ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA BEZPEČNOSTNÉHO INŽINIERSTVA
KRÍZOVÝ MANAŽMENT - 1/2017
ISSN:1336 - 0019
str. 46-52

BUSINESS CONTINUITY PLAN IN ENTITIES OF CRITICAL INFRASTRUCTURE

PLÁN NA ZABEZPEČENIE KONTINUITY PREVÁDZKY V SUBJEKTOCH KRITICKEJ INFRAŠTRUKTÚRY

Zdeněk KOPECKÝ [1], Miroslav ŠPAČEK[2]

SUMMARY:

This article focuses on the use of process management tools and Business Continuity Management to ensure the security, integrity and functionality of critical infrastructure. This issue is the subject of the project of the Security Research of the Czech Republic No. VI20152018039. The project is based on a complex approach to the durability of critical infrastructure in regards to securing continuity of processes for entities and objects of the critical infrastructure in the crisis and emergency planning system of public administration in the Czech Republic.

KEYWORDS: *Business Continuity Management, Business Continuity Plan, Crisis Management, Critical Infrastructure, Process Management*

INTRODUCTION

The protection of critical infrastructure is currently one of the security phenomena, a topical subject of crisis management on both the international and national level. The basic terminology of critical infrastructure that has developed over time primarily arises from the European Council directive 2008/114/EC (hereinafter only 'Directive') [1] and from the Czech Republic Act No. 240/2000 Coll. (all legal regulations mentioned in this article are based upon the legal system of the Czech Republic). The definition stated in the Directive sees critical infrastructure as "*an asset, system or part thereof, located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, 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."*

According to the Directive, protection of critical infrastructure should focus on ensuring integrity and the continual function of critical infrastructure. The owners and operators of critical infrastructure are identified and according to legislature, certain requirements regarding its protection are placed upon them. However, from the perspective of a very significant position of the commercial sphere in protecting critical infrastructure, the priorities of companies must be merged with state requirements by methods that meet the criteria of purpose, effectiveness and efficiency on both sides. The starting points are the respective legislature, systemic approach and infrastructure protection process management using methods of quantitative management for process optimization to ensure its function and integrity. The Directive reflected during the amendment of the crisis act, where both cross-cutting and sectoral criteria for determining the elements of national critical infrastructure were established in the Czech Republic, is the government executive decree No. 432/2010:

The cross-section criterion for determining an element of critical infrastructure includes the aspect of

a) A number of victims with a boundary limit exceeding 250 dead or more than 2,500 victims being subsequently hospitalized longer than 24 hours,
b) An economic impact with a boundary limit of an economic loss to the state exceeding 0.5% of gross domestic product, or
c) An impact on the public with a boundary limit of an extensive limitation of providing necessary services or another serious impact on daily life affecting more than 125,000 people.

[1] Zdeněk Kopecký, Ing., Ph.D., University of Economics in Prague – The Institute of Crisis Management, e-mail: kopecky@vse.cz.
[2] Miroslav Špaček, Doc. Ing., PhD., MBA., University of Economics in Prague.

