Reliability Engineering and System Safety 94 (2009) 954–963

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures

Irene Eusgeld [a,*], Wolfgang Kröger [a], Giovanni Sansavini [b], Markus Schläpfer [a], Enrico Zio [b]

[a] Laboratory for Safety Analysis, ETH Zurich, MLJ 14, Sonneggstrasse 3, 8092 CH-Zürich, Switzerland
[b] Energy Department-Nuclear Section, Polytechnic of Milan, Via Ponzio 34/3, I-20133 Milan, Italy

ARTICLE INFO

Article history:
Received 1 July 2008
Received in revised form
30 October 2008
Accepted 31 October 2008
Available online 13 November 2008

Keywords:
Vulnerability
Reliability
Critical infrastructures
Network theory
Object-oriented modeling
Power transmission network

ABSTRACT

A framework for the analysis of the vulnerability of critical infrastructures has been proposed by some of the authors. The framework basically consists of two successive stages: (i) a screening analysis for identifying the parts of the critical infrastructure most relevant with respect to its vulnerability and (ii) a detailed modeling of the operational dynamics of the identified parts for gaining insights on the causes and mechanisms responsible for the vulnerability. In this paper, a critical presentation is offered of the results of a set of investigations aimed at evaluating the potentials of (i) using network analysis based on measures of topological interconnection and reliability efficiency, for the screening task; (ii) using object-oriented modeling as the simulation framework to capture the detailed dynamics of the operational scenarios involving the most vulnerable parts of the critical infrastructure as identified by the preceding network analysis. A case study based on the Swiss high-voltage transmission system is considered. The results are cross-compared and evaluated; the needs of further research are defined.

1. Introduction

Critical infrastructures are 'a network of independent, large-scale, man-made systems (set of hard and soft structures)…that function collaboratively and synergistically to produce a continuous flow of essential goods and services' [1] and are essential for economic development and social well-being. They are subject to multiple, potentially asymmetrical threats (technical, intentional or unintentional human, physical, natural, cyber, contextual) and may pose risks themselves.

Critical infrastructures are dynamic, complex systems which are also highly interdependent, both physically and through a pervasive use of information and communication technologies.

The European electric power supply system serves as a good illustrating example, facing greater and tighter integration, also of new intermittent power sources, following the liberalization of most markets and being closely interconnected with other infrastructures, particularly the information and communication network.

Investigating risks and vulnerabilities for these kinds of systems has to go beyond the usual cause–consequence analysis to be able to focus on spill-over clusters of failures in case of strong interdependencies [2]. Indeed, the behavior of a complex system cannot be described as the sum of the behavior of its individual elements. This renders questionable the suitability of classical risk analysis methods, e.g. fault tree analysis, which are typically founded on a decomposition of the system into subsystems and basic elements and their subsequent recomposition for quantification. Furthermore, pre-defined causal chains, e.g. identified by event tree analysis, seem inappropriate to identify the hidden risks and vulnerabilities emerging in a complex infrastructure. On the other hand, simulation techniques may be recommended as 'scenario generators', but their computational cost may be excessive on real-size systems.

In practice, there is no single 'silver bullet solution' to the problem of analyzing the risks associated to critical infrastructures. Rather a framework of analysis seems to be needed in order to effectively integrate the different methods in a problem-driven approach to solution.

The present study aims at investigating the feasibility of complementing network analysis for performing an initial screening of the vulnerabilities of a critical infrastructure with object-oriented modeling to further deepen the vulnerability assessment of the screened scenarios.

2. A framework for the vulnerability analysis of critical infrastructures

The proposed methodical framework for the vulnerability analysis of critical infrastructures [3] follows a problem-driven,

* Corresponding author. Tel.: +41 44 632 64 19; fax: +41 44 632 10 94.
E-mail address: Eusgeld@mavt.ethz.ch (I. Eusgeld).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.10.011

