PRINCIPLES FOR MANAGEMENT OF RISKS OF CRITICAL INFRASTRUCTURE

Dana Prochazkova, Jan Prochazka, Miroslav Rusko

Abstract: On the basis of present knowledge, the critical infrastructure is a set of physical (technical and material), cyber and organizational subsystems of human system that are necessary for ensuring the protection of: human lives, health and security; property; human society welfare; environment; minimal functioning of economy and state administration. In these systems, the processes being under way make up the ground of dynamic development of both, the individual systems and the complexes. The paper is directed to critical infrastructure risk management. For improvement of critical infrastructure safety, it gives the basic principles for trade-off with risks that were derived at deep study of problems of technological facilities in practice.

Key words: critical infrastructure, complex technological facility; risk; safety; levels of risk management; principles for risk management.

1. Introduction

The aim of human effort is to ensure the human lives, health and security. Therefore, on the basis of current knowledge [1], the humans need to:

- take care on basic public assets (the human lives, health and security; the property and public welfare; the environment; infrastructures and technologies). Critical infrastructure (further only CI) belongs to essential public assets because it: provides products and services that improve the human lives; contributes to employment, technical education, energy self-sufficiency and competitiveness; and creates a background in response to critical situations (each response needs energy, technical resources, finance, transportation, material, etc.),
- adapt their behaviour so it might be preserved the coexistence of essential systems (environmental, social, and technological) that are inevitable for the existence and life of humans, i.e. for safe human system that has the nature of the SoS; i.e. an open system of systems, which is a collection of series of mutually penetrating open systems. Interfaces are the source of internal dependencies, called the interdependences, namely by those that are required and as well as troublesome; and some of which take effect only under specific conditions.

For reaching the given target, the humans use the tool "management". Management is a very broad term and it means "to have something under direction, to control, to manage, to regulate, to govern". From the time of Mr. Taylor, the scientific management founder [2], and his successor Mr. Fayol [3], the basic management functions have not changed. The executors of the management are the humans, who lead the given entity to the prosperity and efficiency. The fact in question also applies to the semi-automatic and automatic control, because their algorithms are created by humans. In the real world, the human may well drive his behaviour and the behaviour of the technical products and facilities that he created, when he perceives the limitations of his capabilities and skills, and with regard to it, he proposes and implements his measures and activities.

Current knowledge [4] shows that CI is composed of a series of infrastructures, which are composed of objects and networks, which are mutually interconnected, i.e. it goes on the SoS, the nature of which is socio-cyber-technical. Own CI assets comprise constructions, their elements, devices, services, and the staff, the technical and cyber interfaces making up the required links and flows among the listed items, knowledge (know-how), operational procedures, products, reserves (material, financial, human, and other), the agreements on cooperation with public authorities, security units, research institutions, the public, etc. [5].

It is understandable that the management of State and the CI private management need to meet the requirements of good governance [1,6], i.e. the humans in the management of the State, territory and the CI need to:

- consider all protected assets; at the CI it goes on the public assets and the proper CI assets,
- use the current knowledge in the context of systems theory,
- control activities, so that they might not cause the phenomena, which would lead to the disintegration of the human system (i.e., they might nor create the conditions for the emergence of the so-called "organizational accidents").

This means that humans at all levels of management need to adhere to certain safety culture. The effective safety culture is the fundamental element of safety management. It reflects the safety concept and it goes out from values, attitudes and manners of top management workers and from their communication with all involved

persons. It is obvious obligation to participate in solving the problems of safety and it promotes so all involved persons perform safely and so they observe the appropriate legal rules, standards and norms. The safety culture rules need to be incorporated into all activities in each entity and in each territory. Their ground is not the concentration to punishment of malefactors / originators of faults, but the lessons learned from the mistakes and the introduction of such corrective measures so mistakes might not repeat, or rather their occurrence frequency might be distinctly reduced.

The safety culture level is the quantity that cannot be directly and exactly measured, but for all that it has fundamental influence on workers´ behaviours, the management style and the technology level. The definition of weak and strong features in individual parts of safety is important for safety culture level. The comparison of time series of investigations permits to evaluate the effectiveness of corrective measures.

2. Knowledge about the CI safety

According to documents, for example [4-33], the CI can be damaged, destroyed or disrupted by the intentional terrorist attacks, natural disasters, negligence, accidents or computer hacking, criminal activity or illegal actions. To protect the human lives and assets in the EU which are affected by terrorism, natural disasters and accidents, it is essential so each CI disruptions or manipulations may be in the context of options, short, infrequent, controllable, geographically limited and minimally destructive for the welfare of the citizens of the Member States (MS) and the European Union (EU). The EU has created a European programme for the CI protection of (EPCIP) [5], the critical infrastructure warning information network (CIWIN) [34] and it commissioned a number of research projects in the subject area.

The EPCIP should minimise any unacceptable impact at which the increased investments in security could affect the competitiveness of the relevant industrial sector. When calculating the proportionality of the cost, it must not lose sight of the need to maintain the stability of the markets, which is crucial for long-term investments, nor the effects of the protection on the development of stock markets and on the macroeconomic environment.

