Transactions of the VSB - Technical university of Ostrava Vol. VI, No. 2, 2011
Safety Engineering Series, ISSN 1805-3238 pp. 56 - 60, DOI 10.35182/tses-2011-0019

PROTECTION OF THE NATIONAL CRITICAL INFRASTRUCTURE

Libor HADÁČEK[1], Radomír ŠČUREK[2], Jaroslav CÍGLER[3]

Review article

Abstract: Several critical infrastructures have been identified in the Czech Republic that when disturbed or destroyed, they would impact on the performance of the state's functions. Failure of any such infrastructure could cause a failure of critical infrastructure in another Member State or Member States. Considering this international proportion, an integrated approach of the whole EU has been chosen to identify weaknesses, vulnerable points and gaps in protective measures. The goal of every EU member state is to protect entities and elements of critical infrastructure, prevent their disruption or their destruction, and minimize the impacts of possible failures of such infrastructures on the national and regional levels (Explanatory Memorandum, 2000).

Keywords: Infrastructure, management, plan, critical, protection.

Introduction

The issue of critical infrastructure has been once again greatly discussed in recent years. Nevertheless, the topic is not completely new. The term itself, in the least, has been used in the vocabulary of security theories and practices for more than 10 years. The fact, however, is that its substance was and to some extent still is understood quite loosely.

Not even the European Union Council Directive (Council Directive, 2008) (hereinafter the Directive) has succeeded in bringing a clear order into this field. Critical infrastructure is defined as - assets, systems and parts thereof located in Member States which are essential for the maintenance of vital societal functions, health, safety, security or economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

European critical infrastructures (hereinafter ECIs) is defined as - CI located in Member States, the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure (Council Directive, 2008).

Materials and methods

The study materials used were obtained from public sources. Then, through analysis of such secondary documents, an answer was sought to the question of how to protect regional critical infrastructures. In order to do so, critical infrastructure (hereinafter CI), required terminology and defined planning documentation to implement measures to protect the critical infrastructure had to be identified. For the sake of clarity and simplicity, relations between the infrastructure and the documentation have been expressed in a graphic way.

Cross-cutting and sectoral criteria shall be defined through application of general methodologies of the security theory, i.e. analysis and classification of risks and treatment of risks (Government Regulation, 2010). A level of criticality as the fundamental component of risk (in addition to probability and vulnerability) is the key concept. Criticality expresses the severity of damage incurred by protected assets, impact of such damage on our ability to maintain continuity of societal functions, severity of deviations from society's functioning in standard situations, in particular in quality of governance and quality of life and cost of restoring the standard situation.

Criticality of damage incurred is established by the following cross-cutting criteria:

- criterion of casualties (assessed according to the potential number of dead or wounded);
- criterion of economic impact (assessed according to the severity of economic losses or impaired quality of products or services, including potential environmental impacts;
- criterion of public impact (assessed according to the impact on public trust, physical suffering and

[1] Czech Association of Security Managers, Prague, Czech Republic, hadacekl@fsc-ov.cz
[2] VŠB - Technical University of Ostrava, Faculty of safety Engineering, Ostrava, Czech Republic, radomir.scurek@vsb.cz
[3] Czech Association of Security Managers, Prague, Czech Republic, ciglerj@fsc-ov.cz

impairment of daily life, including loss of essential services.

The system approach towards security from an all-society point of view (in this case from the point of view of a supranational community) is based on understanding the society as a structure of elements (in this case of subsystems) with a network of relations (cooperation; hierarchy; cumulative synergies) among them and developing in time. CI and ECI sectoral criteria are the representation of this understanding. It should be noted here that there are partial differences between sectoral criteria as applied by the EU and by the Czech Republic.