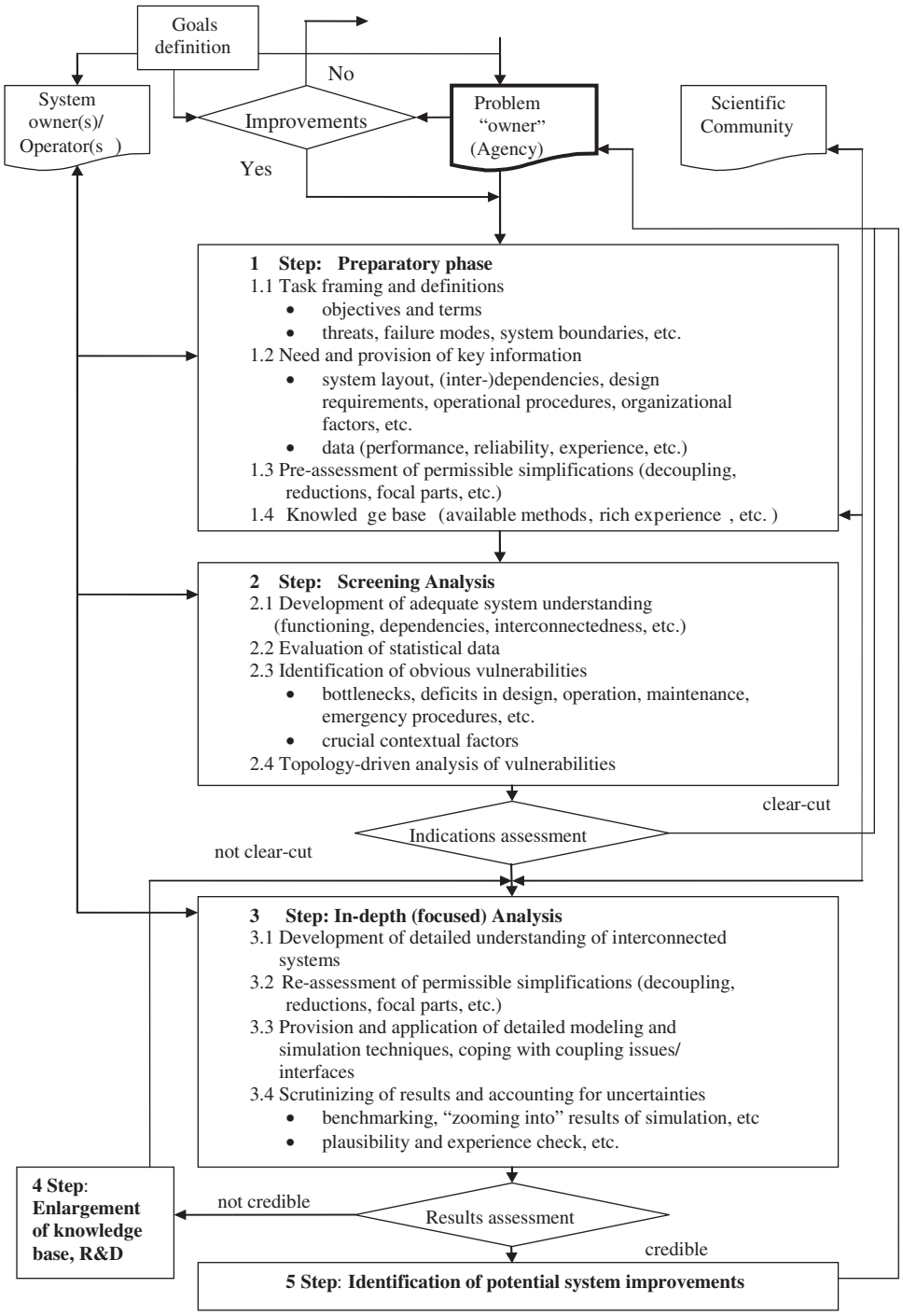

Fig. 1. Framework for the vulnerability analysis of interconnected infrastructures (flow chart-type of illustration; double arrows represent two-ways interactions).

iterative approach and includes five main steps, several decision points and feedback loops (see Fig. 1).

The preparatory phase aims at reaching a clear definition of the terms 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 threats to be included in the analysis which can be of many-sided nature. The proper definition and understanding of the system will facilitate distinguishing between obvious and hidden vulnerabilities. Whereas the former are likely to be recognized by the screening analysis (see step 2), the latter ones require detail modeling. For a more effective screening of the system some reasonable simplification should be done. 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 (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 [4]. To build adequate capability of analysis, interaction with the scientific community needs to be established where appropriate (double arrow in Fig. 1).

The next step "Screening Analysis" leads off with a development of adequate system understanding; we assume that

information provided from system owners in the step 1.2 assures general understanding of main functionalities, interfaces, (inter-) dependencies, etc. In this phase the main emphasis is placed on experts' opinions, brainstorming, etc., rather than on application of detailed models.

Topology-driven analysis of vulnerabilities provides an essential support to the screening analysis of step 2, aiming at identifying the system connection patterns, shortest connection paths, local and global specifics, etc. The techniques used are typically based on network theory (NT) (e.g. [5–10]). The case study of Section 3 serves to evaluate network theory with regards to its suitability for two objectives: for helping (a) to identify obvious vulnerabilities of a critical infrastructure by topology-driven analysis and (b) to guide and focus in-depth (detailed) analysis, based on, e.g., object-oriented modeling.

If the indications obtained in step 2 are not 'clear-cut' and major hidden vulnerabilities still need to be expected, a more sophisticated 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 interdependencies within or among systems. The re-assessment of simplifications made earlier (including bringing together 'decoupled' systems) may call for more sophisticated methods of analysis [6]. In order to integrate a comprehensive spectrum of different phenomena and to derive stochastic, time-dependent event chains an object-oriented modeling approach could be applied. In this regard, object-oriented modeling has demonstrated its attractiveness for the detailed simulation of infrastructures (see Section 3.2, also [11]). The drawbacks of this approach are that the simulations are time consuming and a larger number of parameters need to be set, the data for which may not be readily available in practice.

The last step of the analysis is that of accounting for uncertainties through benchmarking (if possible), plausibility and experience checks, etc. The results of a simulation are sometimes represented as plots: in such cases, the process of 'zooming into results' (understanding of underlying scenarios, examination of main influencing parameters/factors) is helpful for finding relevant failure combinations and potential artifacts, respectively.

If a distinct need to further develop modeling and simulation techniques becomes obvious, R&D work should be triggered (step 4, Fig. 1) and the whole analysis might be delayed.

Depending on the obtained results and related feedbacks, system improvements (step 5, Fig. 1) may be proposed to protect vulnerabilities by means of structural safety provisions (e.g. increased redundancy) or organizational changes (e.g. modified emergency procedures). The final decision about actually implementing the proposals of improvement is left to the 'problem owner', possibly after retrofitting the vulnerability analysis (see 'Yes'-arrow on top of Fig. 1) in order to assess the effectiveness of the improvements and to avoid negative feedbacks.

3. Screening and in-depth analysis of the Swiss high-voltage grid: a case study

The reference system for the study is the Swiss 220 kV/380 kV high-voltage transmission system (Fig. 2), which consists of a single-control area. In 2006 the electric power consumption in Switzerland has totaled to 62.1×10^3 GWh with a peak load of about 10 GW. The electric power production and installed capacity has totaled to 59.4×10^3 GWh and 12 GW, respectively; 42.2% of the electricity is produced by nuclear, 52.4% by hydro and 5.4% by conventional thermal generation [12].

3.1. Network analysis as a screening tool for identifying the most vulnerable parts of a critical infrastructure

With reference to a power transmission infrastructure made of a number N of substations linked by K overhead lines, the screening analysis for identifying the most vulnerable elements may be first carried out by resorting to network theory from a purely topological point of view [13,14]. In this view, the system may be represented as a network of N nodes (also called components or elements) interconnected by K links (also called arcs or edges). Mathematically, this defines a graph $\boldsymbol{G}(N,K)$ whose connections are defined in an $N \times N$ adjacency matrix $\{a_{ij}\}$ with entries equal to 1 if there is an edge joining node i to node j and to 0, otherwise. Each link connecting two nodes has unitary length so that the distance between two nodes i and j is represented solely by the number of edges traveled in the path from i to j.