Critical analysis of selected available documentation to projects [4,6-29] shows the following findings:

1. In order to protect the CI, it is necessary to make a distinction between dependence and interdependence. Dependence means that infrastructure A influences the B infrastructure condition. The dependence is direct or indirect; an indirect dependence is when the A infrastructure influences the B infrastructure by means of the C infrastructure. The interdependence of infrastructures indicates a double-faced relationship between the A infrastructure and the B infrastructure; i.e. the loops of mutual influences are created. The result is the fact that the consequences of any violation cannot be described by the tree structure in which it is assumed that all the events are happening in one direction [30].
2. It is necessary to distinguish four sources of dependencies, namely: physical interdependence – the operation of one infrastructure depends on the physical performance of the another infrastructure; cyber interdependence – the operation of one infrastructure depends on the information transferred across the cyber infrastructure; geographical / territorial interdependence – the infrastructures are territorially close to each other (i.e. two are disrupted by every disaster - explosions, fire, etc.); and the logical interdependence; details can be found in [31,32], which deals in detail with the problems. Since the conditions of each infrastructure are in territory controlled by manually, semi-automatically or cybernetic, so it is possible through the interdependences to trigger the organizational accidents, i.e. the failure of the infrastructures without disrupting the technical elements; the impacts of these failures will disrupt not only the expected services, but they have also the potential to damage the technical elements, the recovery of which may be timely, financially and technically challenging.
3. The different interdependencies cause the failures on different levels, for example: physical interdependence causes the failure of distribution networks for the distribution of electricity, water, gas and other products; cyber interdependence causes the failures of hardware and software components, which are intended to control and manage of infrastructures (SCADA, DSC); and organizational interdependence causes errors in the procedures and functions used for determination of human activities and for support of infrastructures collaboration.
4. In practice, it is necessary to distinguish the various types of failure. Cascading failure means that the distortion of one infrastructure causes that other infrastructures stop to fill their functions. The escalating failure means that the distortion of one infrastructure will worsen conditions for the operation of other infrastructures, namely by increasing demands on their operation, there is no period for recovery or renewal, which over time leads to failure. The malfunction with the same cause means that multiple networks (usually those in which it is a great geographical dependence) fail at the same time, for example, as a result of the strong earthquakes occurrence; for description, the tree structure models are not also suitable [30].

5. The CI protection necessitates coordinated multidisciplinary approach and it is not just a technological problem.

The basic findings of the works [1,27,31] is that the CI disruption causes great economic and social impacts and possible cascades due to CI interdependencies. Therefore, it is the need to better understand the close CI interdependences and to improve risk analysis, and by this the CI safety and protection, it is also the need to improve the response to the disasters, the occurrence probabilities of which are small but impacts severe, to implement exercise, to perform the What, If analysis [35], again to consider the correctness of the decision in order to find lessons for improving the design of the next CI generation. Presented specific project results CIPRNet [27] are:

- recovery of infrastructures is very slow after cascading failures or parallel infrastructures failures,
- the average failure duration is different: electricity-73 minutes to 5 hours; railways – 1 day; gas supply-8 hours; airport-2 days,
- the originators of failures are: the human factor and technical causes - EU 45%, USA + Canada 36%; interdependences - EU 25%, USA + Canada 13%; natural disaster - EU 17%, USA + Canada 46%; intent distortions - the EU 9%, USA + Canada 5%,
- the level of protection for all infrastructures might not be the same, because the disasters impacts on infrastructures also depend on the vulnerability of certain real infrastructure,
- the originators of failure in individual countries and the possible ways of responses are in the EU Member States different, i.e. it does not help a common standard procedure in the EU.

The available CASCADE project results [28,29] are:

- causes of failures of infrastructures are very much,
- for ensuring the CI protection, it is required: to consider the All-Hazard-Approach [36]; and to analyse the historical events.

It is apparent from the results of both projects that the EU Member States only obtain general recommendations, because the specific real implementation depends on the legislation of each State.

Based on studies of professional literature and of practice from operation of technical facilities and of the CI, we use the risk engineering principles and build the rules for risk management, which it is necessary to incorporate into the EU Member States legislations.

On the basis of works [30-33], the CI development is directed more and more to a combination of individual devices and to creation of complex systems with aim to achieve the increase of production and high profitability. Therefore, in complex systems, the safety function needs to be considered in context with other functions of the system and its subsystems. That is, it is not enough to solve the details (i.e. the safety issues within the individual subsystems), but it is need at the same time to solve the whole system safety and the system parts safety (i.e. the subsystems safeties). It is necessary to count with the following hazards: external hazards (hazards from disasters around the system); internal hazards (hazards from internal devices of individual subsystems); operational hazards (hazards associated with the failure of the function of the entire system or device or component of a system, i.e. subsystems failures); hazards associated with the assembling; and human hazards (hazards associated with human activities) [32].

The CI complexity goes out of the required features of the CI system, namely: a large-size; the use of multiple technologies; complex functional dependencies; great interoperability; great performance; and high safety, i.e. functionality and reliability and a low hazard of protected assets under normal, abnormal and critical conditions.

In each territory, there are occurring the disasters, i.e. the harmful phenomena of all kinds, the sizes of which vary in time and space. These phenomena from a certain size damage the technical facilities, i.e. also the CI, and their disruptions can cause a cascade of unacceptable phenomena and domino effects that will increase the losses of human lives and the damages to other public assets. The disasters of all kinds are sources of risk for the technical facilities of all kinds. The risk in engineering disciplines is seen as the probable size of the losses, damage and injury to protected assets in a particular place, normed on the selected time unit [30-33]. It is dependent on the size of the particular harmful phenomena (disasters) and of local assets vulnerability.

The knowledge collected in [30-33] shows that in ensuring the technical facilities safety, i.e. also the CI, it is necessary to consider the risks connected with: security; construction technology and design; credit; market; external phenomena; operation; associated with the management and decision-making. It is necessary to perceive that significant sources of risk are also: disorders of supplier-customer relations; uncertainty in the labour force; the uncertainty of the financial resources; accidents and large incidents on operating equipment; industrial accidents in other bodies; natural disasters; and political or economic instability in the region, where the infrastructure is located.

