INTERNATIONAL JOURNAL OF ECONOMICS AND STATISTICS
DOI: 10.46300/9103.2020.8.1 Volume 8, 2020

Knowledge on Critical Infrastructure Safety

DANA PROCHAZKOVA, JAN PROCHAZKA
Department of Energy
Czech Technical University in Prague
Technicka 4, 166 00 Praha 6
CZECH REPUBLIC

Abstract: - The paper summarizes knowledge on critical infrastructure, its problems and on principles for its strategic safety management. It deals with way of critical infrastructure risk management and with appurtenant tools so the critical infrastructure might be sufficiently resilient to all present hazards. At the end it shows new emerging hazards

Key-Words: - critical infrastructure; safety; failure; risks; interdependences; resiliency; system approach; safety management.

I INTRODUCTION

The basic function of the State from its establishment has been provided the protection of the human society and public assets, which humans need for life and development. Today, that function is fulfilled by the public administration which according to the European Union should realize so-called good governance. The important role plays the critical infrastructures (Figure 1) protection.

Fig.1. Selected objects of critical infrastructure; compiled by help of [1].

The critical infrastructure is a set of mutually interconnected networks, i.e. the systems of various sectors of human system (model of present world). Interconnections of systems mean the mutual dependence. Therefore, their behaviours are dependent on many factors internal or external, which have permanent or random occurrences and under their special combinations they cause emergent phenomena leading to the cascade failures of interconnected infrastructures (Figure 2) [2].

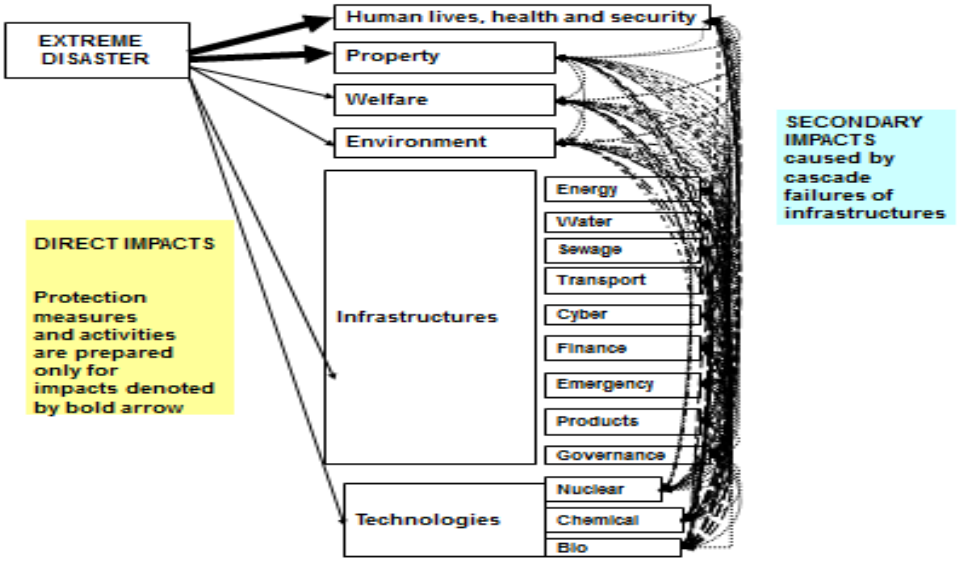

Fig.2. Impacts of beyond design (extreme, severe) disaster on human system. There are shown direct impacts on protected public assets and relevant secondary impacts caused by linkages and flows in human system and also cases for which protected measures exist in the Czech Republic (bold arrows).

II CRITICAL INFRASTRUCTURE PROBLEMS

Due to critical infrastructure complexity, its problems cannot be only solved theoretically by analytical methods, because they are very influenced by characteristics of regions in which they are located, which are multifarious. It is also caused by reality that each region has different possibilities for problems solution and these have been changing in time because the world and its parts have been dynamically varied [3,4]. From the viewpoint of system theory, the critical infrastructure as each other critical element is determined by help of criticality matrixes or by help of special methods of operational analysis [2]. The criticality matrix compares incommensurable items of infrastructure that are the vulnerability following from disasters and from properties of real territory, and the importance (relevance) for territory derived from quality of service of territory, Figure 3.

