https://doi.org/10.26552/com.C.2008.1.54-59

Michail Senovsky – Pavel Senovsky *

CRITICAL INFRASTRUCTURE RISKS

Critical infrastructure can be taken as a phenomenon of recent time. Not only theory but also practice has shown that solving problems of the protection of critical infrastructure, especially ensuring its functionality, is a necessary precondition for the operation of public authorities, services, the viability of a region, area or country. The first step to protect the critical infrastructure must be the identification of risks endangering the security of single systems or elements. The contribution deals with the problems of searching for and denoting these risks and by looking for their interrelations.

Key words: Critical infrastructure, analysis, risk, assessment.

1. Introduction

The priority of critical infrastructure protection is given by efforts to preserve the functionality of public authorities. If the functionality of public authorities is preserved, then an assumption exists that also the population has a real chance of surviving a crisis state or situation without serious health damage. The complexity of ensuring the protection of critical infrastructure is given not only by the fact that it is a case of areas of decisive importance to the operation and functioning of the state, but also by the fact that many elements may significantly influence their surroundings, and cause thus a certain "domino" effect.

Then, the cardinal issue is a question of knowledge of individual limits of the system of critical infrastructure, and thus the determination of adequate protection.

What are the objectives of critical infrastructure protection?

As a simple answer we could use, e.g.: "When taking into account all threats and risks, the objective of critical infrastructure protection is to ensure the functioning of critical infrastructure objects, their interrelations and thus the creation of a basic precondition for the functioning of the state".

This general definition can be specified, for instance, as follows:
- A need to select critical infrastructure objects on individual management levels:
- The preservation of basic functions of a territory (municipality, region, state).
- The preservation of basic functions of the state.
- The preservation of functionality of objects necessary for dealing with incidents.
- The protection of potentially threatened objects.
- Establishing communication between the public authorities and entities of critical infrastructure.

The basic question of critical infrastructure protection is then the finding of interrelations between individual systems of critical infrastructure. By finding these interrelations we are able to assess or evaluate much better their vulnerabilities and consequences on the other systems of critical infrastructure. A result of critical infrastructure protection should be the minimization of consequences of infrastructure destruction so that damage to the functions of public authorities or services may be:
- short-term
- sparse
- controllable (also temporarily)
- limited in area.

To meet these preconditions, at first we must find risks, denote them, be aware of their interrelations across the systems of critical infrastructure, and accept adequate measures to eliminate the risks found. Countries can have various priorities and also different conceptions concerning which countries or elements of critical infrastructure should be included into the critical infrastructure.

The Security Council of the Czech Republic has determined the basic areas of critical infrastructure as follows: Table 1

ENERGY SECTOR	- Electricity - Gas - Thermal energy - Oil and oil products
WATER MANAGEMENT	- Water supply - Water security and management - Wastewater system
FOOD INDUSTRY AND AGRICULTURE	- Food production - Food safety - Agricultural production

* **Michail Senovsky, Pavel Senovsky**
Faculty of Safety Engineering, VSB – Technical University Ostrava, Czech Republic, E-mail: michail.senovsky@vsb.cz

HEALTH CARE	– Pre-hospital urgent care – Hospital care – Public health protection – Production, storage and distribution of pharmaceutics and medical means
TRANSPORTATION	– Road – Railway – Air – Inland water
PUBLIC AUTHORITIES	– State authorities and local authorities – Social protection and employment – Execution of justice and prison service
EMERGENCY SERVICES	– Fire and Rescue Service and Fire Brigades – Police of the Czech Republic – Army of the Czech Republic – Monitoring services of radiation, chemical and biological protection – Prognoses, alert, warning service
BANKING AND FINANCIAL SECTOR	– Finance – Banking – Insurance – Capital market
COMMUNICATION AND INFORMATION SYSTEMS	– Fixed net services – Mobile net services – Radio communication and navigation – Satellite communication – Radio and television broadcasting – Postal and courier services – Access to the Internet and data services

With regard to the fact that in the framework of EU any unambiguous method for the search for individual critical points of systems and their interrelations is not determined, the following part presents the opinion of authors about one of possible solutions for the analysis of critical infrastructure elements.

