CHEMICAL ENGINEERING TRANSACTIONS
VOL. 48, 2016
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.aidic.it/cet
Guest Editors: Eddy de Rademaeker, Peter Schmelzer

ISBN 978-88-95608-39-6; **ISSN** 2283-9216
DOI: 10.3303/CET1648158

European Critical Infrastructure Risk and Safety Management: Directive Implementation in Practice

David Rehak[a], Martin Hromada*[b], Petr Novotny[a]

[a]VSB-Technical University of Ostrava, Faculty of Safety Engineering, Lumirova 13, Ostrava -Vyskovice, 700 30, Czech Republic
[b] Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stranemi 4511, Zlín, 760 05, Czech Republic
hromada@fai.utb.cz

Critical Infrastructure Protection began to be actively addressed in Europe in 2005, when the European Union issued a Call for a European Programme for Critical Infrastructure Protection (further only CIP) that first drew attention to the fact that several sectors and their elements were significant for today´s society - and that their failure could have serious impacts on national security, the economy, public administration and the basic vital functions of member states´ populations. Three years later, the EC issued European Council Directive 2008/114/EC, which requires Member States to identify the European Critical Infrastructure Elements (further only CI).
Based on the above, the paper deals with risk assessment process in context of CI protection and resilience in the Czech Republic. Paper presents the practical conclusions resulting from the obligations of this Directive´s implementation in connection with the Czech legal environment and CI. Due to the fact that the Czech Republic - as one of the few member states of the European Union that has identified European CI in its territories, discusses practical approaches to the protection and resilience of these elements. These approaches are addressed in relation to Risk and Safety Management from the perspective of the application and implementation of deliverable outputs resulting from Security Research. In this context, selected methodologies that optimise Risk and Safety/Security Management are also presented, which fulfil the requirements for CI´s crisis-preparedness plans as equivalents to an Operator Security Plan. Practical benefit of this paper is seen through the real implementation of public-private-partnership into the risk assessment process and CIP which is discussed in the following text.

1. Introduction

The beginnings of the establishment of CIP in the European Union date back to 2004, when the European Commission adopted a Communication entitled: “Critical Infrastructure Protection in the fight against Terrorism” (COM, 2004). The following year, the Commission produced a Green Paper on a European Programme for Critical Infrastructure Protection (COM, 2005), but it has been criticized extensively by Member States. On the basis of its critics, the material was revised and approved in 2006 by the European Commission as a European Programme for Critical Infrastructure Protection (COM, 2006). An important milestone in European CIP was 2008, when the European Council issued its Directive on the Identification and Designation of European Critical Infrastructures and an assessment of the need to improve their protection (Council Directive, 2008). In the following years, CIP issues were implemented into the national laws of the Member States, and then further elaborated. Attention was paid to Safety/Security and Risk Management with a focus on practical approaches to the protection of CIs.

2. Critical infrastructure protection in the Czech Republic

The CIP issues in the Czech Republic were implemented into the Crisis Management field. In response to the European Council Directive (Council Directive, 2008) in 2010, an amendment was made to the Crisis Act (Act, 2000), which thus defines the rights and duties of those authorities involved in preparing for emergencies, their management, and the protection of critical infrastructures. The issue of identifying CI are

Please cite this article as: Rehak D., Hromada M., Novotny P., 2016, European critical infrastructure risk and safety management, Chemical Engineering Transactions, 48, 943-948 DOI:10.3303/CET1648158