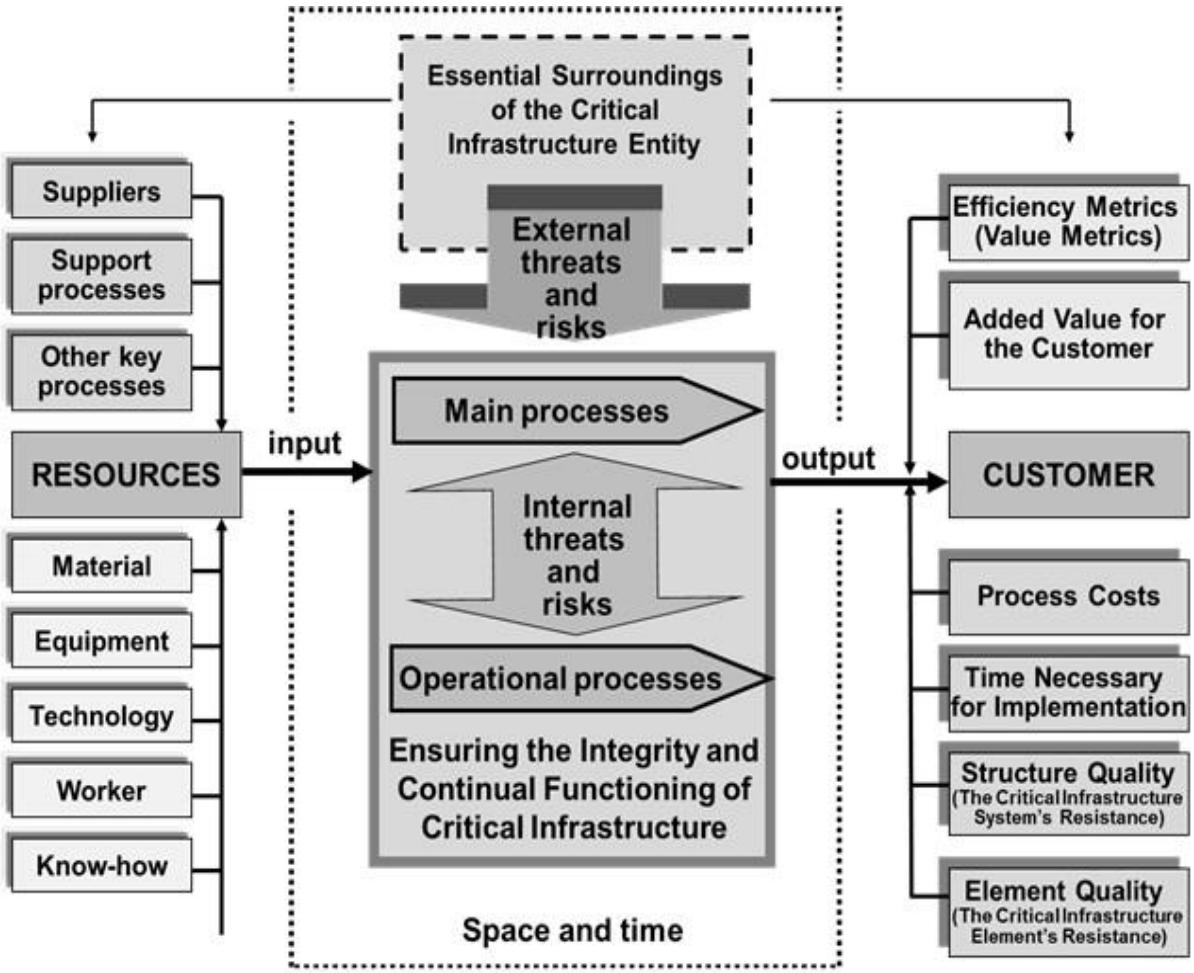

Figure 1. **Protection of critical infrastructure as a resource-conditioned process**

The sectoral criteria are established for the below listed fields of national critical infrastructure of the Czech Republic (also stipulating the scope and relation to the European critical infrastructure):

- *Power industry:* in national and European framework.
- *Water management:* in national and European framework.
- *Food industry and agriculture:* in national and European framework.
- *Health care:* in national and European framework.
- *Transportation:* the European framework with respect to different realities, also including sea and shoreline transportation.
- *Communication and information systems*: the national framework does not specifically mention protection of information systems and networks; the European framework does not include postal services.
- *Financial market and currency*: the national framework additionally includes the insurance industry.
- *Production of dangerous substances*: the European framework does not include biological materials.
- *Emergency services*: only within the national framework, not included in the European framework.
- *Public administration*: only within the national framework, not included in the European frameworks.
- *Space*: the national framework does not include this subject, but it is included in the European framework.
- *Science and research:* the national framework does not include this subject but is it is included in the European framework.

1. PROTECTING SECURITY AND FUNCTIONALITY OF CRITICAL INFRASTRUCTURE AS A PROCESS

Protecting the integrity, continual functionality and security of critical infrastructure should arise from a systemic approach to infrastructure as a system of elements and connection that is dynamic, adaptable and open (ties to its external environment) [2], [3]. Strengthening infrastructure as a system should therefore focus on its:

- *static aspects*, lying in the resistance of the individual elements and connections (particularly the critical ones), source redundancy (creating backups, supplies and reserves) and in the diversification of risk (spreading or possibly transposing the impacts of dysfunctional infrastructure onto multiple entities),
- *dynamic aspects*, lying in flexibility and adaptability (the ability to reconfigure) to new conditions in case of loss of function of a particular element or a connection, to ensure emergency provision of functionality of the infrastructure as a system and the subsequent recovery into a new and stable condition.