2. Network Analysis

For easy understanding, a network is necessary to be conceived as a large pattern with a large number of nodes and links. It is important to realise that we do not only search for individual elements that may endanger their surroundings, but that we search also for their interrelations by which a failure can spread. Some segments of critical infrastructure are of network character (road network, energy supply network); the other segments depend directly on these networks.

We are looking for a network model. We can say that individual objects can form network nodes. Pathways within the CI system then can be links between the nodes. However, we can see this problem also from the point of view of e.g. electricity distribution. Somewhere the transformer station will be located, from which electricity will be delivered to individual objects. Here, a system of distribution substations or switchboards will be implemented and electricity will be distributed to the last machine, to the last office. If we search further, it will be surely possible to map, describe and plot these networks.

2.1 Risk Concentration.

Risks endangering a network infrastructure are usually distributed non-uniformly in the network, concentrated into a relatively small number of "*critical*" nodes. These nodes are easy-to-identify by the number of links to other nodes and the capacity of them (according to the segment considered).

A difference between the uniform and the real distribution of nodes in the network is clear from Fig. 1.

Graphs in Fig. 1 were constructed by using the Scale-free Simulace program [1, 2].

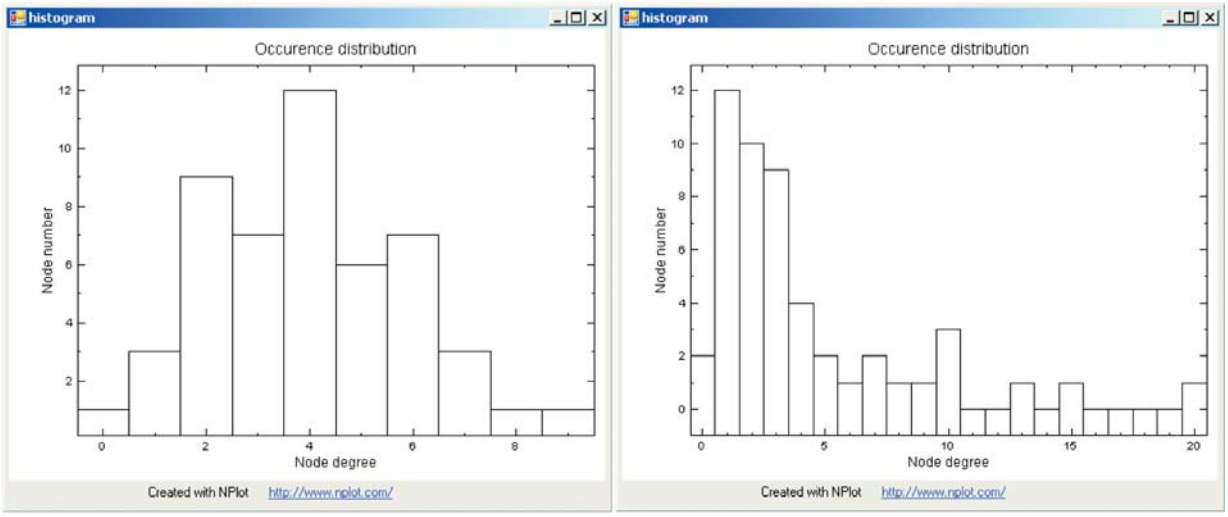


Fig. 1 Random frequency distribution in the network versus real node distribution in the network

The problem of network infrastructure protection often consists in the fact that we cannot afford to realise protection always on the same level for the whole network, and thus it is necessary to search for critical points – their putting out of action will bring the greatest damage. It is effective to protect just these points.

2.2 Networks, Cascades.

A sector failure is often caused by a cascade failure in the network. A relatively small fault in one node spreads through the network to other nodes, e.g. by a series of errors, the propagated error thus may lead to a collapse of the whole network. It is a velocity at which the fault spreads and the velocity at which individual nodes are repaired that will decide whether the damaged infrastructure will be finally restored or will collapse.