For studying the structural properties of the network, the probability distribution $P(d_{ij})$ of the shortest path lengths d_{ij} between any two nodes i and j in the network can be considered. This distribution can be obtained in N steps using the Floyd's sequential shortest path iterative algorithm which at each step constructs an intermediate matrix containing the current shortest distance between each pair of nodes, until convergence [15].

The shortest path length distribution $P(d_{ij})$ is often synthesized by a point value, the 'average' or 'characteristic path length', which represents the average of the shortest distances d_{ij} between

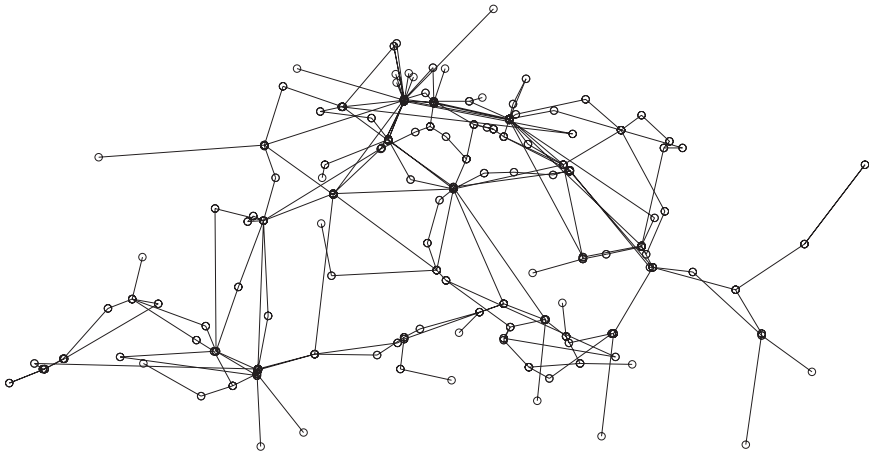

Fig. 2. The 220 kV/380 kV Swiss transmission network.

all pairs of nodes:

$$L = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij} \quad (1)$$

Further insights on the connectivity properties of the network are given by its degree distribution, $P(k)$, i.e., the distribution of the number of substations k, which are connected to an arbitrary substation [16].

Also at a local level, the connectivity of the network is typically synthesized by a single-point value, the 'average clustering coefficient'. The clustering coefficient C_i is a local property of node i defined as follows [17]: if node i has k_i neighbors, then at most $k_i(k_i-1)/2$ edges can exist between them; C_i is the fraction of these edges that actually exist, and C is the average value $C = (1/N)(\sum_i C_i)$.

To further delve into the properties of the power transmission system, the screening analysis proceeds to adopt the formalism of weighted networks [18,19]. This is done by considering the matrix $\{p_{ij}\}$ of the reliabilities of the edges in the network. Using this information to evaluate the shortest path lengths d_{ij} allows characterizing the network in terms of how efficiently it propagates the power flux on both the global and local scales.

From the point of view of the power transmission efficiency, the focus is on the annual transmission reliability between pairs of nodes i and j. On the basis of both $\{a_{ij}\}$ and $\{p_{ij}\}$ (or the complementary to one, $\{q_{ij}\}$), the matrix of the shortest (most reliable) path lengths $\{d_{ij}\}$ can be computed as [19]

$$d_{ij} = \min_{\gamma_{ij}} \left(\frac{1}{\prod_{mn \in \gamma_{ij}} p_{mn}} \right) = \min_{\gamma_{ij}} \left(\frac{1}{\prod_{mn \in \gamma_{ij}} (1 - q_{mn})} \right) \quad (2)$$

where the minimization is done with respect to all paths γ_{ij} linking nodes i and j and the product extends to all the edges of each of these paths. Note that $1 \leqslant d_i \leqslant_j \infty$, the lower value corresponding to the existence of a perfectly reliable path connecting i and j (no failure will occur in the links involving this path, i.e., $p_{mn} = 1$, $q_{mn} = 0 \quad \forall mm \in ij$) and the upper value corresponding to the situation of no paths connecting i and j (i.e., in all connections from i to j there is at least one failure $p_{mn} = 0$, $q_{mn} = 1$).

The reliability efficiency in the transmission between two substations i and j is then defined to be inversely proportional to the distance of the shortest (most reliable) path linking them. Thus, the network is characterized also by an efficiency matrix $\{\varepsilon_{ij}\}$ whose entry is the efficiency in the power transmission between nodes i and j:

$$\varepsilon_{ij} = \frac{1}{d_{ij}} \quad \text{if there is at least one path connecting } i \text{ and } j$$
$$= 0 \quad \text{otherwise} (d_{ij} = \infty)$$

The average reliability efficiency of the power transmission network $\boldsymbol{G}$ is then

$$E_{glob}(G) = \frac{\sum_{i \neq j \in G} \varepsilon_{ij}}{N(N-1)} = \frac{\sum_{i \neq j \in G} 1/d_{ij}}{N(N-1)} \quad (3)$$

This quantity plays a role similar to that of the previous measure L in defining the network connection characteristics on a global scale, the difference being that it also accounts for the reliability of the edges in providing the power transmission. The characteristic path length takes into account the stops required to get from one node to another and it represents the sequential path along the network. The efficiency measure retains also the information about the reliability of a specific path in the network where all the nodes concurrently give contribution to the system service, i.e. it is the efficiency of a parallel system [18]. Since $\varepsilon_{ij} = 1$ when there is at least one perfect path γ_{ij} in the graph which connects nodes i and j through a sequence of non-failing edges, $E_{glob}(G)$ is equal to one in case of a non-failing, perfectly connected network.

