SAFETY AND SECURITY GOVERNANCE PROBLEMS OF CRITICAL SYSTEMS AND INFRASTRUCTURES

Kosmowski K.T.

Gdansk University of Technology, Gdańsk, Poland

Abstract: This paper addresses some problems of the security and safety governance of critical systems and infrastructures. More important critical infrastructures are identified and characterized. Issues of their vulnerabilities and risks assessments are described. New challenges concerning the security and safety related decision making are specified.

1. Introduction

Defining of the critical systems and infrastructures and proposing conceptions of their security and safety managing in USA and Europe were initiated in middle of 1990-ties [7, 14]. Managing the safety and security is based on the risk assessments [2, 4]. The risk governance is a more general conception that requires an integrative approach [3, 8].

The security and safety problems gained lately significant attention in Europe. The report of the Group of Personalities in the field of Security Research was published in 2004 [15] identifying the problem's complexity and indicating integrated directions to deal with. Various preparatory actions started in the field of the security research [10], the critical infrastructure protection in the fight against terrorism [11] and to advance European security through research and technology [14].

In the paper selected issues associated with the safety and security analysis of critical system and infrastructures are outlined. The critical infrastructures can be ranked with regard to several criteria proposed. The final part of the paper describes new challenges of the security vulnerability management and the risk governance issues concerning more important critical infrastructures.

2. Identifying the critical infrastructures

2.1. Defining the critical infrastructures in USA

In the Executive Order 13010 (1996) the *infrastructures* are defined as "the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole" [7]. According to this Executive Order to these infrastructures include: telecommunications; electric power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government.

2.2. Defining the critical infrastructures in Europe

In the Communication [11] the *critical infrastructure (CI) are defined as "*those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments". In this document some other terms are also defined:

- *Infrastructure:* The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.
- *Threat:* Any event that has the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks.
- *Vulnerability:* A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.
- *Risk Management:* A deliberate process of understanding risk and deciding upon, and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

According to [11] the critical infrastructures include:

- *Energy installations and networks* (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system);
- *Communications and Information Technology* (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet);
- *Finance* (e.g. banking, securities and investment);
- *Health Care* (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services);
- *Food* (e.g. safety, production means, wholesale distribution and food industry);
- *Water* (e.g. dams, storage, treatment and networks);

- *Transport* (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems);
- *Production, storage and transport of dangerous goods* (e.g. chemical, biological, radiological and nuclear materials);
- *Government* (e.g. critical services, facilities, information networks, assets and key national sites and monuments).

These infrastructures are owned or operated by both the public and the private sector. Critical infrastructures must be defined at Member States' level and at European level and such lists should be established by the end of 2005 [11].

Some Europe's critical infrastructures have become more dependent on other infrastructures, e.g. the information technologies, including the internet and space-based radio-navigation and communication. Problems can cascade through these interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services [1]. *Interconnectedness* and *interdependence* make these infrastructures more vulnerable to disruption or destruction [6].

3. Ranking the critical infrastructures

The criteria for determining the factors that make a particular infrastructure or element of an infrastructure critical need to be studied. The selection criteria should also be based on a sectoral and collective expertise. Three main factors might be suggested for identifying potential critical infrastructure [11]:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, provincial/territorial or local.
- *Magnitude* - The degree of the impact or loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which could be used to assess potential magnitude are:
  (a) Public impact (amount of population affected, loss of life, medical illness, serious injury, evacuation);
  (b) Economic (GDP effect, significance of economic loss and/or degradation of products or services);
  (c) Environmental (impact on the public and surrounding location);
  (d) Interdependency (between other critical infrastructure elements); and
  (e) Political (confidence in the ability of government).
- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

In the Table 1 some preliminary criteria for considering and ranking the critical infrastructures are proposed. The cross-referencing marked "x" was placed to indicate the relevance of given infrastructure to criteria assumed and "(x)" the conditional relevance depending on the situation.