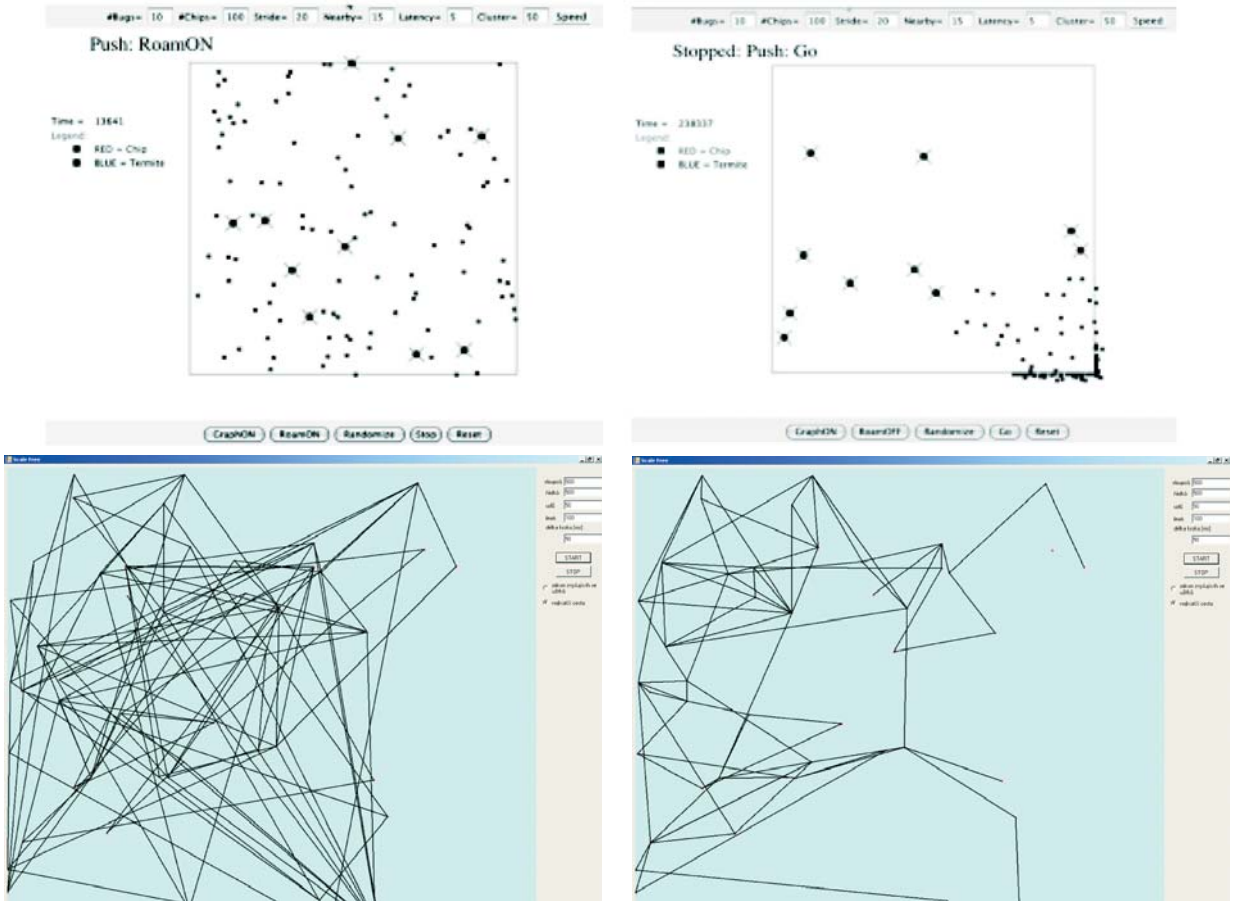
2.3 Simulation – an Approach to Searching for a Solution.

In studying networks, modelling as well as simulation is today implemented by special software. Simulations are usually based on the repeated application of simple principles in the universe of simulation, by which the gradual organisation of universum universe by an emergence effect will be achieved.

An example of result of such a simulation is presented in Fig. 2.

3. Vulnerability Analysis

To be able to assess quantitatively the vulnerability of a sector, we can use the vulnerability analysis that represents a model of vulnerability of critical nodes. The analysis consists of network analysis; for the determination of reliability of the whole system, engineering tools are used. These tools provide a complete system for the identification of system weaknesses and vulnerability estimation, and on the basis of this information we can determine steps leading to an increase in security. If we are able to find thus weak points of the system, in the following step it will be possible to madke the analysis of these critical points focused on searching for a possibility of synergetic effects of expected incident.