addressed by government regulation (Government Decree 432, 2010), which sets out the criteria for determining the national elements of the critical infrastructure. CI protection is dealt with by government regulation (Government Decree 431, 2010), which sets out the requirements - and how to handle the Critical Infrastructure Subject Emergency Preparedness Plan.
CIP - according to the Crisis Act (Act, 2000) refers to measures aimed at disrupting the function risk minimization of CIs. Responsibility for CI protection refers to a Critical Infrastructure Subject – where, to this end, there is a mandatory requirement to: (1) develop a Critical Infrastructure Subject Crisis Preparedness Plan (further only CISCPP), (2) appoint a Security Liaison employee, and (3) allow the competent ministry or another central right authority to carry out inspections of the CISCPP and CI protection.
The Critical Infrastructure Subject in the preparation of a Crisis Preparedness Plan (CPP) is to be discussed with the relevant Ministry - or the Czech National Bank; the range of the CPP is then reprocessed with reference to their comments as well as the possible CI threats to the functions and measures for their protection.
Another mandatory aspect of the CI is to determine the "Security Liaison Employee" (i.e. or SLO Security Liaison Officer) (Act, 2000), who provides for the Critical Infrastructure Subject synergies being carried out under the Crisis Act, and who meets the professional competence requirements by completing university studies in an appropriately accredited study program – providing a comprehensive knowledge of Security to the Czech Republic, to Public Protection or to Crisis Management – or has at least three years working practice in one of these areas.

3. Methodology for selected CIs System Resilience Element Evaluation

The methodology´s aim is to create a comprehensive assessment system using a mathematical model to determine the relationship and values of individual CI indicators (Hromada and Lukas, 2015). CI resilience reflects the extent to which a given entity is able to ensure functions in terms of external and internal factors´ negative effects. The aim of Resilience Self-evaluation should be to determine the CI resistance time to any negative factors. The resulting Resilience Parameter should be determined quantitatively. Due to developments in the Resilience Assessing Method concept: Qualitative Assessment of CI Resilience was used. Qualitative Assessment does not establish a specific time period during which the element will be able to resist; while, on the other hand, allowing Resilience Assessment by determining the level of its preparedness to ensure the given function.
Assessment Disclosure is based on the assumption that the CI which is most threatened must take immediate measures to ensure its resilience through a wider range of measures. It is not just the direct threat to these elements by negative factors; but its Dependence Assessment also concerns other elements by means of a Correlation Assessment. Resilience to the so-called "Domino Effect" also plays a key role in Chain Character Systems. This is especially related to selected supply chain types. In the assessment process, the impact of the negative factor is expressed by the Risk and Dependence Impact and by the Correlation Coefficient. On the other hand, in terms of the Resilience Coefficient, the counterpart represents Structural Robustness, Security Robustness and the Preparedness Coefficient (see Eq. 1):

$$R_E = f\left(C_{RI}, C_C, C_{RO}, C_P\right) \tag{1}$$

Where, R_E = Critical Infrastructure Resilience; C_{RI} = Risk Coefficient; C_C = Correlation Coefficient; C_{RO} = Robustness Coefficient; C_P = Preparedness Coefficient.

The Risk Coefficient – C_{RI}; expresses the potential risk impact on CI functionality. If the potential effect is significant, it will be necessary to minimise this likelihood through the fulfilment of measures.
The Correlation Coefficient – $C_{C;}$ expresses the assessment element function dependence on other elements:- mainly energy supplies, raw materials, data, etc. These elements should reckon with outages and take into account appropriate preparedness aspects.
The Structural Robustness Coefficient – C_{RO}; expresses the ability to assess elements´ abilities to resist negative effects expressed through the Robustness Coefficient – which reflects the element´s ability to withstand negative effects due to their structure, system properties and the technology used. Security Robustness Security reflects the breadth and depth of measures ensuring security against negative effects. These are usually measures like: Physical, Informational, Fire, Personnel and Administrative Security, etc.
The Preparedness Coefficient – C_P; expresses an element´s capability to ensure a response to the occurrence of Emergency/Security incidents and to restore the desired CI functions. In case of function degradation, the element must have appropriate supplies to ensure its restoration.
The CI Resilience Self-evaluation should be based on Risk Analysis and Quality Extent Assessment Countermeasures for “Shared Risk Effect Elimination” or, for degraded function restoration: CI Resilience.