Table 1. Preliminary criteria for ranking the critical infrastructures

Infrastructure	Criteria considered to be critical, vital to			
	National defense	Economic security	Public health and safety	National morale
Energy installations/networks	x	x	x	x
Communication and information	(x)	x	x	(x)
Finance (baking, securities)		x		
Health care			x	x
Urban water supply and waste water treatment		x	x	(x)
Food production/distribution		x	x	(x)
Transportation	x	x	(x)	(x)
Production of chemicals / storage dangerous materials	x		x	(x)
Critical services and information networks, national monuments			x	x

It can be noticed that as more important critical infrastructures in relation to their targeting and vulnerabilities, following infrastructures should be considered:

- The energy installations / distribution networks;
- Communication and information (CI);
- Urban water supply and waste water treatment;
- Transportation (by rail, road);
- Production of chemicals (hazardous processes) / storage dangerous materials.

The energy critical infrastructure is very complex and includes the installations and networks of the electric power supply system and the gas supply system. Especially complex is the electric power system consisting of power plants and the distribution networks at various voltages with own telecommunications that are vulnerable to external hostile influences, malicious intents and cyber attacks.

In Europe it was assumed [10] that information from a number of sources will be needed to conduct threat, incident and vulnerability analysis of Member States critical infrastructure elements and their dependencies. Each sector and Member State will need to identify infrastructure critical to them, within their respective jurisdictions according to an EU harmonized formula and the organizations or persons in charge of security.

Not all infrastructures can be protected from all threats. For example, electricity transmission networks are too large to fence or guard. By applying risk management

techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, the existing level of protective security and the effectiveness of available mitigation strategies for business continuity [11].

Critical infrastructure protection (CIP) requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and Member States authorities. The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests on the owners and operators [11, 14].

4. Problems of the safety and security vulnerability analysis

4.1. The security vulnerabilities analyses of stationary hazardous plants

The *security vulnerability analysis* (SVA) [12] is aimed at determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact on the assets. SVAs are not quantitative risk analyses, but instead are performed qualitatively using the best judgment of the security, safety, and other appropriate professionals. The qualitative determination of risk, which is one of the desired outcomes of the SVA, provides the basis for establishing priorities to apply countermeasures. This is similar to the qualitative risk analysis process that is routinely applied is assessing accidental risk at the same facilities.

The *risk* that is being assessed within the SVA is an expression of the likelihood that a defined threat will exploit a specific vulnerability of a particular attractive target or combination of targets to cause a given set of consequences. For the SVA, the likelihood of the undesired security event is estimated qualitatively. The analysis is based on best available information, using experience and expertise of the team to make sound risk management decisions [2].

4.2. Possible interactions among critical infrastructures

Possible interactions among critical infrastructures are illustrated in Fig. 1. The relations and dependencies between critical infrastructures are becoming nowadays very complex. They require careful analyses, especially for abnormal and accidental situations, to propose effective remedial means based on technical and organizational solutions.

Fig.1. Illustration of possible interaction among critical infrastructures

Some examples of interactions denoted by two letters in Fig. 1 are described below:

A^B – Disruption of the gas supply can reduce the electric power generation that is especially important during abnormal situations and failures in the electric grid (the power plants and distribution system).

B^A – The gas transmission system uses their own gas to power pumps etc., but there are solutions that use partially the external electric power, also for drives of valves and control systems.

A^C – Disruption of CI systems that support monitoring, controlling and protecting the electric grid or managing the electric power market can contribute to significant economic losses.

C^A – Disruption of the electric power to the CI systems without backup makes their unavailability.

A^E – Disruption of the coal supply for a longer time will cause reduced generation of the electric power (especially important in cases of the lignite fired power plants when the electric transportation from a local mine is used).

E^A – Disruption of transportation relying on the electric grid.

B^C – Disruption of CI systems that monitor and control the gas system, support managing the gas markets can contribute to the safety problems and economic losses,

C^E – Communication lines follow the rail rights-of-way and can be disrupted by rail accidents or attacks.

E^C – Disruption of CI systems that control rail system or manage reservations and dispatch contribute to the safety problems and economic losses.

D^A – Disruption of electric power for water treatment and for pumps in water supply system can make significant problems for citizens; disruption of the electric

power in the sewer and sewage treatment systems can cause environmental problems.

D^E – The urban water system can be contaminated due to derailments and transportation spills.

One of the most important critical infrastructures is the electric power system [5, 9, 13].