It is the fact that the individual technological sectors safety depends on traditions that have been evolved during the certain period in the sector. Therefore, in the whole, consisting of several sectors are carried out safety measures diverse and they correspond to the knowledge and experience of the period in which they were created. To this day, the reality is that at making up the technology systems and at creating their safety, the experts from different fields have been working separately, which does not guarantee the optimal safety, nor even the optimal costs.

3. The CI risk management aimed at safety

Present tried-and-true management is based on management of processes, and specially on management of risks that are connected with these processes, which is directed to human security and development. To this purpose it is performed the synthesis of verified knowledge and experiences from work with risks, professional inspections and analyses of accidents and failures of technological facilities.

Because the CI represents a set of the overlapping systems of various sectors, its model is the SoS. Therefore, it is not fitted to work with partial and integrated risks, it is necessary to consider the integral (system) risk [30-33]. It represents direct and indirect losses on assets with reality that the indirect losses are increased by: delays or errors in response; cascades of failures caused by synergic and cumulative effects, which are caused by linkages and couplings among the assets; and by domino effects. It is expressed by following formula

$$R(H) = \left[\sum_{i=1}^{n} A_i(H) Z_i(H) + \sum_{i=1}^{n} \int_0^T \int_S F(H, A_i, P_i, O, t) \mathrm{d}S\mathrm{d}t\right] \cdot \tau^{-1} \quad ,$$

where: H is the hazard connected with the considered disaster; A_i are the values of assets, i = 1,2, ..., n that are considered in connection with complex technological facility safety, where n is the number of monitored assets; Z_i are the vulnerabilities of assets taken under account, i = 1,2, ..., n; F is the loss function; P_i is the occurrence probability of i-th asset damage – conditional probability; O is the vulnerability of safeguard measures; S is the size of followed territory / facility; t is the time that is measured from the origin of harmful phenomenon in facility; T is the time for which losses arise; and τ is the return period for the given disaster [30,32]. The reality is that we do not know the shape of the loss function. Therefore, we use the procedure below.

On the basis of current knowledge, we can determine direct damages, losses and injuries of the assets if we select the correct disaster scenario. We cannot properly determine the damages, losses and injuries associated with linkages and flows in complex systems, which are the CI [30-33]. Therefore, in practice, we set up by the expert manner a number of relevant scenarios of priority critical disasters. Their risks, we determine by help of scenarios making up by the case studies, with the expectation that we use the disasters scenarios that are most likely to occur. Then, we set the risks values and on their basis the protective measures [30,32-33].

The task of risk management is to find the optimal way how the assessed risks to reduce to the socially acceptable level, or to keep them at this level. Therefore, it is necessary to agree on requirements which the risk assessment output needs to meet and at the risks settlement it is necessary to try to comply with these requirements, and any failure to justify. Based on the knowledge, the modern way of working with the risks [30-33] requires to:

- set the risk throughout the entire object life cycle (sitting, design, construction, operation),
- focus the risk determination on the users' requirements and on the level of provided services,
- establish risks according to the criticality of the impacts on the processes, on the service provided and on the assets, which provides for the public interest,
- mitigate unacceptable risks through risk management tools, i.e. by technical and organizational proposals, standardization of operating procedures or automated control.

Procedure in the case that the risk is unacceptable [32], consists in:

- avoiding the risk (i.e. not to initiate or not to continue activities that are a source of risk), when it goes – in the case of natural disasters it is not possible,
- removing the risk sources of risk, i.e. to avert disasters origination, when it goes – in the case of natural disasters it is not possible,
- reducing the risk occurrence probability, i.e. to avert severe big disasters occurrence (e.g. by reducing the amount of hazardous chemical substances in enterprises), when it goes – in the case of natural disasters it is not possible,
- reducing the severity of the risk impacts, i.e. the preparation of the mitigation measures such as alert systems, response and recovery systems,
- risk-sharing, i.e. sharing the risk among the participating persons and insurance undertaking,

- retention of risk.

The CI safety needs to build continually, because the world is dynamically developing. The CI program on safety increase needs to provide the precise methodological procedure checks on safety aspects and to evaluate the facilities design in terms of identifying the possible sources of risks and prescribing the time and costly efficient corrective interventions. The objectives of this program are to ensure:

- measures for ensuring the safety of the individual devices incorporated inherently,
- risk management measures for the acceptable level of hazard, namely for all the risks associated with the system, subsystem, and sections,
- risk management measures for hazards, which cannot be eliminated (beyond design disasters), where they are needed such measures that protect the staff, facilities and assets,
- minimum risk when using new materials, or the products and test techniques,
- implementation the corrective measures required to improve the safety of temporary by incorporating safety factors that were created during the formation of the system,
- considering historical data about the safety that were generated by similar programs of safety, wherever it is appropriate.

Activities related to the whole CI safety begin in the earliest stages of development of the CI concept and go through all activities of the design, manufacture, testing, operation, and decommissioning. A significant aspect that distinguishes the access of the system safety from other approaches to safety (operation, process, products, inventory, etc.) is its primary emphasis on the timely identification and classification of danger so that they can be received redress for their elimination or minimization before final design decision [30-33].

Effective safety management lies in: the determination of policy and in defining the safety objectives, i.e. in the planning the tasks and procedures; in defining the responsibilities and in determining the competencies; in documenting and ongoing monitoring the hazards and dangers resulting from them including the inspections; in maintaining the safety information system including the feedback and forms of reporting the incidents / accidents, etc.