(start of the simulation) *(end of the simulation)*

Fig. 2 Application of shortest path principle to a randomly generated network

3.1 A Model Based on the Vulnerability Analysis.

The basic model of vulnerability analysis is a comprehensive analysis method that puts the network, faults (events) and reliability analysis together into one method for the quantitative sector analysis of a branched network. In the analysis, network branching is evident. We analyse the vulnerability of branching by using a fault tree; all possible actions are organised as an event tree.

Network analysis. The first step to make the vulnerability analysis is the mapping (identification) of a system being assessed. This step will also help us to search for individual nodal points and their interactions.

3.2 Fault Tree Analysis.

A fault tree contains vulnerabilities, and it is possible to model how single elements interact and create an error or fault. The root of the tree is there at the top of the tree and represents the whole zone or its main part, and the "leaves" of the tree represent partial threats endangering the zone. In the course of solving the fault tree we use logic and probability to estimate the occurrence (origin) of faults in the system. The outcome of fault tree analysis is a list of element vulnerabilities with the expression of probability of origin. In the following figure, an example of fault tree analysis is given.

3.3 Event Tree Analysis

We shall use the outcomes of fault tree analysis as input information for an event tree analysis. The tree of events is a list of all possible events and their combinations leading to faults. Event trees are binary trees, we consider yes/no. Each error may occur only once. The "root" of the event tree is there at the top of the tree and "leaves" are there in the lower part of the tree. The leaves represent all possible actions that may occur, including faults. The