4.3. Security and safety of the electric power system

The electro-energy safety is understood as covering energy flow to the consumers continuously or with very short breaks, which do not disturb the technological processes and meet the consumers' requirements and living conditions [9].

In normal states of the electric power system the safety relies on assuring that the generated power is sufficient to cover the demand. In abnormal states, during sudden and unexpected changes of the system structure, the safety relies on stopping the emergency situation growth, limiting its consequences, preserving supply of most important consumers, and enabling the system restoration in possible shortest time. The safety can be considered in different time horizons [9]:

- *Strategic safety*, related to the system development plans and investments – *several and more years*;
- *Long period safety*, related to environmental conditions and repair/maintenance plans – *one year*;
- *Middle period safety*, associated with preparing to operation – *one month*;
- *Short period safety*, associated with dispatching procedures – *24 hours*;
- *Online safety*, associated with current dispatching (during normal and abnormal states) – 0.1÷1 hour;
- *Violated safety*, associated with functioning the control and protection systems – *0.1÷1 sec*, and starting restitution of the electric power system.

Various factors and undertakings in relevant time horizons influence the electric power system safety [5, 6, 9]:

- Correctness of the forecast of the electrical energy demands in various time horizons;
- Investments ventures;
- Equipping the dispatching centers with advanced technical measures and the information infrastructure;
- Planning the repairs and maintenance, and supervising relevant tasks;
- Knowledge and skills of the personnel at various dispatching levels;
- Functions and the scope of protections and the system automatics;
- Procedures developed to deal with transients and abnormal states;
- Procedures for heavy abnormal states and blackouts protecting the system "islands";
- Procedures and the communication infrastructure for the system restoration after the system blackout.

Because the system breakdowns are probable and will take place, it is necessary to work out, for a particular system, the strategy of defense against failures and procedures to reduce the consequences when they occur, which will include reconnecting of "islands" and other subsystems.

Most dangerous subsystems states in the potential process of spreading breakdowns are states of significant overloads by the real power and the reactive power. For appropriate analyzing of the system operation with regard to its structure and automation it is necessary to develop the quantitative models based on deep understanding of the system characteristics and the influence of relevant phenomena in transients and dynamic breakdown situations [9]. However the risk modeling in such a complex systems require to use both quantitative and qualitative information [2, 3].

4.4. Directions in the governance of safety and security vulnerabilities

Managing the safety and security vulnerabilities of critical systems and infrastructures should be based upon the risk assessment. For some critical systems and especially critical infrastructures the life time can not be easily defined as they are subjected to processes of modernization in time and the complexity of such systems usually increases. Thus, the risk analyses in time should be carried out using the methodology useful for dealing with complex systems and including more important influencing factors, and being suitable to make assessments under uncertainty [2].

In Fig. 2 a schematic representation of the criticality degree versus adequacy of risk governance for six critical infrastructures is illustrated. Nine of categories of actions are distinguished: from 1 (No action required) to 9 (Urgent need for action). Taking into account international situation and given state conditions as regard criticality of services, from the point of view security and safety, it can be noticed that in the case of Poland following infrastructures are most critical and require further research to support the policy and decision making: Electricity (electric grid including the power plants and distribution networks), Communication and Information (telecommunications & computer networks, Internet), Gas Supply, Hazardous Plants (including hazardous material storage), Transportation (rail and road) and Urban Water.

The policy options that can be used to promote the protection of critical infrastructures depending on their degree of criticality and respective environment include [2, 13]:

- The creation of institutions and governance processes that involve all relevant actors to consider and balance conflicting social objectives such as economic efficiency, security, privacy etc.
- Legal framework and mandate for specific system structures and capabilities and binding operational rules; independent monitoring of compliance of legal requirements.

- Mandatory public reporting of metric for service disruption; independent investigation of system failures.
- The creation of insurance mechanisms to compensate losses.
- Tax incentives to create desired behaviors during investments and operation.
- The creation of institutions that identify, codify and promulgate voluntary standards and "best professional design practice"; monitoring and public reporting of compliance.
- Create legal, standardization and regulatory environment that allows and when needed promotes multiple service routes and certified providers.
- Mandate basic technology research as a "cost of doing business" for all players.