Always, when we work with risk, let we manage it or we negotiate with it, namely in the classic concept or in the modern concept focused on the security and sustainable development, so we need to respect that the main characters of each risk are random uncertainty and epistemic uncertainty. Their causes can be divided into deviations arising in the course of the matter, that is:

- usual under normal system conditions, where only small variations (source of uncertainty) occur,
- real, where the occasional changes in the system processes occur and they lead to the occurrence of the occasional extreme values (source of uncertainties and occasional epistemic uncertainties),
- variable, where big changes in the system processes occur, for example caused by external causes (the source of the epistemic uncertainty).

The random uncertainty is related to the scattering the observation and measurement. It can be incorporated into the assessment and prediction using the apparatus of mathematical statistics. The epistemic uncertainty is related to both, the lack of knowledge and information about the process, and the natural variability of processes and events that cause disasters, or even to blunders. For the incorporation and consideration of epistemic uncertainties, the mathematical statistics apparatus is insufficient, and it is necessary to use a different, more modern mathematical apparatus that provide for example, the theory of extreme values, theory of fuzzy sets, theory of fractals, theory of dynamic chaos, the selected expert methods and suitable heuristics [35].

To ensure the CI safety, it is necessary according to [30-33] to do: to establish what and why it is necessary to protect; to establish a minimum level of protection; to assess the current level of protection; in the event that the protection is insufficient to propose countermeasures; to ensure the resources; to apply the measures for protection; periodically to check the conditions; to maintain an appropriate level of protection; and to revise the measures depending on the development. Tasks have: owner; public administration; security forces; and citizens [30-33].

From the system viewpoint, it is necessary for the CI safety to monitor: information activity to support decision-making; the devices, measures and actions promoting the safety; humans as subjects and objects of safety; and procedures connecting he humans and the CI structure.

In the context of the CI risk management, it is necessary to perform high quality five key activities:

1. Definition of objectives and the focus of safety management, i.e. to identify: the context; priority objectives; and areas and major tasks. Selections are based on the evaluation of assets and objectives. By this we determine which risk in given case is a priority.

2. Description: it moves towards an objective understanding of the occurrence probability and the impacts size (in qualitative or better in quantitative expression) of possible disasters and CI failures. This is a highly professional activity requiring the deep knowledge and high-quality data.
3. Decision: the evaluation of quality of the predictions of the CI development, if possible such as optimum, taking into account the benefits and losses in the CI operation in the dynamically varying the area. The decision how to mitigate and to manage the risks and how to implement the measures, represents a key step in the context of risk management.
4. Communication: negotiation of set of measures and activities with key actors in the CI operation process and with other stakeholders. Legislation requires in the important issues of communication with the public, the consultations, the removal of conflicts and the establishment of the partnership.
5. Monitoring and lessons learned: monitoring the designated variables and their values that characterize the implications of the decisions and actions on the CI, and in the event of significant deviations, which may undermine the achievement of the objective, to apply corrections.

The [33] summarizes: alternatives that are used when the risk is not acceptable; and procedures for risk put under control (prevention, preparedness, response, recovery, insurance). It shows that pulling off the risk is necessary to split among all involved. The split in the good governance is performed so that for risk tame are responsible all participants (from politicians over the public administration workers, the CI management up to the CI technical staff and the citizens), and that the work with the specific risks is allocated to the body that is the best prepared. On this principle, it is also based the CI resilience formation (technical and organizational) [37].

Because resources, forces and means are always limited, it is necessary to ensure in the selection of measures on the risk management so that the cost of measures on risk managing might not exceed potential damages caused by the risk realisation. Requirements on the CI management teams and other participating were formulated by the OECD [38]; their elaboration for the CI is in work [32].

In the public interest, the legislation needs to ensure that the risk associated with the CI will be acceptable, especially for whose, who may be affected by the risk, i.e. above all, the staff of CI operators and the citizens who are dependent on the CI services. In terms of security and development, it is necessary to create such knowledge, personnel, material and technical background for the CI so that the CI may not threaten under critical conditions neither itself nor its surroundings, and it may be recovered; and also at extreme conditions it preserves capability to recover.

4. Data and methods used for determination of principles for CI risk management

The CI is understood as the set of complex socio-cyber-technology systems and the aim of our effort is to manage the risks by such way that the optimum CI safety is reached. To derivate the principles for the CI risk management, there were used as the data findings summarized in previous paragraphs and hundreds of sources that are listed in the works [30-33]; it goes on:

1. Knowledge of the literature and own research on the risk and safety.
2. International Organization for standardization guidelines for qualified risk management.
3. Pieces of knowledge from the application of the ALARA, the ALARP, RAM, RAMS, etc. in industry and construction.
4. The guidelines of the IAEA, WANO, NEA, OECD, UN, FEMA, EMA, ISO, IRIS, etc.
5. Findings from the published results of the evaluation of accidents, that were published e.g. by: NASA, OECD, IAEA, WANO, NEA, the United Nations and others.
6. Findings from own studies for industrial and energy objects in the Czech Republic and abroad.
7. Own results obtained from database of disasters and accidents (consisting of 258 world's resources on 922 technological accident hazards involving the dangerous substances since 1916; 168 world's resources on 223 road accidents involving the dangerous substances since 1929; 281 world's resources on 207 nuclear accidents, etc.).
8. Evaluation of the calculations of risks and quantities that are needed to determine the risk.
9. The experience from forming the tools for safety management based on risk management for industrial and transport systems in the Czech Republic.
10. The experience gained from inspections and investigations of incidents and accidents in industry and transport.
11. The experience gained from the assessment of the safety reports of complex technological facilities.
12. The results of the research and application projects solved for the EU, OECD, NEA and the IAEA.

All data used are collected in the archive [39].

At derivation of the results, there were used both, the general logical methods and the selected risk engineering methods as: determination of critical items, panel discussion, multi-stage Delphi method [35].