As for the local properties of the graph $\boldsymbol{G}$, these can be quantified by specializing the definition of the average efficiency (3) on the subgraph $\boldsymbol{G}_i$ of the neighbors of each node i in the network,

$$E(G_i) = \frac{\sum_{n \neq m \in G_i} \varepsilon_{nm}}{k_i(k_i - 1)} \quad (4)$$

Averaging the efficiency of the local neighborhoods of all nodes in the network, a measure of the network local reliability efficiency is defined:

$$E_{loc}(G) = \frac{1}{N} \sum_{i=1 \in G}^{N} E(G_i) \quad (5)$$

Since $i \notin \boldsymbol{G}_i$, this parameter reveals how much the system is fault tolerant in that it shows how efficient the power transmission remains between the first neighbors of i when i is removed.

The quantity defined by Eq. (5) has a similar local character as the clustering coefficient C. Yet, these two different indicators convey complementary information.

Further insights in the properties of the power transmission network can be inferred from an analysis of the most vulnerable overhead lines, i.e. those edges most crucial for the efficient connectedness of the network [20,21]. When some edges are unavailable to transmission, due to some failure or disconnection, the safest paths between nodes change due to forced detours around the failure. In this view, the vulnerability of the network is defined in terms of the degradation in the global safety efficiency of the network due to the disconnection, i.e. the interruption, of a set of its links:

$$V^* = \frac{E_{glob}(G) - E_{glob}(G^*)}{E_{glob}(G)} \quad (6)$$

where $\boldsymbol{G}^*$ is the new graph resulting from $\boldsymbol{G}$ when the disconnected connections are taken out. By construction, V^* takes values in the range [0,1].

This measure could be also regarded as the capability of the network of effectively redistributing the load over its working part. The vulnerability will be higher if the new shortest paths which the load is to be carried along will not be as effective as those in the previous unfailed configuration.

3.1.1. Application to the Swiss high-voltage grid

The system is made up of $N = 161$ nodes (busbars) connected by $K = 219$ overhead lines (double lines are modeled by single lines).

The system is modeled as a stochastic, undirected, connected graph $\boldsymbol{G}(N, K)$ in which each substation is transposed into a node, linked by edges representing the overhead lines connecting two subsequent substations (Fig. 2).

Depending on the analysis, each edge is either unweighted (weight = 1), for a purely topological analysis, or weighted by its reliability for an analysis of the power transmission efficiency.

The stochastic failure behavior of the power transmission system is described by introducing for the generic overhead line connecting substation i to substation j, a constant annual failure rate λ_{ij} per km. Such failure rate represents the number of failures occurred in 1 year along 1 km of overhead line connecting a given pair of substations i and j. For the sake of simplicity, it is assumed that $\lambda_{ij} = \lambda$ for the whole power transmission network. Given the assumption of constant failure rate, the annual reliability of the

line connecting nodes i and j is

$$p_{ij} = e^{-\lambda l_{ij}} \tag{7}$$

where l_{ij} is the length of the line.

We shall refer to this quantity as the reliability of edge ij and call failure probability of edge ij its complement to one, $q_{ij} = 1 - p_{ij}$. Thus, in addition to the adjacency matrix $\{a_{ij}\}$, the matrix $\{p_{ij}\}$ (or the complementary $\{q_{ij}\}$) is introduced to describe the failure behavior of the power transmission system.

Some cautious words should be spent on the crude homogeneity assumption that $\lambda_{ij} = \lambda$ for all lines in the power transmission network. A single value of annual failure rate per 100 km of overhead line was available from [22]. This value takes into account atmospheric effects, external effects (due to external human actions) and operational margins (unexpected overloads, wrong operations, planned maintenance, failure of the material). With the homogeneity assumption of all line failure rates being equal, the probabilities of failure of the various overhead lines differ only due to their length. In reality, other factors should be taken into account in the reliability evaluation, like the geographical position or the age of the material of the line and its usage.

Both topological and reliability efficiency analyses have been carried out for assessing the power transmission network properties and transmission performances [14]. Fig. 3 shows that the shortest path length distribution has a tail up to $d_{ij} = 17$, implying that one has to pass at most through 17 nodes for the power to be transmitted from one point to another in the network. This value is the so-called diameter of the network [17]. The largest portion of the distribution is concentrated around values of $d_{ij} = [3,5]$ and the distribution peaks at $d_{ij} = 5$, implying that the connectivity of this network is high.

A characteristic path length $L = 6$ is found. This clearly reflects the d_{ij} distribution and confirms that the network has good global connectivity properties.

The degree distribution, plotted in Fig. 4, peaks at about $k = 2$ but has quite large values also for $k > 2$. This implies that a failed substation disconnected from the network can easily be overtaken through other paths in the system. Nodes with $k = 1$ are the boundary substations of the Swiss power transmission network.

A direct measure of the clustering coefficient of the power transmission network gives the rather small value of $C = 7.79 \times 10^{-2}$. The predominant series structure of the network is responsible for the large number of sparse subgraphs around the nodes, a phenomenon which leads to the small values of the average clustering coefficient [21].

In Table 1, the values of global and local reliability efficiencies are shown. They are compared with the topological efficiencies,

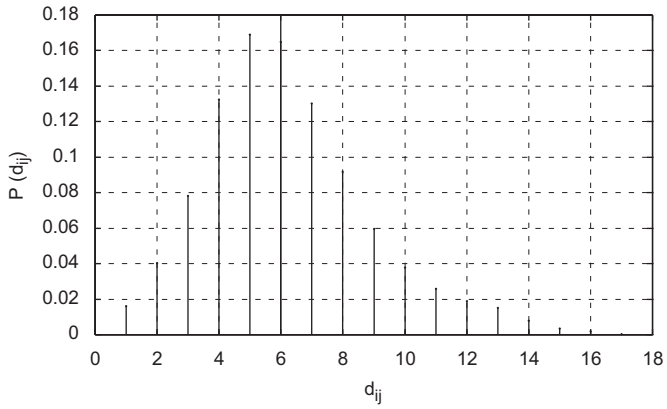

Fig. 3. Shortest path length distribution for the Swiss power transmission network.