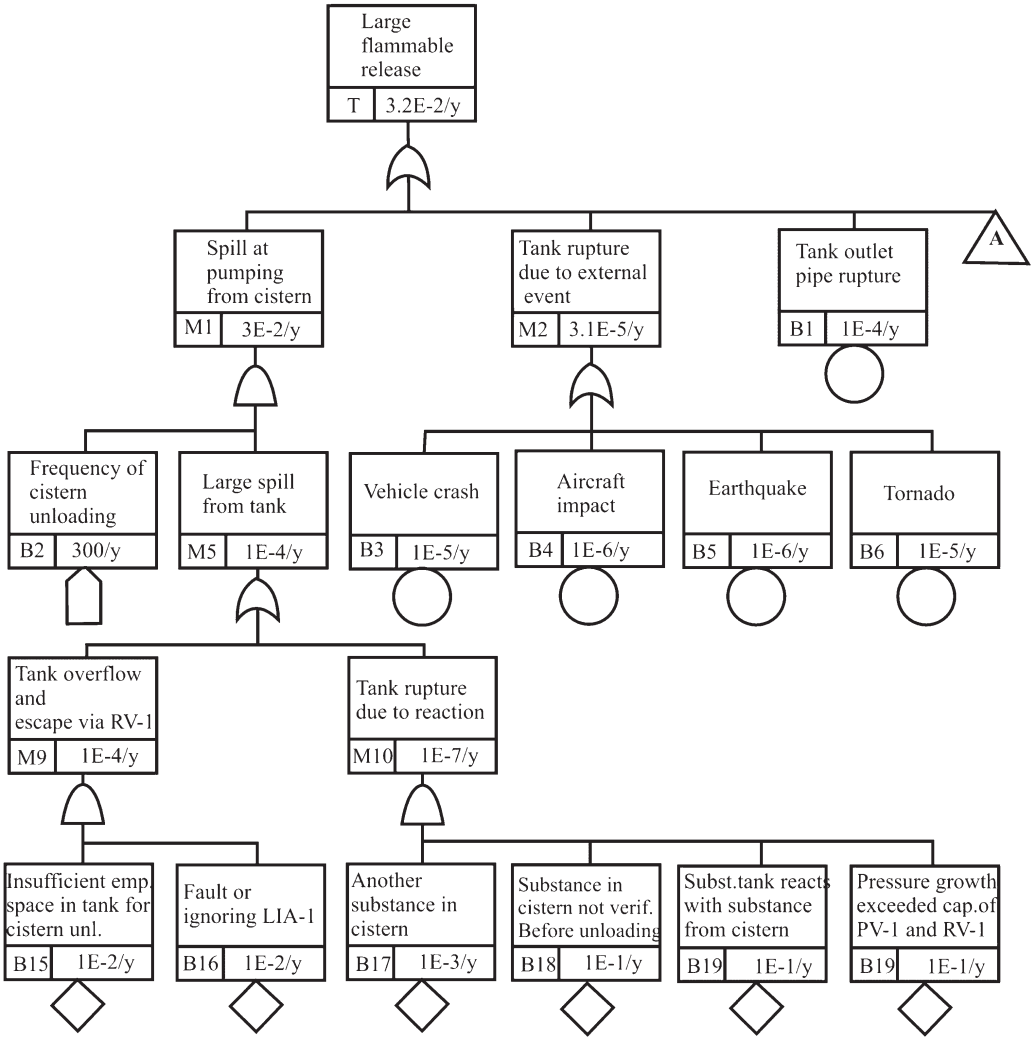


Fig. 3 An example of fault tree analysis

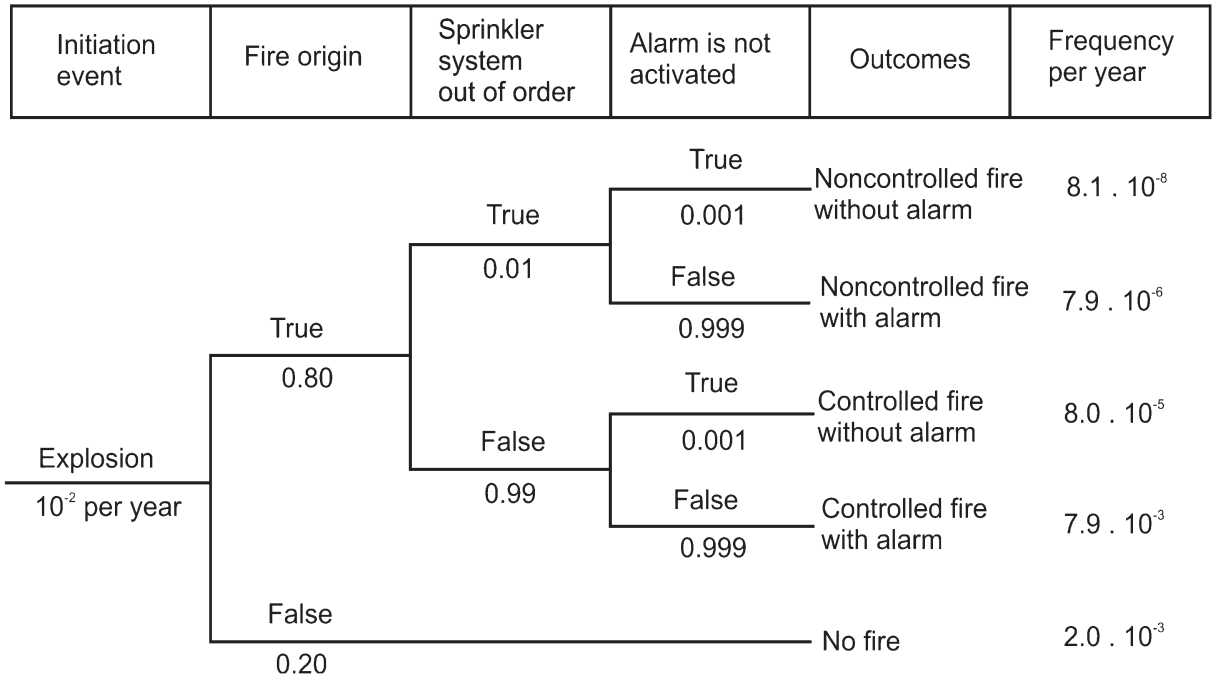


Fig. 4 An example of event tree analysis

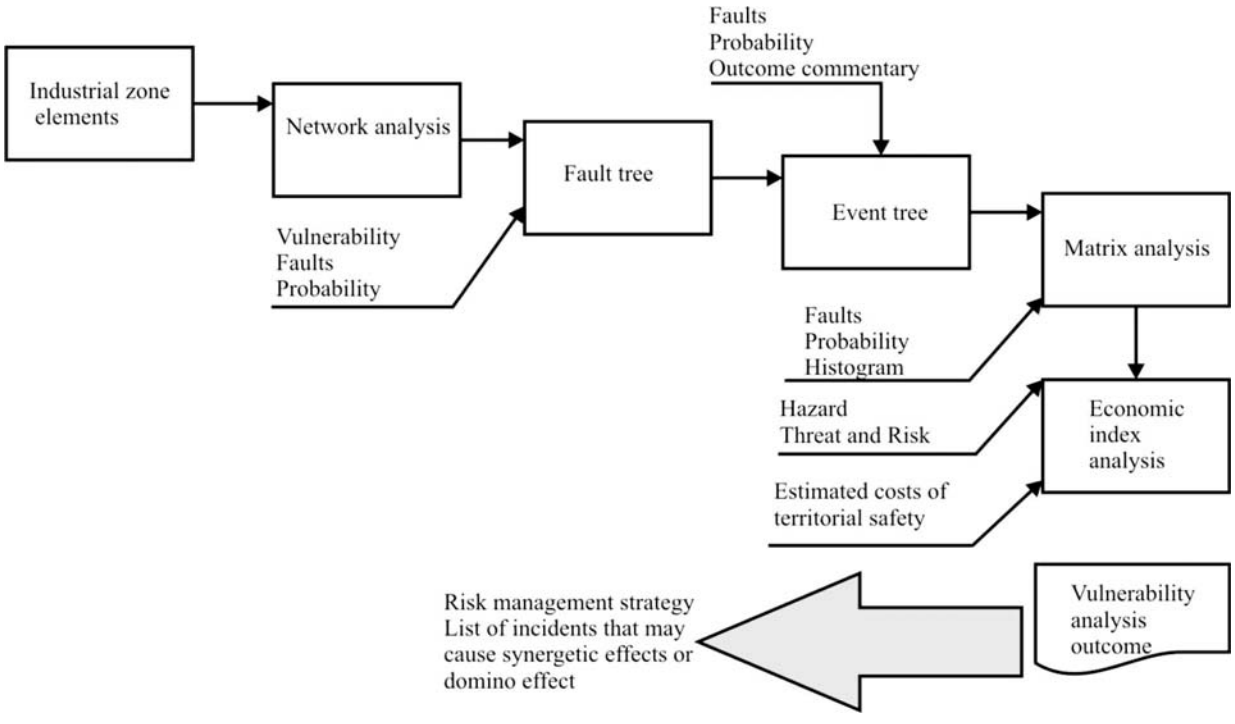


Fig. 5 Vulnerability analysis process

outcome of the event tree is a list of errors (vulnerability) and the probability of their occurrences expressed as the probability of error in a histogram. In the following figure an example of event tree is illustrated.

3.4 Matrix Analysis

The number of events listed in the event tree will become the number of potential errors. A matrix analysis can also work on the binary level or, in a more modern conception, each event can be described by more parameters, and thus we shall obtain a rather strong tool with which we are able, among other matters, to determine the severity of faults.

Diagrammatically the described system of analyses can be illustrated as shown e.g. in a figure given below.

4. Conclusion

Searching for an approach to the assessment of risks of critical infrastructure elements is at its very beginning. At present, we do not know any method being used by anybody with satisfactory results. The approach described in this contribution is a possible