5. CI risk management aimed to safety

In the risk determination, i.e. normed damages, losses and injuries to the assets, and in the countermeasures determination, we lean on basic terms: disaster; hazard; security; danger; safety; secure system; safe system; and system integral safety management, which are defined in [30]. In this concept, the safety management of the CI, which is the SoS, is the discipline applying the methods, tools and techniques based on the engineering and managerial approaches, in order that the CI might be safe. It relies on risk management, in which the precautionary principle is incorporated. In the case of the integral safety management, it goes on the integral risk management; Figure 1; the whole description is in [30,32].

6. Principles for the risk management of the CI and the territory

According to the TQM principles [40] used in the EU, and the experience of the practice, it is needed in the context of the problems solution in the splitting the tasks and responsibilities to take into account the possibilities that exist at different management levels. Options are given by the both, the authority and the availability and the amount of available resources, forces and capabilities that are needed for problems solution:

- at the CI operational management level, safety problems being well structured can be solved successfully,
- at the CI middle management level, they can be successfully solved safety problems being structured and poorly structured ones that are not associated with major risks,
- on the CI top management level, they can be successfully solved complex and unstructured safety problems that have risks that can be controlled using the tools, which are only available to top CI management,
- complex and unstructured safety problems of the CI with great extent and huge ricks can be solved only by mutual deep co-operation of the public administration and the CI top management.

For solution of safety problems of the CI with transnational extent, the international cooperation is needed.

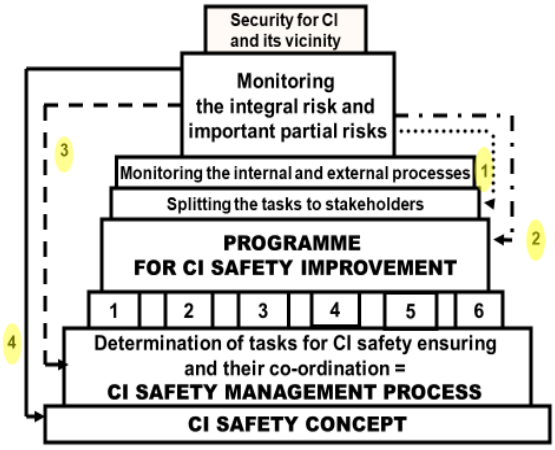

Fig. 1. Model of the CI safety management in time. Processes: 1 - concept and management; 2 - administrative procedures; 3 - technical matters; 4 - external cooperation; 5 - emergency preparedness; and 6 - documentation and the investigation of accidents. Feedbacks that are used to control when the risk is unacceptable - the numbers in the yellow circle.

To derive the CI risk management principles, there are used the knowledge and experience listed in the previous chapters and the base viewpoints:

1. The CI needs to be secure throughout the lifetime, and therefore, risk management needs to be: focused on the integral safety; and in all aspects comprehensive, systemic and proactive.
2. The CI needs to fulfil during the lifetime the tasks in demanded quality, and at its critical conditions it must not endanger itself or its surroundings, i.e. they are applied the All-Hazard-Approach developed for Europe at work [36], the Defence-In-Depth developed for the technical facilities, including the CI in [32]; it, has a program for the continuous improvement of safety and safety culture.
3. The CI is important for ensuring the basic functions of the State (power plants and electricity distribution, water works and water supply, sewer, highways, big airports, transportation communications, large production units, etc.), and some its parts also for the EU, and therefore, the obligations for putting the risks under control are divided among all stakeholders.

Therefore, from the perspective of human security and development, it is important the CI risk management in two areas:
A. The territory administration and the CI management.
B. The CI real safety management.

6.1. Risk management principles for territory administration and CI management

Based on critical analysis of the accidents and failures of the CI, thereinafter, there are given risk management principles for the territory administration and the CI management in the number 40 for the levels:
A1. Political (Parliament, Government, public administration) - a total of 4 requests.
A2. Strategic (public administration, owner, investor, operator) - a total of 8 requests.
A3. Tactical (public administration, owner, investor, operator) - a total of 4 requests.
A4. Operational / functional (local administration, operator) – a total of 5 requests.
A5. Technical (operator) – a total of 19 requests.

A1. Principles for CI risk management – political level: for Parliament, Government and public administration:

- to create conditions for the long-term stability of public space, which the CI need for quality operation, (it goes about all on ensuring the stable government, mitigating the corruption, prevention of formation of intolerant groups, mitigation of impacts of terrorism and national and transnational conflicts on the CI),
- to promote the public interest and to respect the fact that the CI risks enter into the public area, i.e. it goes on the externalities that cannot be solved by market mechanisms (harmful impacts; by operation failure it is threatened a considerable part of the public; the political decision has the potential to trigger an event, in which the risk is realised; and adverse events, which are caused by unacceptable risks are distributed by the way that they do not take respect to the political fairness),
- to respect that the frequent changes in legislation, taxes and the requirements to the CI operators may lead to CI lower quality of service,
- to consider the views of specialists when deciding on the CI and not to prefer momentary political interests and actions of pressure groups.