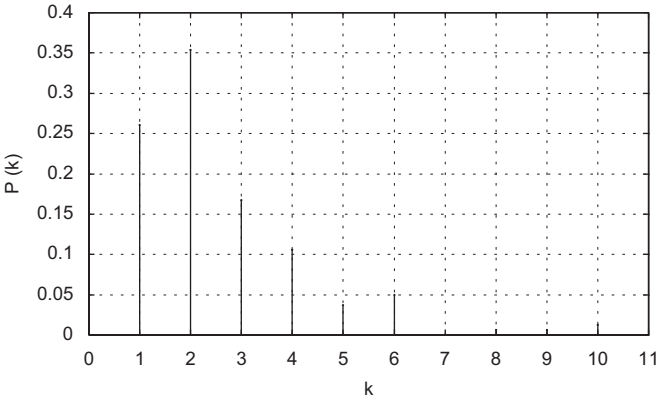

Fig. 4. Degree distribution for the Swiss power transmission network.

Table 1
Topological and reliability efficiencies $E_{glob}(G)$, $E_{loc}(G)$.

	Topological efficiency	Reliability efficiency
Global efficiency, $E_{glob}(G)$	20.5×10^{-2}	9.30×10^{-2}
Local efficiency, $E_{loc}(G)$	7.89×10^{-2}	4.72×10^{-2}

Table 2
The five most vulnerable lines according to the topological vulnerability evaluation.

Line index	Starting node—arriving node
55	30—85
127/191 (double line)	16—27
58	38—45
217	26—27
218	29—30

which are the upper values of reliability efficiencies for perfectly reliable overhead lines. The topological efficiencies account only for the topological connectivity pattern in the network (unweighted links).

In synthesis, it is interesting to underline the good global topological connectivity properties of this network, which provides it with a good robustness to random failures.

With respect to the vulnerability assessment against targeted attacks, two different analyses have been performed: a topological and a reliability one.

In the topological analysis, only the connectivity pattern of the network has been considered and the vulnerability index has been evaluated with respect to the global topological efficiency. The five most vulnerable lines resulting from the topological vulnerability evaluation are reported in Table 2 and displayed in Fig. 5.

In the reliability analysis for the identification of vulnerabilities, both the connectivity pattern of the network and the reliability of each line have been considered. The same assumption on the line annual failure rates has been made. The vulnerability index has been evaluated with respect to the global reliability efficiency. The five most vulnerable lines according to the reliability vulnerability evaluation are reported in Table 3 and displayed in Fig. 6.

Comparing the results in Tables 2 and 3, Figs. 5 and 6, one notices little difference between the vulnerable lines identified by the topological and reliability analyses. Indeed, the four lines ranked most vulnerable are actually the same in the two cases. This is possibly due to the crude assumption of equal failure rates,

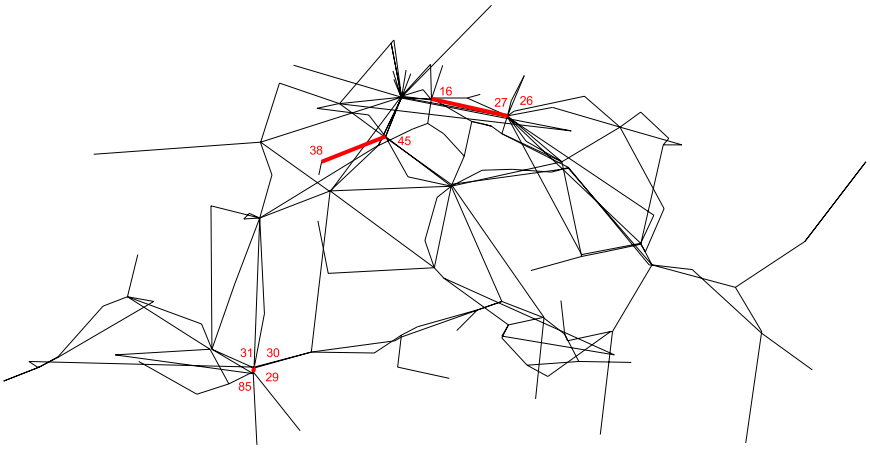

Fig. 5. The five most vulnerable lines according to the topological vulnerability evaluation.

Table 3
The five most vulnerable lines according to the reliability vulnerability evaluation.

Line index	Starting node—arriving node
55	30—85
127	26—27
127/191 (double line)	16—27
58	38—45
151	45—80

which makes the reliability of a line only dependent on its length. This implies that the reliability evaluation is very similar to a weighted evaluation, with the weights being the lengths of the lines.

3.1.2. Considerations on the network analysis approach for screening

The network theory approach is computationally very fast and easy to implement. In this sense, it is a valuable tool for performing an initial screening of the vulnerabilities of the system so as to focus the directions of further detailed vulnerability analysis by more sophisticated models.

However, the static character of the analysis cannot capture the dynamic behavior of the system, i.e. the dynamics of the loads and generators and their reconfigurations in this case. Moreover, the topological model that the system analysis relies upon does not take into account the load patterns in the system, so that the system vulnerabilities are identified based only on the connection patterns of the network. This is a limitation in the physical description of the system behavior since the load distribution on the overhead lines may not necessarily follow the topology of the system.

Finally, the Swiss grid is an open system with given energy flux boundary conditions with neighboring countries. These conditions should be taken into account as they may bring additional vulnerabilities to the network.

3.2. Object-oriented modeling for the in-depth analysis of the most vulnerable parts of a critical infrastructure

One of the major advantages of an object-oriented approach for modeling and simulating critical infrastructures, is the possibility to include physical laws into the simulation and to emulate the behavior of the infrastructure as it emerges from the behaviors of the individual objects and their interactions. In other words, the overall system behavior results from the interactions among the multiple single objects of different kinds which make up the system.

This modeling achieves a closer representation of the system behavior by integrating the spectrum of different stochastic phenomena which may occur, thus generating a multitude of representative stochastic, time-dependent event chains.

3.2.1. Introduction to the object-oriented modeling approach

In order to integrate stochastic time-dependent technical and non-technical factors into the vulnerability assessment of a critical infrastructure such as the electric power system, a two-layer object-oriented modeling approach has been proposed by some of the authors [11]. Objects are used to model both technical components such as generators, and non-technical components such as grid operators. The different objects interact with each other directly (e.g. generator dispatch) or indirectly (e.g. via the physical network). Within the two-layer concept (Fig. 7), the lower layer represents the separate modeling of the physical components by means of conventional, deterministic techniques such as power flow calculations, whereas the upper layer represents the abstraction of the electric power system with all its technical and non-technical components as individual objects.