The evaluation process also includes the following phases: (a) A Systems Analysis of the evaluated CI; (b) Analysis and Risk Assessment; (c) A Security/Safety Evaluated Areas Determination; (d) The Attributes and Indicators Determination Calculation; (e) The CI Resilience Calculation; and (f) A CI Resilience Assessment. This sequence of steps using mathematical models enables the quantitative expression of Resistance Parameters as well as the quantitative description of System Values Resistance. In view of the extensiveness of the mathematical model, we shall not go into further detail. (Hromada et al., 2014)
The methodology presented herein, discussed the status and importance of Critical Infrastructure Resilience in relation to ensuring its operational continuity and – thus, the functional continuity of societies. This approach allows a broader perception and Critical Infrastructure Protection status within the framework of Critical Infrastructure Sustainability and Functionality.

4. A methodology for ensuring the protection of CIs in the production, transmission and distribution of electricity

The aim of this methodology (Deloitte Advisory, 2012) is to support the development and improvement of selected areas´ Critical Infrastructure Protection Management Systems. The methodology is intended for practical use by Critical Infrastructure Operators. The Protection Management System relates to security areas that reflect the Risk Analysis methodology implementation process - including the outputs and outcomes resulting from the pilot application and verification of the Protection Management System for a pre-selected location. Standards are parts of the methodology, developed and tested for:

- Ensuring the Critical Infrastructure Physical Security System in the: Generation, Transmission and Distribution of Electricity
- Ensuring Information Security in Information Systems that Support the Generation, Transmission and Distribution of Electricity
- Ensuring Administrative and Personnel Safety
- Ensuring Critical Infrastructure Crisis Management Systems

In order to optimize the Critical Infrastructure Protection System (CIPS) development process in the selected area as determined by a general description of the individual development process (see Figure 1): Where: (1) Is a Critical Infrastructure Assets Classification and Evaluation; (2) A Threats and Risks Definition Catalogue; (3) An Analysis and Risk Assessment; (4) A Security Measures Determination Catalogue – Including categorisation and parameters; (5) A Critical Infrastructure Protection Management System determination of design requirements; (6) A pilot application and verification of the suggested CIP management system at the selected location; (7) The Pilot Application and Methodology Adjustment Assessment; and (8) The Critical Infrastructure Protection Management System´s documentation development.