The law includes the critical infrastructure protection into the system of crisis management defined as a complex of management activities by responsible authorities analyzing and assessing security risks, planning, organization, implementation and control of activities executed in connection to crisis situation resolution. (Act, 2000) (hereinafter the Crisis Act). The Crisis Act further defines the following basic terms and concepts:

a) critical infrastructure as a system of elements, the disruption or failure of which would have a serious impact on the state's security, provision of necessities to its population or on its economy;

b) European critical infrastructure as a critical infrastructure on the territory of the Czech Republic, the disruption or failure of which would have a serious impact on another EU member state;

c) critical infrastructure element means in particular a building, facility, asset or technical infrastructure, the disruption of which would cause the critical infrastructure to fail;

d) critical infrastructure entity means a legal person or self-employed individual operating the element or otherwise responsible for functionality of critical infrastructure; if the element does not have an operator, the owner of the element becomes the critical infrastructure entity; in case of the European critical infrastructure, such entity is considered an European critical infrastructure entity, this includes authorities of state administration or government departments (organizational components of state) operating the element or otherwise responsible for functionality of critical infrastructure;

e) critical infrastructure protection pursuant to the Crisis Act means activities aiming to reduce the risk of disruption or failure of a critical infrastructure element.

Results

If the protection of state's critical infrastructure falls under the Crisis Act and becomes part of the crisis management system that includes regional authorities and other authorities with territorial competencies among entities of the crisis management system, then it would be logical, based on the above, to define critical infrastructure also on these levels, in particular on the level of regions, taking into account potential synergies and cumulative effects should the elements be disrupted from the point of view of regions (Říha, 2007).

The following Fig. 1 shows concentrated intersections of sets of CI categories and planning and security documents of CI protection.

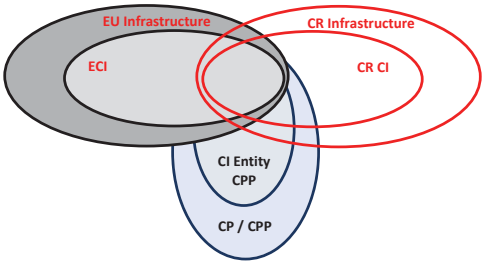
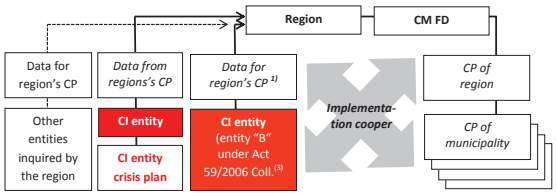


Fig. 1 The Crisis Preparedness Plan for Critical Infrastructure (hereinafter referred to as CPP CI)

Pursuant to the Crisis Act, in particular pursuant to § 29 (a) and (b), legal entities and self-employed individuals shall prepare a defined planning documentation and provide for implementation of CI protection measures (Act, 2000).

The entities identified are obliged to adopt all essential measures to prevent major accidents caused by dangerous chemical substances or chemical preparations (Act, 2006). In addition, the entities have certain obligations when it comes to providing some services (e.g. supply of energy, gas, urgent health care etc.).

A simple representation of the most significant relations in crisis planning is provided in the Fig. 2.



Legend:
CM FD = Crisis Management of the Fire Department
CP = Crisis Plan

Fig. 2 The region crisis plan development

Crisis plan structure has been defined in the Act and regulations to implement the Act as follows:

a) General section, containing in particular the following:
   - Specification of the scope of activities by a legal person or self-employed individual, and the tasks and measures that are subject to crisis preparedness plan;
   - Specification of crisis management;
   - Overview and assessment of possible risk sources in the risk analysis, and possible impact of such risks on the activities by a legal person or self-employed individual;
   - List of critical infrastructure elements;
   - Identification of possible threats to operation of critical infrastructure elements.

b) Operational part, containing in particular the following:
   - Overview of measures pursuant to the crisis plan of a responsible crisis management authority, and methods of implementation;
   - Ways to provide for ability and capability of legal entities or self-employed individuals to implement crisis measures and protect its operations, including defined protective measures - this part regarding the ability and capability to implement crisis measures is an analogy to preparation of an Operator security plan (Council Directive, 2008). It includes in particular the following:
     i. Conclusions of the threat and risk analysis;
     ii. Permanent (regular) security measures:
        - Technical security systems (Mechanical barriers, Alarm, security and emergency systems, Closed-circuit television, Access control systems);
        - Physical security guards;
        - Communications security;
        - Cybernetic security;
        - Administrative security;
        - Personnel security;
        - Critical infrastructure protection management;
     iii. Graduated (enhanced) security measures corresponding to the security situation developments;
     iv. Description of the system the for verification of security measures and their functionality, and training:
        - Procedures to solve crisis situations identified in the risk analysis;
        - Planned measures of economic mobilization for the suppliers of mobilization deliveries;
        - Contacts of responsible crisis management authorities;
        - Overview of plans prepared according to special legal rules and regulations that can be used in crisis resolution.