Each object is modeled by attributes, e.g. physical constraints on technical components such as thermal limits of transmission lines, and by rules of behavior, which include both deterministic and stochastic time-dependent processes, each triggered by an input from the object environment. A deterministic process is for instance the outage of a component when its condition reaches a failure threshold, while stochastic processes are probabilistic component failure modes, changing load levels or operator reactions in case of contingencies. Further details of the modeling of the different objects are given in Ref. [11].

During simulation, the objects provide informational input to the physical network layer (e.g. generator out of service due to maintenance), whose conditions are updated accordingly, and then sent back to the objects that react to the new conditions in accordance with their behavioral rules. This approach allows to explicitly include the grid operator (transmission system operator (TSO)) into the model.

3.2.2. Application to the Swiss high-voltage grid

The aim of the analysis of the Swiss high-voltage grid (Table 4) is to investigate the applicability of the object-oriented approach to in-depth modeling of a real system. The results obtained make no claim as to actually quantifying the vulnerability of the Swiss high-voltage grid.

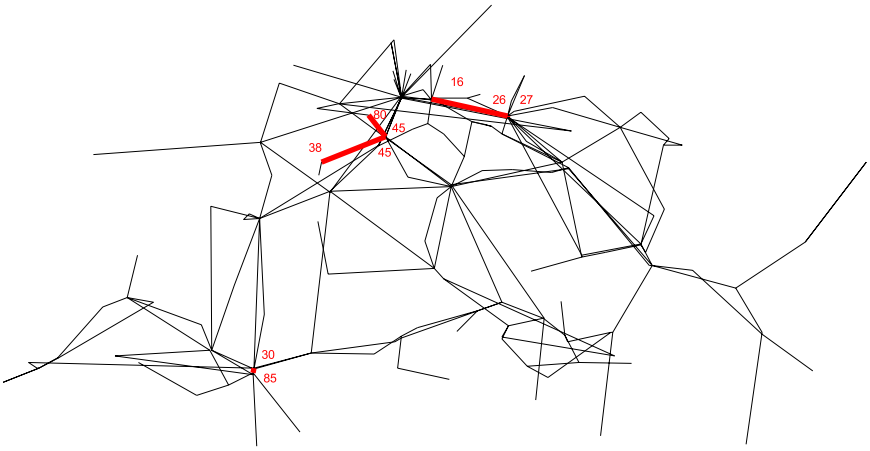

Fig. 6. The five most vulnerable lines according to the reliability vulnerability evaluation.

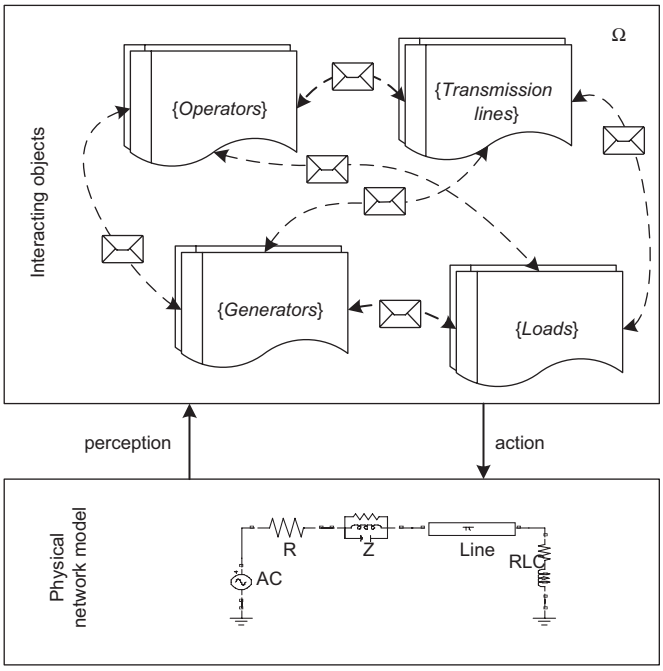

Fig. 7. Two-layer concept applied to the electric power system.

Table 4
Number of components of the Swiss system.

Components	Number
Loads	99
Generators	34
Transmission lines	229
Busbars	161
Grid operators	1

Some results from the simulation are depicted in Fig. 8, with respect to the unserved energy per event (in particular, the complementary cumulative blackout frequencies, $\hat{F}_c(C_E)$, and the histogram of the different outage causes). The complementary cumulative blackout frequency follows an exponential curve. Generation inadequacy is the dominant factor regarding the larger events, while load shedding for line overload relief becomes important in the range of the smaller events. The influence of load disconnections due to system splitting is significant, but the frequency of this outage cause never exceeds the frequency of load disconnections due to generation inadequacy or load shedding due to the operator action.

Hence, under our model assumptions, it can be concluded that the system reliability is somewhat more sensitive to generation outages than to transmission line failures.

The relative overload frequencies for each transmission line, h_l, are reported in Fig. 9. About 15% of all overload contingencies are occurring on only two lines. Furthermore, several groups of adjacent lines can be identified as being prone to overloads, helping to highlight the most critical system regions.