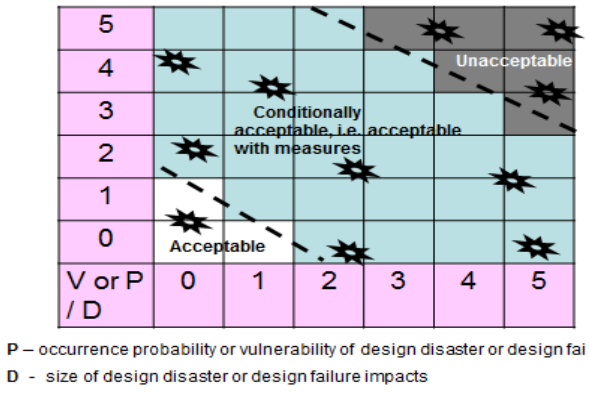

Fig.3. Criticality matrix of infrastructure, i.e. scaling the infrastructure vulnerability vs. infrastructure necessity at disasters.

The vulnerability of infrastructure is the rate of the failure of infrastructure (i.e. the infrastructure stops working of will work incorrectly) in the time and space. This rate is possible to measure with e.g. normed overall (integral) risk by all the expected nature and other disasters in a given area or by the probability of the failures of infrastructure, which occur as a consequence of these disasters, to which also the inner problems of the infrastructure itself are included. Figure 2 shows that vulnerabilities of partial infrastructures induce cascades of phenomena that cause the failure of other infrastructures, i.e. it will be happen loss of services in affected territory, and secondary impacts on humans and property. The importance (relevance) of infrastructure in area is possible to measure by necessity of its products for human society in a given territory and the State. The criticality rate is the result of the overall assessment of the impacts of infrastructure failure, i.e. of losses, damages and harms on the protected assets with reference to the duration of occurred emergency situation, which includes both, the time necessary for renovation of the infrastructure functionality when the direct damages arise and the time when the indirect damages, caused by the causal chain of impacts awakened by the infrastructure failure in area, are settled [4,5].

III DEMANDS ON CRITICAL INFRASTRUCTURE

Human society needs the safe critical infrastructure; the safety includes its protection, function and reliability under conditions normal, abnormal and critical. Process model for critical infrastructure safety management is based on principles, methods and procedures of risk engineering in advance form (i.e. safety engineering) [2-4]. Its main unknowns are interdependences across critical infrastructure subsystems that are on several levels, namely physical, cyber, organisational and territorial. The interdependences also originate as consequence of disruption of finances, energies, information, material and flows induced by directed management activities [2-4]. The basic strategic approach for the critical infrastructure safety [2,3] is: nothing is absolutely safe; and elements and networks of critical infrastructure can fail sooner or later, and therefore, it is necessary to establish the sophisticated regional safety management. The effective and efficient safety management needs to lean on the present knowledge and on their right assessment in a context that is valid for a given region [4]. It is necessary to distinguish the impacts according to their severity (Figure 3). Therefore, the basic role also belongs to the special research that at present solves: impacts of interdependences among the critical infrastructure subsystems and the human system subsystems on the basis of model “system of systems”; procedures and targets for ensuring the critical infrastructure safety from managerial view on the State level; possible distribution of tasks in the critical infrastructure safety management between the public and private sectors (it goes out of risks in a

region with the aim to reach an optimal position for public and private sector); requirements on the personnel of critical infrastructure and technology owners; tasks of security components at defeating the emergency situations, induced by the extensive outage of critical infrastructure; and general frame for critical infrastructure safety.