c) auxiliary part, containing in particular the following:
   - List of legal rules and regulations that can be used when preparing for an emergency or crisis and their resolution;
   - List of treaties and agreements signed to implement measures pursuant to the crisis preparedness plan;
   - Principles of manipulation with the crisis preparedness plan;
   - Maps and other graphics;
   - Other documents related to an emergency or crisis preparedness and resolution (Government Regulation, 2000).

The operative part of the Crisis Preparedness Plan for Critical Infrastructure Facilities, which is a potential part of the operator's Security Plan (Guideline, 2008), is directed at protection of health, lives, property and natural environment of the legal or physical entity (Act 2006). The optimum approach for ensuring protection of critical infrastructure is to consider both the current security of technologies and the way of protecting them (Genserik, 2010). The primary steps for implementing an appropriate level of security measures for a facility is essential to establish the current level of measures in place and to compile an analysis of threats to security and risks of physical protection. An independent part of the security analysis is an analysis according to the ISO ČSN 27000 standards.

For the effective management of security risks it is essential to analyse the security threats and risks which could have a negative impact on the protected assets. Various qualitative and quantitative methods of technical reliability analysis can be used to compile an analysis, such as the methods specified in ČSN IEC 60300-3-1 Reliability Management - Part 3-1: Instructions for Use of a Technical Reliability Analysis - Systematic Instructions. In security analyses, technical analyses thereby take the place of an as yet not issued single methodology for analysis of threats and risks. The European Commission expects that this will be created. Evaluation the threats to and vulnerable aspects of the critical infrastructure can be made using descriptive methods or else software applications for verifying their function as part of

risk management (Yusta, 2011). This will be based on evaluation of serious threat scenarios, the types of vulnerability of the separate facilities and possible impacts (Guideline, 2008).

These scenarios can include the place and method of attack, a description of the type of attacker, possible consequences of such an attack etc. The severity of separate scenarios must be evaluated in connection with the risk map for the asset in question. The conclusions of the security analysis are used for categorising the assets, security zoning and plans for the physical protection of separate security zones.

The aim of physical protection system is to prevent access of unauthorised persons to a protected asset inside the security zone. This is achieved by introduction of a physical protection system, which is a combination of systems of technical security, regime measures and physical protection, which are divided into permanent and graduated security measures.

The permanent security measures are those measures whose use is justifiable at all times. Depending on the type of security zone, it may be possible to install some type of technical security system (TSS) on the perimeter:

a) mechanical barrier equipment (MBE),

b) security and emergency alarm system (SEAS),

c) entry check system,

d) CCTV system,

e) Security lighting,

f) Electric fire alarm (EFA).

The physical protection system of the facility includes physical security. Physical protection means the system of organisational, regime and technical measures and physical security preventing access of unauthorised persons to the protected asset.

The interrelations between elements of physical protection are specified in regime measures, which are laid down by facility owner's management regulations and documents, comprising regimes for movement of persons and vehicles in the facility, manipulation with assets, use and manipulation of identification features and maintenance activities, checking systems, training and measures for exceptional events and crisis situations.

Interrelations between separate measures, their levels and security zones can be illustrated in the "Physical Protection Standard". Specific measures are suitable for each security zone. Their type and technical specification reflect the level of measure, i.e. its quality. An example of this standard appears in Fig. 3.

PHYSICAL PROTECTION STANDARDS Brief overview of all physical protection measures			Security Zones			
Measure	Type	Technical Specification	I.	II.	III.	IV.
	type 2		P	P		
	type 1				P	P
	type 3		P			
	type 2			P		
	type 1				P	P
	type 3		P			
	type 2			P		
Key:	Especially Secure Zone	Secure Zone	Protected Zone	Checking Zone		

Fig. 3 Example for compilation of Physical Protection Standard - Permanent Measures

Varying grades of security measures can be activated according to various degrees and risks. These are the measures gradually graded in time, which can be implemented at the specific asset for ensuring protection. In view of the short reaction period, their implementation is possible in the areas of physical protection and technical protection systems.