Table 5 and Fig. 10 depict the five most vulnerable lines, i.e. those which were disconnected most during blackouts and are thus the most critical with respect to the system vulnerability. Interestingly, the line which is disconnected most during

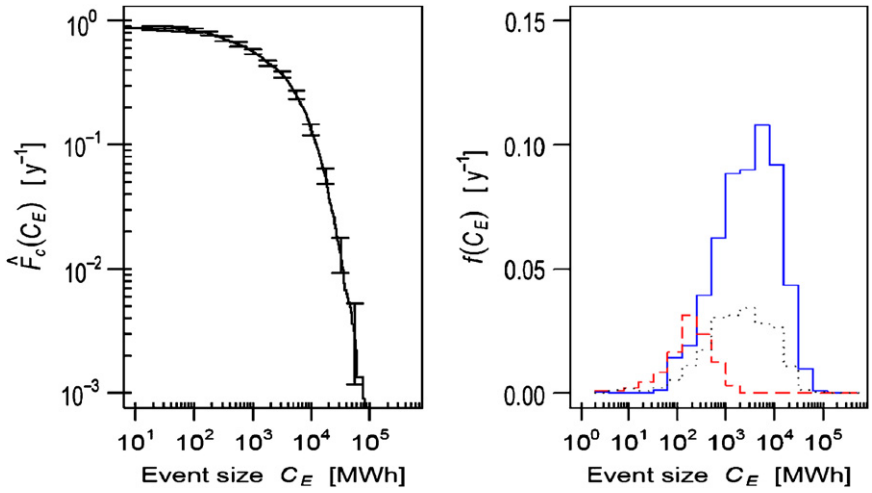

Fig. 8. Left: complementary cumulative blackout frequencies for the Swiss system with respect to the unserved energy. The error bars indicate the 90% confidence intervals. Right: histogram indicating the distribution of the outages due to generation inadequacy (continuous line), system splitting (dotted line) and load shedding for line overload removal (dashed line) [11].

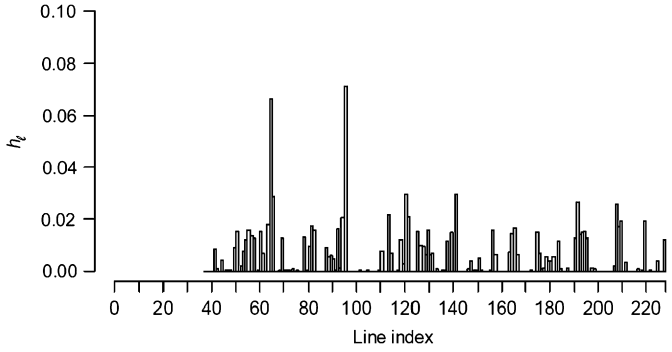

Fig. 9. Relative frequency of transmission line overloads [11].

Table 5
Five most disconnected lines during blackout events.

Line index	Disconnections per blackout event
193	0.459883
142	0.155538
114	0.147926
129	0.098218
89	0.082184

blackouts is not one of the most overloaded lines. Instead, line 193 triggers most blackouts in the model.

A cross-comparison of the line indices in Table 5 with those in Tables 2 and 3 show that the results of the two approaches do not correspond to each other.

3.2.3. *Considerations on the object-oriented approach for detailed modeling of vulnerabilities*

Although several model refinements are still needed, the results obtained in the present case study prove the capability of the object-oriented approach to assess the availability of bulk power systems for the purpose of mid- or short-period power planning. The level of modeling detail allows analyzing a multitude of time-dependent availability aspects, e.g. system weak points and upgrades. Although so far the approach focuses only on technical failures, the integration of other factors such as natural hazards, institutional weaknesses or security-related issues is possible and straightforward.

The main problems to overcome are the slow simulation speed and the large number of parameters to be input in the analysis. In order to obtain statistically significant results for a system-operating period of 1 year, around 50 h of simulation are needed on a single conventional desktop computer (Dell Optiplex GX260 with a Pentium 4 CPU of 2.66 GHz and 512 MB of RAM).

However, by focusing on specific safety aspects, the model can be significantly simplified and the computational burden reduced. Besides its application to the 'pure' electric power system, the approach seems also appropriate for analyzing interdependencies among different critical infrastructures.

4. Open issues on the methods for screening and in-depth vulnerability analysis of critical infrastructures

The framework for the vulnerability analysis of critical infrastructures underpinning the presented work stands basically on two successive phases: (i) a screening analysis for identifying the parts of the critical infrastructure most relevant with respect to its vulnerability and (ii) a detailed in-depth modeling of the operational dynamics of the identified parts for gaining insights on the causes and mechanisms responsible for the vulnerability. The application of the two phases (by network analysis and object-oriented modeling, respectively) on a realistic case study has shown that:

1. In the screening analysis, the network theory approach can be useful for identifying structural criticalities, e.g. the most connected nodes and shortest path lengths of connection.
2. On the other hand, the findings by the network theory analysis of the system structure do not match those obtained by the detailed, in-depth modeling of the system physical behavior by object-oriented modeling. This suggests that additional investigation must be carried out to identify appropriate static indicators of the physical behavior of the system, to be used as representative weights of the connections in the network structure. These indicators should capture the main physical characteristics of the transmission load capacities and reliabilities of the network elements so that their criticalities are

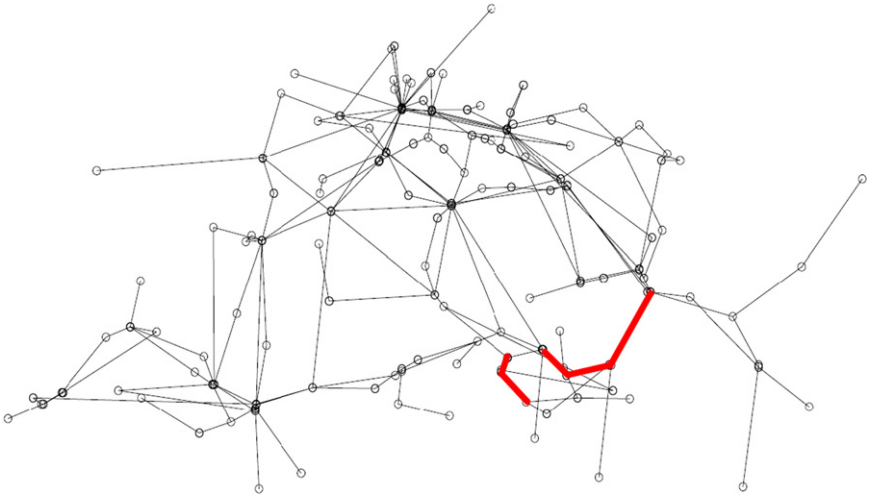

Fig. 10. The five most vulnerable lines according to disconnections during blackout events.

evaluated accounting also for these physical aspects. In this definition of the appropriate indicators, the in-depth, detailed analysis of the physical behavior by object-oriented modeling should serve for providing insights on the operational aspects to be captured in the indicators and for verifying whether such indicators indeed lead to identifying the critical elements of the infrastructure. Of course, it is still to be shown that it is indeed possible to identify static indicators representative, in a lumped manner, of the system physical behavior, which is dynamic in nature.