A2. Principles for CI risk management – strategic level: for public administration, investor, owner and operator of the CI:

- to respect the value and cultural context (comfort strategy of insurance and compensation is not fully reliable, because at the great risk realization, it can happen hitting the social system, and therefore, it needs to be promoted the precautionary principle and responsibility from all participating),
- to prevent the use of incorrect technologies, the CI technological inadequacy and insufficient preparedness of the site for the CI operation (surveillance, supervision of the State),
- to ensure that the liabilities associated with the CI may be fulfilled in good quality (surveillance, supervision of the State),
- to ensure the CI staff training, mainly at the level of technical and technical-organizational; the relevant research, planning and legislation to support the CI operation,
- to promote a proactive, systematic and strategic approach at working with the CI risks,
- to pay attention to the CI goodwill at work with the risks,
- to ensure that significant risk sources for the CI might not been underestimated, which are: uncertainty in the labour force (unsuitable qualifications, lack of staff, the unreliability of the workers - fluctuation, strike, etc.); the uncertainty of the financial resources (insolvency of business partners, credit uncertainty, problems with insurance, etc.); accidents and large faults on operating equipment; industrial accidents in other bodies; natural disasters; and political or economic instability in the region,
- to ensure the capability of public administration and the CI management to handle the impacts of extreme disaster and to perform recovery of the CI and its vicinity.

A3. Principles for CI risk management – tactical level: for public administration, investor, owner and operator of the CI:

- to ensure that at designing, building, construction and operation of the CI, all serious disasters that are possible in the CI site are considered and properly dealt with,
- to ensure so that the CI design documentation is correct and errors-free; the CI building and construction done according to professional requirements, i.e. without errors, exceedance of construction costs and unnecessary environmental pollution at the site,
- to ensure that the CI is safe under the conditions normal, abnormal and critical (monitoring and supervision of the State),

- to ensure the cooperation with the local population and local security forces for case of accident or failure of the CI (to build organizational resilience [37].

A4. Principles for CI risk management – operation / function level: for public administration and the CI operator:

- to ensure a proper settlement of all risks, in particular market risks, such as the reduction of demand for the product, changes in the exchange rate; inflation, deflation and changing the interest rates,
- to ensure the CI high-quality operation from the perspective of ensuring the material inputs and qualified personnel,
- to create inside the CI, the safety culture based on mutual cooperation, i.e. to have the tools to control conflicts among employees,
- to provide resources and protective equipment for employees and the local population, including the information fittings and documents (for case of accident occurrence),
- to ensure the appropriate training and education of employees, and the local contractors and local population.

A5. Principles for CI risk management – proper CI management level: for the CI operator:

- to improve permanently the risk understanding, risk management and trade-off with risks,
- to implement the risk sources continuous monitoring,
- to consider the risks of organizational accidents,
- to consider the risks associated with the CI complexity (because the complexity not only creates new dangers, but makes them even worse identified; new hazards are e.g.: increasing the automation, the growth of production capacity, the large pace of technological change),
- to count with the appearance of atypical accidents, the causes of which are unexpected combination of events, and for this case to have a high-quality response plans for multiple scenarios of accidents and also for special accident caused by a combination of a series of unacceptable phenomena,
- to admit that the safety systems and safety related systems may fail,
- to process a response plan to extreme phenomena,
- to train responses to situations created by extreme phenomena,
- to have prepared place for response management in the case of great accident and technical equipment for clearing debris,
- to ensure that the professional top management is constantly interested in the development of knowledge and evaluated the experiences from the CI operation, because there is no previous experience, which could be used to overcome new dangers and the relevant laws and standards for many of the new engineering and technology sector are not yet developed,
- to ensure performance of all tasks associated with the real CI operation,
- to ensure the implementation of all tasks of the State (the products in the required quality, services, accessibility),
- in the CI managing to be based on the qualified professional criteria for risk assessment (established according to: the nature and kind of consequences that may occur during the realization of risks including their measurement; the way of risks occurrences setting; the time frame of the consequences and the risk probability occurrence; the way of determination of risk level, i.e. the level below which the risk is acceptable or tolerable, and the level of risk, from which it is necessary to ensure a targeted response; and the possibility of combining multiple risks),
- to ensure the professional performance of actions, qualified maintenance, skilled repairs, timely modernizations; and timely adaptation to changing conditions (to have a qualified professional management and a highly effective professional inspection, including motivational resources to target employees on the safe implementation of the activities and cooperation),
- to ensure the protection and the necessary training the critical employees, i.e. also the protective equipment and utilities and other necessary formalities, including the appropriate resources and protected space for hide of employees,
- to ensure the CI high-quality operating rules for normal, abnormal and critical conditions,
- to ensure high-quality monitoring and timely response to operational deviations, failures, near accidents and accidents (to ensure that in due time there are accepted necessary measures, especially in sites where it is accumulation of a large amount of failures and near accidents),
- to provide the making up the basic plans: CI safety management plan, which will provide safety during the life cycle; the risk management plan, in which the clear responsibility for the individual measures and individual activities are given; in-site emergency plan (in which the clear responsibilities for the individual measures and individual activities are given); business continuity plan (to overcome the highly critical to the extreme conditions in which they will be clear responsibilities for each of the measures and activities for the conservation and survival of the CI; the external emergency plan and crisis plan (in which the clearly

defined cooperation and accountability of the CI components and their security forces, the public security forces, and public administration),
- to ensure permanent consideration of new knowledge and lessons learned from the near accidents and their implementation into practice in a form suitable for the CI.

6.2. Risk management principles for CI real management

It goes on a real subject area that deals with data, methods, material and technical issues, organisational, legal, financial and personnel matters directly in the CI. Risk management needs to respect that fundamental role has: knowledge; respect for the physical and other patterns (properties of material, structures, buildings and environments and their changes in time), i.e. the existence of limits and conditions; the human factor and with it connected the performance of high-quality work and the proper execution of responsibilities at all stages of the life cycle; the availability and the modalities of application of processes and technologies, etc. General principles for working with risks are: to be proactive; to imagine the possible consequences; to properly prioritize public interest; to think of mastering problems; to consider synergies; and to be vigilant.