Fig. 2. Schematic representation of the criticality degree versus adequacy of risk governance for six critical infrastructures (based on [13])

A number of strategies can be proposed to promote the effective system design standards without resorting to inflexible government regulations: best professional practice, legal frameworks, certification, tort and liability, insurance, taxes or fees on uncertified equipment and systems, etc.

5. Conclusions

The strategies to deal with the safety and security management proposed in USA and Europe are similar to some extent but differ in implementation stage due to multi state character of Europe and necessity to coordinate efforts within European member states. Recently, as homeland security has been assigned the highest national priority, the term critical infrastructure has developed into a major policy concern. The risk analysis methods used for the safety management are not fully applicable for the security risk analysis and security managing. A new challenge is to develop an integrative approach for the risk governance.

The system security analysis is a challenging task and the risk assessment for the integrative safety and security governance is based mainly on expert opinions. Proposed approaches should include focusing on vulnerabilities that cut across more than one infrastructure. Interdependencies where the failure or attack on one infrastructure can have adverse effects on others, and geographic locations where a number of critical infrastructure assets may be located, need additional research to support rational security and safety oriented decision making. Important directions and ambitious programs of research in security domain are currently being proposed in Europe.

Prioritizing research efforts should be based on preliminary ranking the critical systems and infrastructures for a set of criteria. The electric power system and the communication / information networks are considered as most important critical infrastructures. As a complement to the measures which have been taken at national level, the European Union has already undertaken some legislative initiatives for setting minimum standards for infrastructure protection in the framework of EU policies. It is notably the case of the transport, communication, energy, occupational health and safety, and public health sectors.

References

1. Gheorghe V., Mili L. (Ed.): *In risk management, integrating the social, economic and technical aspects of cascading failures across interdependent critical infrastructures*. International Journal of Critical Infrastructures , p.1-7, 2004.

2. Kosmowski K.: *Challenges in security and safety management of critical systems and infrastructures*. Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety. TEHOSS 2005. Gdansk University of Technology, p.511-520, 2005.
3. Kröger W.: *Emerging risks: from risk management to risk governance*. Proceedings of the IEEE International Conference on Technologies for Homeland Security and Safety. TEHOSS 2005. Gdansk University of Technology, p.3-8, 2005.
4. Kunreuther H. C., Ley E. V. (Ed.): *The Risk Analysis Controversy.* An Institutional Perspective. Berlin, Springer-Verlag, 1982.
5. Marecki J., Kosmowski K.T.: *Problems of risk analysis and safety management in critical systems*. Energetyka III, p.83-89, 2004.
6. Mili L., Qiu Q., Phadke A.G.: *Risk Assessment of catastrophic failures in electric power systems*. International Journal of Critical Infrastructures 1, p.38-63, 2004.
7. Moteff J., Copeland C., Fischer J.: *Critical Infrastructures: What Makes an Infrastructure Critical*? Congressional Research Service, The Library of Congress; Resources, Science, and Industry Division; August 30, 2002.
8. Renn O., Graham P.: Risk *Governance, Towards an Integrative Approach*. International Risk Governance Council. Geneva, Switzerland, September 2005.
9. Szczerba Z.: Problems of electric power system safety (in Polish). Przegląd Elektrotechniczny 10, s. 982-985, 2004.
10. Commission Decision of 4th February 2005 concerning the adoption of the Programme of Work 2005 for the Preparatory Action in the field of Security Research. C(2005) 259, Brussels, 18.01.2005.
11. Critical Infrastructure Protection in the fight against terrorism. Communication from the Commission to the Council and the European Parliament. COM(2004) 702 final, Brussels, 20.10.2004.
12. Guidelines for Analyzing and Managing Vulnerabilities of Fixed Chemical Sites. New York, Center for the Chemical Process Safety of the American Institute of Chemical Engineers, 2003.
13. Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures. A report of the Scientific and Technical Council of the International Risk Governance Council (Draft). Geneva, Switzerland, September 2005.
14. On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research, Towards a programme to advance European security through Research and Technology. COM (2004) 72 final, Brussels, 3.02.2004.
15. Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research. Luxembourg, Office for Official Publications of the European Communities, 2004.