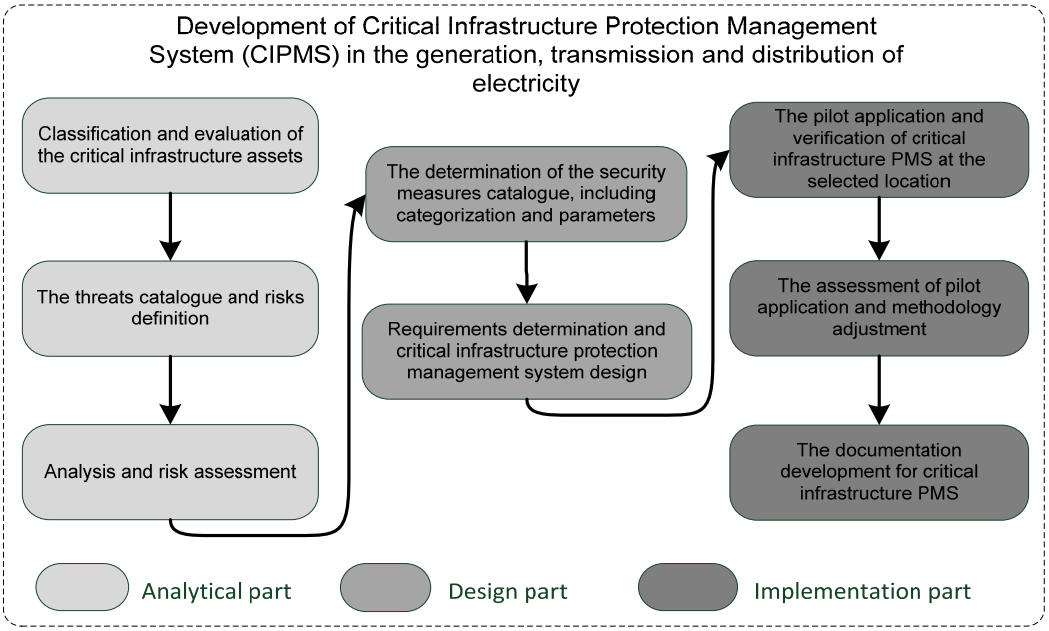

Figure 1: Description of the Protection Management System Development Process (Deloitte Advisory, 2012)

In connection with the Risk Analysis and Assessment Implementation process, the assets relating to a selected Critical Infrastructure area in an extension of the Crisis Law, have been defined and categorised (Act, 2000) and the Government Decree on Criteria for (the) Identification and Designation of Critical Infrastructure Elements (Government Decree 432, 2010).
The design and optimisation of a selected Critical Infrastructure Area Protection Management System (CIAPMS) is conditioned by the Threat Analysis and Risk Assessment Process and the selection of the appropriate methodology. The following Risk Assessment Methodology is a Semi-quantitative Approach that works with these three risk components: (Asset, Threat, and Vulnerability); Where:

- Asset – Is a part of the system, or its data, with relevant value for a company.
- Threat – Any activity intentionally, or unintentionally using a vulnerability with a negative impact on the Confidentiality, Availability and Integrity of assets - expressed as a Threat Occurrence Probability.
- Vulnerability – The expression of an asset´s, or group of assets´, weak points - under certain assumptions resulting in a threat of injury or asset loss as well as any processes/functions that support these assets, will be used.

Table 1: Risk Component Assessment (Deloitte Advisory, 2012)

Numerical value	Asset value	Threat level	Level of vulnerability
0	none or no unrated	unlikely or unrated	none or no unrated
1	low	very unlikely	low
2	insignificant	unlikely	insignificant
3	middle	moderately likely	middle
4	high	very likely	high
5	very high	highly probable or certain	very high

In order to finalise the Risk Assessment Process in relation to selected Critical Infrastructure areas; Equation 2 was defined:

$$R = A \cdot T \cdot V \tag{2}$$

Where, R = Risk Level; A = Asset Value; T = Threat Level; V = Vulnerability Level.

After the determination of the risk components, it is possible to quantify the risk value and the resulting value is divided into groups reflecting the increasing level of risk. To be able to express the risk level, the following categories were identified: *1-40* Low Risk; *41-70* Intermediate Risk, *71-125* High Risk.
For the next step in the risk analysis and the determination of the protection management system process, it is important to express the correlation between the identified risks. For this purpose, the KARS Methodology was used (Pacinda, 2010), which - through their correlation, enables the Risk Quantitative Analysis. The importance of this method is seen especially in the context of risk diversification based on the level of risks´ activity or passivity in relation to other risks (i.e. whether the selected risk has the potential to cause other risks; or whether it may be caused by other risks – the Domino Effect). The KARS implementation process analysis is a multi-step process where - in the first step, an inventory of risks is defined, that is to say, those specific for the electricity generation, transmission and distribution areas), and the Correlations Assessment is performed (see Table 2).