At all stages of the CI life cycle it is required so risk management may be complied with the main principles:
- it is targeting to an integral safety, using the All-Hazard Approach [36], the Defence-In-Depth developed in [32], and relying on the program for safety improvement targeted on the safety integrity (i.e. to have a safety management system, process safety management and safety culture),
- it is containing in each decision-making the followed CI – TQM [40] and ISO standards (International Organization for Standardization),
- it is complying with the key concepts in risk engineering targeted at safety, i.e. it considered a critical quality attributes and critical process parameters (quality of implementation of measures and actions of prevention, preparedness, response, recovery and lessons learned),
- it is using: high-quality data, methods, and engineering approaches, progressive types of safety approaches - the inherent, passive and active safety,
- it is optimally governing the factors of different nature: knowledge; experience; the budget; competences; the way of management and decision making; team work; etc.
- it is optimally dealing with the conflicts.

Based on critical analysis of the accidents and failures of the CI, thereinafter, there are given risk management principles for real CI management in the number 66 for the domains:
B1. The concept and way of real CI management - 21 requests,
B2. Requirements for data, methods, and techniques that ensure the quality of decision-making and management of the CI - 9 requests,
B3. Procedures for the correct sitting, the quality of: the CI design, building, construction and operation - 13 requests.
B4. Provisions for the CI business continuity and for support the basic functions of the State, i.e. public interest – 23 requests.
It goes on the requirements for data, methods, and ways of solving problems in the areas of technical, methodological, organizational, staffing and financial; the results are at work [33].

7. Conclusion

The CI safety depends on the quality of negotiations with risks. Integral safety is associated with negotiation with integral risk, i.e. not only with the partial risks (that are focused on the individual protected assets), but also with the risks that are associated with the linkages and flows between the protected assets. Reducing the risk is associated with: an increase in costs; the lack of knowledge and technical resources, etc. Therefore, in practice there are used the boundaries given by the ALARP or ALARA principles [32].

It is not enough to know the sources of risks and impacts related to the risks realization, because for coping with the risks there are needed the available resources, forces, and capabilities for their mastery, so that damages, losses and injuries to protected assets may be reasonable. Therefore, the rate of risk reduction is also subject to top management and political decision-making, which make use the current scientific and technical knowledge and take into account the economic, social and other conditions. Therefore, it is necessary to ensure the good safety culture for all levels of territory management and the real CI management.

Analysis of accidents and failures of different CI showed that the safety culture needs to be solved in two domains, namely in the interface of the territory administration and the CI management and in the CI real safety management. In both areas, it is needed the cooperation of the participating stakeholders, especially decision-

making bodies and individuals and experts. Practice shows that still it is the fact that in the CI designing and operation, and in the CI safety creating, the experts from different fields are working separately, which does not guarantee optimal safety, nor even the optimal costs. Therefore, it is often the case that the individual subsystems are safe, because for them there are standards and norms, but the safety of the whole, which was formed by their interconnection with the cyber and other infrastructures has not already followed, because the evaluation and demonstration of safety are not required by the relevant legislation, and in addition to such purpose the relevant professional practice is not yet available.

The principles for the CI risk management in number 40 in the domain interconnected the public administration and the CI management were determined for management levels: political (parliament, government, public administrations levels); strategic (state public administration, owner, investor, entrepreneur); tactical (regional public administration, owner, investor, entrepreneur); executive / functional (local public administration, owner, investor, entrepreneur); and technical (entrepreneur).

The principles for real CI risk management in number 66 were determined in domains: concept and way of real CI management; requirements for data, methods, and techniques that ensure the quality of decision-making and management of the CI; procedures for the correct sitting, the quality of: the CI design, building, construction and operation; and provisions for the CI business continuity and for support the basic functions of the State.

References

[1] PROCHÁZKOVÁ, D. *Strategic Management of Safety of Territory and Organization* (in Czech). ISBN: 978-80-01-04844-3. Praha: ČVUT 2011, 483p.

[2] TAYLOR, F. *The Principles of Scientific Management*. ISBN 0-415-27983-6. Routledge 1911.

[3] FAYOL, H. *General and Industrial Management: Henri Fayol's Classic Revised by Irwin Gray.* Belmont: David S. Lake Publishers 1987.

[4] EU. Green paper on a European Programme for critical infrastructure protection, Brussels, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC05 76&

[5] EU. European Programme for Critical Infrastructure Protection (EPCIP). Council Directive 2008/114/EC, on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection.

[6] ROSSIGNOL, M. Critical infrastructure and emergency preparedness. *Report PRB 01-7E,* Canada, 001. http://publications.gc.ca/Collection-R/LoPBdP/EB/prb017-e.htm.

[7] BRUNNER, E. M., SUTER, M. *International CIIP handbook 2008/2009*. Zurich: ETH, Center for Security Studies, ETH 2008. http://www.css.ethz.ch/content/dam/ethz/special interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf.

[8] BOLOGNA, S., SETOLA, R. The need to improve local self-awareness in CIP/CIIP. *First IEEE international workshop on critical infrastructure protection (IWCIP'05).* IEEE 2005.

[9] LUIIJF, H., NIEUWENHUIJS, A. H., KLAVER, M., VAN EETEN, M., CRUZ, E. Empirical findings on European critical infrastructure dependencies. *Int. J. Syst. Syst. Eng.*, 2 (2010), 1, pp. 3-18.

[10] VAN EETEN M., NIEUWENHUIJS, A., LUIIJF, E., KLAVER, M., CRUZ, E. The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Adm.*, 89 (2011), 2, pp. 381–400.

[11] US GENERAL ACCOUNTING OFFICE. Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants. *Report GAO-03-251*, Washington DC, Feb 2003. http://www.gao.gov/new.items/d03251.pdf.