At the same time, the required protection of critical infrastructure (ensuring its continual functionality and integrity) should be understood as a process conditioned by resources, adding a value to the customer that in this case is the state, (although in the final sequence it is still the citizen). It is schematically shown in Figure 1.

This enables the implementation of Business Process Management – BPM[3] that, as a management branch, arises from clearly specified goals of an organization and hierarchy of processes to achieve them [4].

The goals of protecting the continual functionality and integrity of critical infrastructure must arise both from the 'state requirements'[4], and from the business strategy of the organization, and they should fulfill the attributes contained in the English abbreviation of SMART[5] in the sense of being:

- *Specific* – The goals in this case are clearly formulated, whether in legislation or in the related implementation documentation of crisis management of the public administration.
- *Measurable* – Measurability (quantification) is an important requirement particularly from the point of view of clear, ongoing and final control of the fulfilment of goals. However, at the moment the only quantification is the criteria for determining an element of critical infrastructure[6]. The quantification of the required level of protection (resistance) of the critical infrastructure in relation to the quantification of the individual potential threats (the risks of discontinuity) is missing.
- *Attainable (Agreed)* – (accepted upon mutual consent of the stakeholder parties) – The method of attainment should be established by crisis plans and plans of readiness of the critical infrastructure entity, as rational ways to achieve the goals, stipulating a clear answer to the questions of what and how (when, where, with which resources) should be accomplished for the protection of critical infrastructure.
- *Realistic* – The stipulated goals (from the state perspective) should also consider conditioning and related goals (including the business goals of the critical infrastructure entities). This is the systemic approach to protection of critical infrastructure entities in relation to their essential environment.
- *Properly Timed (Trackable)* – A time frame should be stipulated for achieving the goals and their fulfillment must be trackable over time, as the basic phenomena of their course.

The processes (of critical infrastructure protection) must be identified, specified and analyzed both on their own and in relation to their role in the hierarchy of processes within an organization (process maps), in relation to the hierarchy of goals, as well as to the corresponding management level for their streamlining or redesign. This should also reflect in the organizational structure[7], information support [5] and other support processes.

Unlike the function-oriented approach (typical for public administration), process management enables greater organizational

[3] For example VEBER, J. a kol.: Management, základy moderní manažerské přístupy výkonnost a prosperita. Management Press, 2009, ISBN 978-80-7261-200-0

[4] Security Strategy of the Czech Republic and legislature related to it.

[5] Specific, Measurable, Attainable (Agreed), Realistic,

[6] Government Decree No. 432/2010 Coll., Regarding the Criteria for Identifying an Element of Critical Infrastructure

[7] A project organizational structure within the existing hierarchy of competencies (responsibilities and authorities) or in case a higher flexibility is required, an interdisciplinary structure.

flexibility in solving risks and complex processes and, in the wider context, also improves their effectiveness and optimization, as in the case of maintaining functionality and integrity of critical infrastructure. Although, on the other hand, implementation of BPM into practice [5] poses greater demands on information support and changes in organizational structure and thus is a related subject of the human factor involved in these changes.

2. BUSINESS CONTINUITY PLAN AND ITS INTEGRATING ROLE IN ENSURING CRITICAL INFRASTRUCTURE FUNCTIONALITY

The most suitable method of implementing the systemic approach and process management into the practice of critical infrastructure protection from the point of view of the company management sphere is Business Continuity Management (BCM)[8]. BCM can be understood as the management of continuity of business processes (continuity of functioning of critical infrastructure) in relation to its operational risks[9] [4].

It is a systemic and integrated approach, ensuring sustainability of a company's activity (protecting the integrity and functionality of critical infrastructure). Considering the operational risk management, it only focuses on the individual factors of operational functioning and thus would be both too narrow and ineffective.

The subject of operational risk has two meanings in the commercial sphere [6]. We come across it in the financial analysis of a company where we recognize[10]:

- Financial risk – related to the degree of the ratio of external sources of financing from the overall resources. It arises from the composition of sources depending on the requirements regarding the sequence of payments,
- Operational risk - the degree of use of tangible fixed assets and thus related fixed costs and their ratio toward variable costs.