Table 2: Correlations Assessment Table (Deloitte Advisory, 2012)

	Index	1	2	3
Index	Risk	High temperature	Lightning	Tree fall
1	High temperature		1	0
2	Lightning	0		1
3	Tree fall	0	0	

To express the relationships between the risks, the Risk Correlation Table is filled with values where:
1 – Is the real possibility that Risk Ri may cause Risk Rj
0 – Expresses a condition where there is no real possibility that Risk Ri may cause Risk Rj

The next step is to express the above-mentioned activity - which reflects the overall risk potential to cause additional risks; or whose passivity expressions indicate a number of risks which may cause the risk. Equations (3) and (4) are used for the calculation of the coefficients.

$$K_A R_i = \frac{\sum_{i=1}^{x} R_i}{x-1} \quad (3) \qquad K_P R_i = \frac{\sum_{i=1}^{x} R_i}{x-1} \quad (4)$$

Where, $K_A R_i$ = the Activity Coefficient of i-th Risk; $K_P R_i$ = the Passivity Coefficient of i-th Risk; $\sum R_i$ = the Sum of the Risk; and x = the Total Amount of Risks.

The last step of the analytical part of the Protection Management Systems development process is the Assessed Risks Prioritisation. In this step, the assessed risks are divided into the following four segments according to their significance: (1) Primary Significant Risks, (2) Secondary Significant Risks and (3) Tertiary Significant Risks. In line with the Pareto Rule (Koch, 2008), it is assumed that the first segment will have 80 % of the most significant risks. In this part of the process, Criteria Risk Analysis of Facilities for Electricity Generation and Transmission (Rehak et al., 2014) or Preferences Risk Assessment of Electric Power Critical Infrastructure (Rehak and Senovsky, 2014) can also be used.

In the following part of the process, attention is paid to the Critical Infrastructure Protection Management System (CIPMS), which connects the various security areas into a managed deployment process that improves measures aimed at protecting the assets of a pre-defined Critical Infrastructure area. The CIPMS is designed according to the PDCA (Plan-Do-Check-Act) continuous process. Inputs are individual requirements defined by the CIPMS´ areas of interest. The output is a continuous CIPMS in selected security areas or other areas that will be later included in the CIPMS. The individual steps of the CIPMS can be depicted as a continuous cycle (see Figure 2).

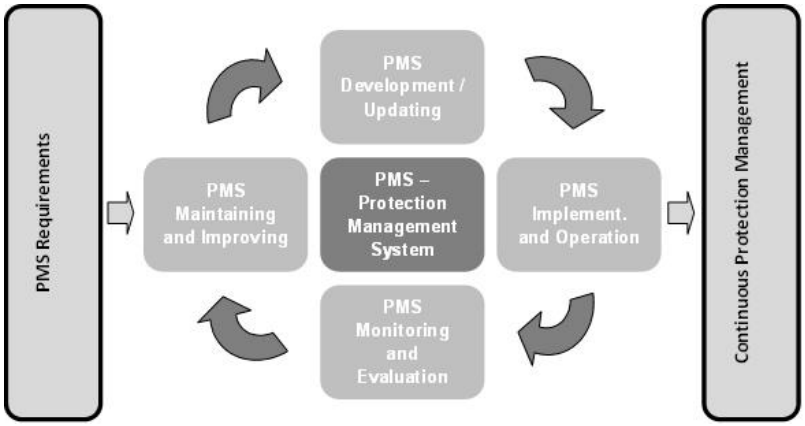

Figure 2: Graphical Representation of the CIPMS Continuous Cycle (Deloitte Advisory, 2012)

Due to the different needs and conditions of individual subjects, it is necessary to clarify and consequently perform a differential analysis of the current and proposed states of identified safety/security areas. The results of the Difference Analysis are inputs for the subsequent steps of the CIPMS process. The activities that should be implemented step-by-step in the CIPMS process are presented in Table 3.

Table 3: Setting Requirements for the CIPMS (Deloitte Advisory, 2012)

PMS phases	Description of continuous cycle
Plan - Create	The Security Manager should - in cooperation with the responsible employees, make regular planning for protective measures, their implementation, and regular internal and independent controls and other activities in the field of security. A schedule should be established and capacity should be allocated that will enable one to implement the planned activities
Do - Implementation and operation	In cooperation with System Administrators, Physical Protection Staff, the Administrator or Deputy of Administrative Security and other selected persons responsible for security should implement and operate those security measures for which these managers are responsible
Check - Monitoring and evaluation	Control Measures should take place – not only at the Security Events Assessment level in these areas, but also directly by individual measures setting controls in relation to their projections to their success in the prevention and detection of security incidents
Act - Maintenance	Based on the findings gained through regular monitoring and assessment of the CIPMS - including the consideration of the current situation in the legislative area and other security requirements, it will be necessary to be ready to modify the current requirements / update the CIPMS in all selected areas.