The graded measures are applied to the current system of technical and physical protection according to developments in the security situation. A sample of an overview of graded security measures appears in Fig. 4.

Physical Protection Standard			Security Zones			
S.no.	Graded Physical Protection Measures		I.	II.	III.	IV.
1						
2						
3						
...						
Graded TPS Measures			Security Zones			
S.no.	Location		I.	II.	III.	IV.
...	perimeter - MBE	Mobile fencing				
		Surface or spatial retarders				
		portable barriers restricting free vehicle entry				
...	Wireless SEAS					
Key:	Normal situation	Increased risk situation	High-risk situation	Actual risk situation		

Fig. 4 Example for compilation of Physical Protection Standard - Graded Measures

Compiling a physical protection standard for a facility and implementing it is a precondition for building an effective physical protection system which will satisfy requirements for protection of health, life, property and environment laid down by valid legislation and technical standards. The standard optimises protection management and links preventative measures with crisis measures in one package (Loveček, 2010).

Conclusion

In general, the framework of critical infrastructure protection, based from a legal perspective on the amended Crisis Act and related rules and regulations, including regulations to implement such rules and regulations, is a step ahead. At the same time it should be noted that in many aspects this solution is a compromise and does not fully meet the needs of all stakeholders (regional authorities in particular). In addition, the relations between the lines of preparation for resolution of military crises and lines of civilian crisis management have not been fully resolved in a satisfactory manner (in particular when it comes to process intersections, as expressed by the terms "facilities important for protection of the state" and "facilities targeted by a potential attack"). Security specifics of the global environment, including anticipated possible forms of military attack (micro battlegrounds), have been at least blurring the interface between these traditional lines of crisis management.

The resulting situation can be seen as an essential qualitative advance but needs to be developed further. The "regional critical infrastructure" is among the issues to be contemplated from the points of view of the state, as well as of crisis management. On a regional level, it is a source of unanswered and in essence unanswerable practical questions.

The first steps to resolve such issues are to consistently meet all the requirements resulting from the current legal framework, to detect unclarities and gaps when it comes to issues raised and regulated, and to formulate requirements as to the further development of legal rules and regulations in this area.

Acknowledgements

The article is connected to a research, development and innovation project called "Objectification of Threats and Risks of Equipments for the Production and Transmission of Electricity", identification code VF20112013019. Project funding has been provided by the Ministry of Interior of the Czech Republic as part of its program "Security Research for the Needs of the State 2010-2015".

References

Act No. 59/2006 Coll., concerning prevention of major accidents caused by selected dangerous chemical substances or chemical preparations.

Act No. 240/2000 Coll., on crisis management and on amendment to certain Acts (the Crisis Act).

Council Directive 2008/114/EC - on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Explanatory Memorandum (2000) to the Draft Act No. 240/2000 Coll., on crisis management and on amendment to certain Acts (the Crisis Act), as amended.

GENSERIK, R., INGE, D. A. (2010). Framework for the Integration of Safety and Security in case of Critical Infrastructure Protection. Disaster Advances, 2010, Volume 3, Issue 4, Pages 4-12. ISSN 0974-262X.

Government Regulation No. 432/2010 Coll., on the criteria for determining the element of critical infrastructure.

Government Regulation No. 462/2000 Coll., for implementation of Section 27(8) and Section 28(5) of Act No. 240/2000 Coll., on crisis management and amendments to certain acts.

LOVECEK, T., RISTVEJ, J., SIMAK, L. (2010). Critical Infrastructure Protection Systems Effectiveness Evaluation. Journal Of Homeland Security And Emergency Management, 2010, Volume 7, Issue 1, Article Number 34. ISSN 1547-7355.

ŘÍHA, Josef (2007). Kritická infrastruktura a riziko mimořádné události [online]. *Urbanismus a územní rozvoj*, Brno, 2007, Volume X, Issue 4, Pages 44-51 [cit. 2011-09-30]. Available from: http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf.

YUSTA, J.M., CORREA, G.J., LACAL-ARANTEGUI, R. (2011). Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy, 2011, Volume 39, Issue 10, Pages 6100-6119. ISSN 0301-4215. DOI: 10.1016/j.enpol.2011.07.010.