The interpretation of results for the given infrastructure (or for a set of infrastructures) is derived from the site position, the coordinates of which form obtained value of service measure (indeed measures of importance for region) and measures of vulnerability. If it belongs to the sector:

- „high vulnerability and high importance of service“ the condition of infrastructure is precarious, i.e. critical for a given region and from the viewpoint of security and sustainable development the situation needs to be solved by back up and enhance of the given infrastructure,
- „lower vulnerability and lower importance of service“ the condition of infrastructure is satisfactory and it is necessary from time to time to perform check-up of conditions in a given region,
- „high vulnerability and lower importance of service“ the condition of infrastructure is conditionally satisfactory and it is necessary to ensure preparedness for sophisticated response in the case of infrastructure failure and the prevention to concentrate on preventive and mitigation measures leading to the reduction of infrastructure vulnerability against to possible disasters that can cause the failure,
- „lower vulnerability and high importance of service“ the condition of infrastructure is conditionally satisfactory and it is necessary to ensure the preparedness for the sophisticated response in the case of infrastructure failure and the prevention to concentrate to reduction of criticality of infrastructure in a region or to build redundancies of being objects of infrastructure / technology / set of infrastructures.

For ensuring the critical infrastructure safety, there are on the basis of professional works, technical norms, technical standards and appropriate legal rules summarized in [2-4] used:

- special solutions in the land-use planning, sitting, designing, building, operating, maintenance, repair, upgrade, renovation, procedure changes and at putting out of operation – here it is used the concept of safety strategists, namely the emergency situations are always considered; they are not extraordinary, and therefore for the critical infrastructure safety support there are implemented the measures and activities, protection and security systems specially distributed in a site and backed up (today redundancy up to 4 x 100% is used),
- continuity plans for ensuring the critical infrastructure survive during the possible emergency situations – here it is used the concept of safety strategists, namely emergency situations are considered; they are not extraordinary, and therefore, for the critical infrastructure safety support they are implemented certain measures and activities, that ensure the conservation of minimal functionality of critical infrastructure and the perspective for future, that after emergency situation stabilisation it would be possible to start and to renovate the critical infrastructure operation in a whole extent,
- crisis plan for a case in which all or the most of safety countermeasures fail owing to an extreme disaster size or owing to unforeseen combination of random phenomena that intensify disaster impacts. It contains protective and mitigating measures and activities for humans´ survival and for conservation of infrastructure state stabilisation which is necessary for interoperability needs in a given region.

For protection and development of humans, it is necessary above all to solve the problems of survival of humans at critical conditions. It is evident and logic that for human survival it is not necessary the function of all elements and nets of infrastructures that ensured comfort live and social welfare. According to estimations being in appropriate professional literature [2] about 27-30% of functional infrastructure elements conveniently distributed in the territory can ensure under critical conditions to ensure the human survival up to term of 180 days that is usually considered as time interval during which the qualified public administration is capable to find an alternative solution [2,5-7]. It of course puts demands of territory safety management that needs to know to regulate the humans´ behaviours and activities by way, so it may be possible to reach the conditions favourable for human survival. What restrictions, what rationing system is suitable, effective, having the promise of success; it is necessary to propose and to test in the practice.

IV CRITICAL INFRASTRUCTURE SAFETY MANAGEMENT

As continuation to work [2], on the experiences from territory safety management [3-15] the method for critical infrastructure safety management for public administration needs as follows:

1. To identify elements and nets of infrastructures, which would be followed from the viewpoint of human system safety and development, to determine their location and to characterize them from the viewpoint importance for territory.
2. To determine elements and nets that are followed from the viewpoint of human system safety, which are under the public administration governance and those being out; i.e. they have private owners.
3. In the case of infrastructures that have insufficient capacity or are out of the public administration governance, the situation is more complicated, because public administration chances for influence of such infrastructures is not so simple. With regard to lessons from electricity blackouts (Table 1), this source of failure caused by increasing globalisation is not trivial. Therefore, it is necessary to find out, how reliable (from technical, finance, legal and managerial viewpoints) to ensure supply of services mediated by infrastructures from other territories, and for case of failure to prepare alternative solution for human survival from the higher regional unit management viewpoint. In the other case, it is necessary to solve problem of human survival at failure of followed infrastructures from own sources, i.e. as emergency up to critical situation.

Table 1. Expected impacts of long-term blackout of electricity (author summarizes results of 121 case studies collected for blackout) [2].