However, for the purposes of BCM (as well as for implementation in the area of protection of critical infrastructure), operational risk is understood as:

- Limitation or thwarting of business conduct due to internal influence (operational breakdowns, machine damage, strike, injuries, etc.),
- Limitation or thwarting of business conduct due to external sources (natural disasters, epidemics, terrorism, power supply shortages, disrupted transportation or power infrastructure, etc.)

The system of ensuring business continuity is a system of organizational, personnel, material, technical, financial and other measures for minimizing discontinuity and ensuring necessary resources (input), as well as sustaining conditions necessary for execution of business activities (for example in construction, maintenance and operation of critical infrastructure) during emergency and subsequent crisis situations.

The immediate goal for ensuring continuity is the longest possible retention of the business process. However, even here there is an expectation of a possible managed limitation or, from the perspective of recovery (revitalization), an acceptable interruption due to limitations of necessary resources in terms of their quantity, quality and functionality, in relation to space and time, in order to sustain the required functions at least to a minimal degree.

The basic tool of BCM is the Business Continuity Plan (BCP), as the output of the first sequential managerial function of BCM. BCP builds bridges between where we are (the current condition protection of infrastructure functionality) and where we want to go (the level of protection we intend to achieve).

The crisis legislation requires placing many duties upon the entities of commercial and economic sphere [6] (including entities of critical infrastructure) regarding planning and preparation for case of an emergency situation and, in particular, their solutions. These are specifically:

[8] BCM was originally and usually still is connected to maintaining and recovery of information technologies after their breakdown (Disaster Recovery). Currently there are attempts to use the BCM methodology in the area of public administration crisis management, such as Government Continuity Management (GCM).

[9] BCM deals with such risks that are not connected to the application of a product or services within a market, but with ensuring the conditions and 'sufficiency' of resources for their production. For example, in ERM (Enterprise Risk Management), an operational risk is considered a part of the organizational risk, which is then supplemented in the basic categorization from the point of view of creating a value by strategic and market risks.

[10] For example Grünwald, R. - Holečková, J. 1994. Finanční analýza a plánování podniku. VŠE Praha,

- Crisis readiness plan[11] (a plan of crisis readiness of a critical infrastructure entity),
- Economic mobilization measures plan[12], Internal emergency plan[13],
- Security program of prevention of serious emergency including a description of management system of safety within the business premises,
  Safety report (in basic structuring according to the respective regulation),
- Plan of physical protection.

Figure 2 shows the framework structure of BCP in relation to the system or emergency and crisis planning within public administration in the maximum scope[14].

[11] In accordance with the Act N. 240/2000 Coll. on Crisis Management and on amendments of certain acts (Crisis Act) as amended.

[12] Should the enterprise be subject to Economic Mobilization in accordance with the Act of the Czech Republic No. 241/2000 Coll., Regarding Economic Measures for Crisis Situations

[13] In accordance with the Act of the Czech Republic No. 224/2015 Coll., Regarding Prevention of Serious Emergencies Caused by Selected Chemical Substances or Chemical Agents (The Serious Emergencies Prevention Law)

[14] In case this is at the same time, for example, an entity subject to economic mobilization according to Czech Act N. 241/2000 Coll., or an enterprise listed in class A or B according to Act N. 224/2015 Coll.

All these plans touch upon one and the same reality seen from different points of view and thus also relate to different management and control authorities of public administration[15].

The reality, common to all plans, is on one hand formed by threats and risks and on the other hand by the capabilities of the given entity (it still has the same sources and abilities) to face the impacts of these threats. Additionally, everything that is required from the commercial and economic entities is primarily viewed from the point of view of the needs of public administration[16]. The fact that this partly also covers the interests of the enterprise, which is, of course, beneficial to the enterprise, is secondary.

As opposed to this, BCP primarily solves the interests and needs of the enterprise, although based on this, the company is also better prepared to fulfill the tasks required from it within crisis and emergency planning. It therefore makes sense, to an acceptable degree, to integrate[17] and thus also rationalize the system of planning commercial and economic entities (the critical infrastructure entities and their subjects) in relation to safety and operational threats of the given entity and its subjects (subjects of critical infrastructure).