approach, but certainly not a single existing approach. We suppose that the final result of our research and search for a suitable model could be a knowledge-based system that would furnish the user with required information on critical infrastructure security requirements.

This article was written for the project no. VD20062008A04

References

[1] SENOVSKY, P.: *Scale-Free Simulace v1.1* [on-line], WWW <URL: http://homen.vsb.cz/~sen76/programy/cs/scalefree_v110_bin.7z > [cit. 2007-10-3].
[2] SENOVSKY, P.: *Usage of Emergence Effect for Simulation of Network Based Critical Infrastructure,* Proc. of conference Nebezpecni latky, SPBI: Ostrava 2006, 168 - 172, ISBN: 80-86634-91-4.
[3] SENOVSKY, M.; ADAMEC, V.: *Crisis Management Basics (in Czech)*, SPBI Ostrava, 2005, vol. 2, ISBN: 80-86111-95-4.
[4] URBANEK, J.F.: A *Prognosis for the Vulneranility of Cybernetic Items of Critical Infrastructure (in Czech)*, Proc. of 9. conference Soucasnost a budoucnost krizoveho rizeni, Praha, 2006, ISBN 80-239-7296-0, 06K-BE-12, pp. 5.
[5] VALASEK, J.: *Common Steps in the Risk Analysis (in Czech)*, Proc. of 11. conference Riesenie krizovych situacii v specifickom prostredi, Zilinska univerzita, Zilina, 2006, ISBN 80-8070-565-8.