Asset	Expected impacts
Human lives and health	- loss of light, heating and air-conditioning, possibility to prepare meal, access to drinking water, liaison, connection and information sources, access to money (cash dispensers) and by those to purchase of foodstuffs etc., - loss of transport connection based on electric energy (fuel and petroleum pumping are based on electricity).
Property	- debased of meal in storage of foodstuffs and in refrigerators, - damages caused by fires that are induced by loss of function of regulative mechanisms on furnishings with open fire or on furnishings that burn down from other reason at regulation failure, - damages induced by transport and technological accident, - damages on technologies and another property caused by sudden loss of energy accompanied by dangerous fluids and gases, - damages on domestic animals caused by failure of service processes based on electric energy, - losses caused by consequences of production failure.
Environment	- increase of gaseous, liquid and teat emissions into environment as a consequence of loss of function of waste separators, disconnects, water cleaning plants, cooling devices etc., - impacts of technology accidents that occur as a consequence of electric supply disruption.
Security	- loss of furnishing the basic human needs (meal, hygiene, heat, connection with other people, isolation, lack of information etc.), - loss of medical care based on electricity supply (operation of advanced examinational instruments and installations), - loss of social care on children, old peoples, ill and handicapped people, - mental detriment at staying in closed space (lift, metro tube etc.), - origination of panic and chaos, - increase of frequency of occurrence of criminal actions and attacks etc.
Critical infrastructure	- loss of function of supplies, operations and services that are depending on electric energy and by those massive limitation of capability to put the situation under the control and to ensure the return into stable conditions and renovation, - cascading effects and domino impact in systems and networks, - origination of unexpected very unfavourable situations as a consequence of unforeseen phe-

	nomena.	
	Energy supply system	- failure of heat supply from central sources (pumps and overpowering mechanisms), - failure of central gas supply as a consequence of loss of function of pumps and overpowering mechanisms based on electric energy, - failure of activities of storages (refrigerators, air-conditioning etc.), - outage of production, stores, physical and cyber networks and different services conditioned by electric energy supply.
	Water supply system	- failure of water supply into households, public facilities and operations (pumps, regulative mechanisms, control systems) and by that start of selected emergency conditions, - problems with regulation and maintenance of drinking and utilitarian water in tanks.
	Sewerage system	- loss of control of sewerage system, - putting out of operation of cleaning water plant, i.e. failure of waste water cleaning, - damage of pipes as a consequence of overfilling the pipes by waste waters and subsequent pollution of environment, subsoil liquefaction etc.
	Transport network	- failure of transport service based on electric energy (metro, trains, trams etc.), - outage of pumping fuel stations and mass stores of tractive material, - traffic jumps, traffic accidents and with time progress the lack of foodstuffs as a consequence of getting the traffic means into traffic jams etc. - failure of regulative mechanisms (lights on crossings, tunnels etc.), - lack of transport means that are not based on electric energy, e.g. busses substituting the metro).
	Communication and cyber systems	- loss of networks management during the time (after getting discharged redundant batteries), - loss of mutual connection (after getting discharged redundant batteries), - failure of cash dispenser safety protection, - failure of working performances controlled by cyber control systems, - loss of data put into information systems and databases, - loss of access to information put into media conditioned by operation of facilities droved by electric energy (after getting discharged redundant batteries).
	Bank and finance sectors	- loss of sector operation (banks, cash dispensers, insurance offices etc.) as a consequence of loss of access to data in information systems and in network and loss of function of controlled mechanisms, - loss on finance market as a consequence of sanctions provided for unrealised transactions and for wasted chances, - failure of cash dispensers and e-bank, - failure of service on clients, - loss of view on finance market as a consequence of loss of function of information means.
	Emergency services (Police, Fire Rescue Service, Medical Service)	- loss of foreknowledge from information sources dependent on operation of equipment droved by electric current from central sources, - loss of connection based on systems dependent on operation of equipment droved by electric current from central sources, i.e. problems with population warning, - in health service loss of capability to perform surgeries and provide the care based on performance of equipment droved by electric current from central sources, - stopping the maintenance and repair works based on operation of equipment droved by electric current from central sources.