The PDCA Cycle should not be regarded only as a summary stage for all security areas´ progress during the selected period but - if it is possible, to also simultaneously monitor multiple cycles in different security areas, or even by means of individual measures, because deploying measures does not usually take place simultaneously for all measures in all areas, but rather - during the year, according to the needs and possibilities of individual entities.
The methodology presented here is an integrated approach, in relation to the comprehensive definition and the structural and qualitative requirements definition of selected safety and security aspects in relation to the needs of the selected critical infrastructure area.

5. Conclusions

The Czech Republic's approach to CIP can be assessed as very active and responsible. This is evidenced among other things by the fact that the Czech Republic is one of the few member states of the European Union that has identified European CIs on its territory. Subsequently, the Czech Republic has focused its attentions in the Safety/Security and Risk Management areas, with relation to practical approaches to CI protection development. These issues were addressed - among others, by means of National Security Research, whose results include: (1) A methodology for selected CIs and System Resilience Evaluation elements; and (2) A methodology to ensure Critical Infrastructure Protection in the generation, transmission and distribution of electricity. By applying these methodologies in practice, the Czech Republic has optimized its management of Safety/Security and Risks of national and European critical infrastructure elements. In addition, the requirements for a Critical Infrastructure Subject’s crisis preparedness are also fulfilled.

Acknowledgments

This article was elaborated within the Ministry of the Interior of the Czech Republic project, filed under: VI20152019049; entitled: ‘Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems’.

Reference

Act 240/2000 of 28 June 2000 on Crisis Management.
COM/2004/0702. Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the Fight against Terrorism.
COM/2005/576. Green Paper on a European Programme for Critical Infrastructure Protection, Commission of the European Communities.
COM/2006/0786. Communication from the Commission on a European Programme for Critical Infrastructure Protection.
Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
Deloitte Advisory, 2012. Methodology to ensure of critical infrastructure protection in the area of electricity generation, transmission and distribution. Deloitte Advisory, Prague, Czech Republic. (in Czech)
Government Decree 431/2010 of 22 December 2010 amending Government Decree 462/2000 to implement §27 and §28 of the Act 240/2000 on Crisis Management. (in Czech)
Government Decree 432/2010 of 22 December 2010 on criteria for determination of the critical infrastructure element. (in Czech)
Hromada M. et al., 2014, System and the approach to critical infrastructure resilience evaluation. SPBI, Ostrava, Czech Republic. (in Czech)
Hromada M., Lukas L., 2015, Methodology for selected critical infrastructure elements and elements system resilience evaluation, In Proceedings of The 2015 IEEE Symposium on Technologies for Homeland Security, held 14 - 16 April in Greater Boston, Massachusetts.
Koch R., 2008, The 80/20 Principle: The Secret to Achieving More with Less. Crown Publishing Group, London, United Kingdom.
Pacinda S., 2010, Network Analysis and KARS, The Science for Population Protection, 2(1), 75-96. (in Czech)
Rehak D., Senovsky P., 2014, Preference Risk Assessment of Electric Power Critical Infrastructure, Chemical Engineering Transactions, 36, 469-474, DOI: 10.3303/CET1436079
Rehak D., Danihelka P., Bernatik A., 2014, Criteria Risk Analysis of Facilities for Electricity Generation and Transmission. In Steenbergen et al. (eds). Safety, Reliability and Risk Analysis: Beyond the Horizon (ESREL 2013), 2073-2080.