) Comparative evaluation of modeling and simulation technique for interdependent critical infrastructures. In: Proceedings of PSAM9, Hong Kong, 18-23 May 2008, pp. 49–57

Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E (2009) The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Safe 94:954–963. doi:10.1016/j.ress.2008.10.011

Johansson J, Hassel H (2010) An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Safe. doi:10.1016/j.ress2010.06.010

MIA (2010) Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation/transmission infrastructures. Final report, September 2010, Italian National Agency for New Technology, Energy and Environment, Italy

Piwowar J, Châtelet E, Laclémence P (2009) An efficient process to reduce infrastructure vulnerabilities facing malevolence. Reliab Eng Syst Safe 94:1869–1877. doi:10.1016/j.ress2009.06.009

Qu G, Rudraraju J, Modukuri R, Hariri S, Raghavendra CS (2002) A framework for network vulnerability analysis. ITL Lab, the University of Arizona, University of Sothern California

Utne IB, Hokstad P, Vatn J (2009) A structured approach to modeling interdependencies in risk analysis of critical infrastructures. In: Proceedings of the European safety and reliability conference, ESREL 2009, Prague, Czech Republic, 7–10 September 2009