3. Object-oriented modeling has been shown to offer an attractive modeling paradigm for describing the dynamic system operational behavior with close adherence to the reality of the coupled processes involved. On the other hand, this simulation-based approach becomes highly computer intensive for complex realistic systems such as the infrastructures of interest in this paper. The challenge in this respect is to reduce the computational burden, e.g. making use of rare event simulation techniques or by substituting some objects with empirical models, like neural networks, while quantifying the uncertainty introduced in the approximation of the empirical models.
4. In the end, there is the usual inevitable compromise between adherence to reality and the budget of resources/costs available for the analysis. The availability of data for estimating the model parameters also plays a decisive role. The combination of a screening stage followed by a zoom with a more in-depth analysis on the screened critical areas may in principle be effective in optimizing such compromise. However, research is still needed to show how the two phases of analysis can be carried out in a meaningful way and then combined with efficacy.

5. Conclusions and outlook

This paper has looked into the role which network analysis and object-oriented modeling can play in a framework for the vulnerability analysis of critical infrastructures.

The potentials of using network analysis based on measures of topological interconnection and reliability efficiency have been scrutinized. The results of the case study presented, based on a model of the Swiss high-voltage grid, have demonstrated that network analysis is suitable for identifying structural criticalities, e.g. the most connected nodes, shortest path lengths of connection, most vulnerable nodes, etc.

The potentials related to the use of object-oriented modeling for the detailed description of the dynamic behavior of infrastructures have been examined. With respect to the case study presented, although model refinements are necessary for a more realistic description of the system, the results confirm the applicability of such technique.

The indications derived from the two analyses, i.e. the most vulnerable parts of the Swiss high-voltage grid, were critically compared; the fact that the results obtained by the two approaches do not match, confirms that the two analyses look at different aspects of the problem and reveals the need for further research on how to merge the insights gained from both into a practical framework of analysis.

In particular, some research efforts may be worthily directed to:

- Identifying appropriate static indicators of the physical behavior of the system, to be used as representative weights of the connections in the network structure. These indicators should capture the main physical characteristics of the transmission load capacities and reliabilities of the network elements so that "their criticalities" better account for these aspects.
- Considering the trade-off between very realistic modeling (including physical laws and system dynamics), in an attempt to reduce the model parameters and speed up the simulation on one side, and to increase the degree of sophistication of 'quick and simple' methods to satisfactorily describe the system behavior, on the other side.
- Optimizing the technical implementation of the models, relying on the evolution of both hard- and software simulation tools.
- Gaining experience in applying the proposed approaches to get insights in the parameters to be used and the model adaptations to be introduced.

Acknowledgments

The authors would like to thank "swiss*electric research*" for co-financing the work on which the present paper is based and Swissgrid AG for providing the operational data of the Swiss electric power system.

References

[1] Ellis J, Fisher D, et al. Report to the President's Commission on Critical Infrastructure Protection. S.E. Institute, Editor Carnegie Mellon University, 1997.
[2] White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures, IRGC, 2006.
[3] Eusgeld I, Kröger W. Towards a framework for vulnerability analysis of interconnected infrastructures. In: Proceedings of the ninth international conference on probabilistic safety assessment and management (PSAM 9), 2008. p. 107–16.
[4] Eusgeld I, Kröger W. Comparative evaluation of modeling and simulation technique for interdependent critical infrastructures. In: Proceedings of the ninth international conference on probabilistic safety assessment and management (PSAM 9), 2008. p. 49–57.
[5] Barabasi AL. Linked: the new science of networks. Cambridge, MA: Perseus Publishing; 2002.
[6] Bar-Yam Y. Dynamics of complex systems. Westview Press; 2002.
[7] Capra F. The web of life. New York: Doubleday; 1996.
[8] Kauffman SA. The origins of order. Oxford: Oxford University Press; 1993.
[9] Special section on complex systems. Science 1999:284(5411);79–109.
[10] Watts DJ, Strogatz SH. Collective dynamics of 'small-world' networks. Nature 1998;393:440–2.
[11] Schläpfer M, Kessler T, Kröger W. Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. In: Proceedings of the 16th power systems computation conference, Glasgow, 2008.
[12] Swiss Federal Office of Energy. Swiss electricity statistics 2006 (German), Bern, 2007.
[13] Sen P, Dasgupta S, Chatterjee A, Mukherjee G, Manna SS. Small-world properties of the Indian railway network. Phys Rev E 2003;67:036106.
[14] Zio E, Sansavini G. A systematic procedure for analyzing network systems. Int J Crit Infrastruct 2008;4(1/2):172–84.
[15] Floyd RW. Algorithm 97: shortest path. Commun ACM 1962;5(6):345.
[16] Barabasi AL, Albert R, Jeong H. Mean-field theory for scale-free random networks. Physica A 1999;272:173–87.
[17] Albert R, Barabasi AL. Statistical mechanics of complex networks. Rev Mod Phys 2002;74(1):47–97.
[18] Latora V, Marchiori M. Efficient behavior of small-world networks. Phys Rev Lett 2001;87(19).
[19] Zio E. From Complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. Int J Crit Infrastruct 2007;3:488–508.
[20] Latora V, Marchiori M. Vulnerability and protection of infrastructure networks. Phys Rev E 2005;71(015103).
[21] Zio E, Sansavini G. An analytical approach to the safety of road networks. Int J Reliab Qual Saf Eng 2008;15(1):67–76.
[22] VSE–AES, Statistik 2005 über die Verfügbarkeit der Elektrizitätsversorgung der Schweiz, 2005.