[12] OCIPEP. The September 11, 2001 Terrorist Attacks - *Critical Infrastructure Protection Lessons Learned, IA02-001*, 27 Sept 2002, Ottawa. http://www.au.af.mil/au/awc/awc gate/9-11/ia02-001_canada.pdf.

[13] NIEUWENHUIJS, A. H., LUIIJF, H. A. M., KLAVER, M. H. A. Modelling Critical Infrastructure Dependencies. In: Mauricio P, Shenoi S (eds) IFIP international federation for information processing. *Critical Infrastructure Protection II*, 290 (2008), Springer, Boston, pp. 205–214.

[14] SETOLA, R., LUIIJF, E., BOLOGNA, S. R&D Activities in Europe on Critical Information Infrastructure Protection (CIIP). *Int J. Syst. Syst. Eng.*, (2008), pp. 257–270.

[15] OUYANG, M. Review on Modelling and Simulation of Interdependent Critical Infrastructure Systems. *Reliab. Eng. Syst. Saf.*, (2014), 121, pp. 43–60.

[16] UNISDR. Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction. Geneva: UNISDR 2009. http://www.unisdr.org/ we/inform /publications/7817.

[17] MOTEFF, J. D. Critical Infrastructures: Background, Policy, and Implementation., *Congressional Research Service, 7-5700, RL30153, 2015*. https://www.fas.org/sgp/

[18] KLAVER, M., LUIIJF, E., NIEUWENHUIJS, A. *Good Practices Manual for CIP Policies for Policy Makers in Europe.* TNO 2016.

[19] EC. *Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure*. Brussels: SWD (2013) 318. http://ec.europa.eu/transparency/regdoc/rep/10102/2013 /EN/10102-2013-318-EN-F1-1.PDF.
[20] LUIIJF, E., VAN SCHIE, T., VAN RUIJVEN, T., HUISTRA, A. *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers*. TNO 2016. https://www.tno.nl/gpciip.
[21] EC. *Examples of CIPS Projects*. http://ec.europa.eu/dgs/home-affairs/financing/fundin gs/projects/per-program/cips/index_en.htm#/c
[22] EU. *Critical Infrastructure Preparedness and Resilience Research Network* (CIPRNet) 2016. www.ciprnet.eu.
[23] AUSTRALIAN GOVERNMENT. *Critical Infrastructure Resilience Strategy*. ISBN: 978-1-921725-25-8. 2010. http://www.emergency.qld.gov.au/publications/pdf/CriticalInfrast ructure_Resilience_Strategy.pdf.
[24] PURSIAINEN, C., GATTINESI, P. Towards Testing Critical Infrastructure Resilience, EUR— *Scientific and Technical Research Reports.* Brussels: EC.
[25] OUYANG, M., DUEÑAS – OSORIO, L., MIN, X. A Three–Stage Resilience Analysis Framework for Urban Infrastructure Systems. *Struct. Saf.*, 36-37 (2012), 23–31. http:// dx.doi.org/10.1016/j.strusafe.2011.12.004.
[26] SETOLA, R. ET AL. (eds.). *Managing the Complexity of Critical Infrastructures, Studies in Systems.* Decision and Control 90, ISBN 978-3-319-51043-9. http://cipedia.eu
[27] EU. Ciprnet.eu
[28] EU. http://www.cascade-project.eu/
[29] EU. http://esdac.jrc.ec.europa.eu/projects/cascade
[30] PROCHÁZKOVÁ, D. *Analysis and Coping with Risks Connected with Technical Facilities* (in Czech). ISBN 978-80-01-06480-1. Praha: ČVUT 2018, 222p. http://hdl. handle.net/10467/78442
[31] PROCHÁZKOVÁ, D. *Challenges Connected with Critical Infrastructure Safety*. ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.
[32] PROCHÁZKOVÁ, D. *Safety of Complex Technological Facilities.* ISBN: 978-3-659-74632-1. Saarbruecken Lambert Academic Publishing, 2015, 232p.
[33] PROCHÁZKOVÁ, D. *Principles of Management of Risks of Complex Technological Facilities* (in Czech). ISBN: 978-80-01-06180-0, e-ISBN:78-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle. net/10467/72582
[34] EU. COM (2008) 676.
[35] PROCHÁZKOVÁ, D. *Methods, Tools and Techniques for Risk Engineering* (in Czech). ISBN 978-80-01-04842-9. Praha: ČVUT 2011, 369p.
[36] EU. *FOCUS project*. EU, 2012, http://www.focusproject.eu/documents/14976/-5d763378 -1198-4dc9-86ff-c46959712f8a
[37] KOZINE, I. ANDERSEN, H. B. Integration of resilience capabilities for Critical Infrastructures into the Emergency Management set-up. In: *Safety and Reliability of Complex Systems.* ISBN:978-1-138-02879-1. London: Taylor &Francis Group 2015. eISBN:978-1-315-64841-5, www.crcpress.com – www.tayloeandfrancis.com
[38] OECD. *Guiding Principles on Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2003, 192p.
[39] CVUT. *Archives.* Praha: ČVUT 2018.
[40] ZAIRI, M. *Total Quality Management for Engineers*. Cambridge: Woodhead Publishing Ltd, 1991.

Doc. RNDr. Dana Prochazkova, PhD., DrSc., ČVUT v Praze, prochdana7@seznam.cz ,+420 608147773
RNDr. Jan Prochazka, ČVUT v Praze, fakulta dopravní, japro2am@seznam.cz, +420776103369
Doc. RNDr. Miroslav Rusko, STU v Bratislavě, mrusko@centrum.sk, +421905365519