Given the complex understanding of threats and discontinuity risks, BCP should become the basis for integrating the common parts (for example identification of threats, analysis of risks and processes, etc.) while the attachment part would specify the individual plans arising from the requirements of crisis and emergency planning.

[15] For example the Ministry of Interior of the Czech Republic, the Administration of State Material Reserves, The Ministry of Environment of the Czech Republic, regional offices, administrative offices in the segments of fire protection, population protection, as well as the Integrated Rescue System, the Czech Environmental Inspectorate, State Labor Inspection Office, regional hygienic stations, etc.

[16] For example a plan of crisis readiness deals with the readiness of a commercial and economic entities included in the crisis plan only within the scope of fulfilling what is required from them. Simply put, the state does not care, for example, about an operational emergency in a company that endangers fulfillment of business goals, but does not endanger health and lives of employees and does not affect the company's essential surroundings (from the perspective of the state).

[17] This regards, for example, information subject to Act No. 412/2005 Coll., on Protection of Classified Information and regarding personnel security, or information having the character of Exceptional Matters according to Act N. 240/2000 Coll., on Crisis Management.

The amendment of Act No. 240/2000 Coll. already covers the possibility of rational integration of existing planning, organizational and technical documentation that the entity of critical infrastructure already processes within their public-administration related duties.

CONCLUSION

Given the current security threats, ensuring protection of critical infrastructure is a necessary part of fulfilling the basic functions of the state.

Commercial and economic entities must both comply with their processes of ensuring protection criteria of purpose, effectiveness and efficiency, optimizing them from the perspective of resources and time in relation to their goals, as well as the requirements of the system of state crisis management.

The Business Continuity Plan, primarily focusing on ensuring continuity of processes within a critical infrastructure entity, can play the integrating role here, given its complex approach to both internal and external operational risks in relation to economic factors and risks. In this case, those would be processes of ensuring protection and sustaining continuous function and integrity of critical infrastructure for the purposes of achieving business goals of the critical infrastructure entity (the owner or operator of the infrastructure).

They include requirements arising from the respective legislature and documentation of crisis and emergency planning with focus on the security of the state, ensuring basic vital needs of the population, human health or the state economy.

The paper was created within the execution of the Security Research project *'Tools for Introduction of Process Management in Ensuring Protection and Functionality of Critical Infrastructure with Emphasis on the Field of Transportation'* of the Ministry of Interior of the Czech Republic – (BCM), registration number VI20152018039.

REFERENCES

[1] 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.

[2] JANUŠOVÁ, L., LEITNER, B.: Postup na identifikáciu potenciálnych prvkov kritickej infraštruktúry v podsektore železničná doprava. In: Krízový manažment, roč. 14, č. 2, s. 5 – 13.

[3] KOPECKÝ, Z.: Východiska zvýšení odolnosti subjektů kritické infrastruktury. In *Riešenie krízových situácií v špecifickom prostredí.* Žilina: Fakulta špeciálneho inžinierstva Žilinskej univerzity, 2010, s. 375–381. ISBN 978-80-554-0203-1.

[4] BENDA, L., KOPECKÝ, Z., PŮLPÁN, P., ŠPAČEK, M., ŽIVOTA, V., et al: *Nástroje zavedení procesního řízení v zajištění bezpečnosti a funkčnosti kritické infrastruktury s důrazem na odvětví dopravy*. [CD]. VI20152018039, Ministerstvo vnitra ČR. Program bezpečnostního výzkumu České republiky v letech 2016-2020. Praha: WAK SYSTEM, s.r.o, 2016. 33 s.

[5] KOPECKÝ, Z. et al.: Návrh systému informační podpory ochrany kritické dopravní infrastruktury pro potřeby řešení typových plánů krizového řízení veřejné správy (KRIZ - CG941-055-030) [CD-ROM]. 2011, VŠE v Praze.

[6] KOPECKÝ, Z.: Podnik jako subjekt kritické infrastruktury v krizovém řízení státu. In Majtán, Š. (ed.). Aktuálne problémy podnikovej sféry 2013. Bratislava: Ekonóm, 2013, s. 265-270. ISBN 978-80-225-3636-3.