	Primary services (foodstuff supply, waste liquidation, social services, funereal services), industry and agricul-	- stopping the production and sale of foodstuffs (dairies, bakeries, meat processing equipment, restaurant and workrooms preparing the food), - stopping the working plants for waste processing and liquidation, - in social service the loss of capability to provide the care dependent on operation of equipment droved by electric current from central sources, - stopping the store operation and the care on foodstuffs stored, - stopping the operation of schools, nursery schools and the other social facilities, - stopping the production of industrial plants, - stopping the agriculture plants dependent on operation of equipment droved by electric current from central sources, i.e. operation lines for feed production, equipment for drawing milk from cows etc.
	State and Regional Government	- loss of foreknowledge from information sources dependent on operation of equipment droved by electric current from central sources, - disruption of connection and loss of mutual communication and communication with citizens, - decrease of capability to manage the response to emergency and to sustain the situation in land under the control, - no chance to satisfy all tasks from responsibilities determined by legislation for state and regional governments dealing with good governance of public affairs, emergency management and crisis management.
	Public welfare	- stopping the marketing and services for citizens, - stopping the societal and cultural actions, - stopping the rehab and care personal services, - decrease of medical care service, - debase of medicaments and materials necessary for surgeries, - debase of foodstuffs and eatables, - decrease of level of hygiene.

4. To perform analysis and assessment of elements and networks of infrastructures, which are followed with regard to safety and development of human system, from the viewpoint of their function under normal, abnormal and critical conditions using the „All-Hazard-Approach“, i.e. to consider impacts of all possible disasters.
5. To perform analysis and evaluation of criticality of elements and nets of followed infrastructures in territory and to determine critical elements and nets of followed infrastructures by help of decision matrix (Figure 3) rating their vulnerabilities (considered aspects – small number, function is violate at each higher disaster that have impacts on a given territory, no redundancies, no alternative solutions, repair and renovation take weeks till months etc.) and capability of service of territory (number of human affected by failure, damages caused by failure of technology or infrastructure exceeding the acceptable level (according to the UN the high critical condition is if damages exceed 10% of annual territory budget), number of victims that cannot be averted by measures of crisis plans).
6. To process territory continuity plan for case of failure of one or more followed technologies or infrastructures that are on the criticality analysis critical for a given territory. From it to derive the demands for territory management under critical conditions in critical technologies and infrastructures. By application What, If method to derive situation scenarios in a real territory and to process procedures for coping the possible situations in a given territory with aim to prevent victims and human injuries and to reduce expenses on response by the way that at response the loss prevention will be sophistically performed [8].
7. By legal and finance support of critical infrastructure owners to ensure the alternative technical solution. I.e. to assign commitment to process continuity plans and to verify their effectiveness from viewpoint of territory of both, the territory needs and the adjusted technical conditions of operation that ensure feasibility of measures of continuity plans under all possible conditions, i.e. it will be performed back-up of technical elements and nets, safety system installation, installation of passive and active security elements etc.
8. For high critical situations to propose special measures for crisis plans in which there are implanted e.g. rationing systems for inhabitants, obligations to performed determined activities in a designated extent, time and quality by all

participated etc. To codify these special measures and to propose the way of their financing.

Regarding the core of critical infrastructure safety, the methodology for the critical infrastructure safety management (inherently containing the critical infrastructure protection) needs to lean on keeping the further given procedure [2-4], i.e. the management:

- is always directed to essential aspects,
- considers that the development needs to be sustainable and far-sighted (i.e. there must be balance among economy, technology, environment and social domain) and the primary target is the vulnerability reduction,
- pays attention to aspects that are the most vulnerable,
- defeats the emergency situations and during this it is directed to needs and priorities respecting that the basic priorities are the human protection and the protection of critical sources and systems on which the community existence depends,
- supports the prevention culture, programmes for the prevention and the preparedness to defeating the emergency situations and it insures that these items are included in the territory development programme,
- ensures that the citizens have right on rightful aid (remedial service) and that the aid is dispensed fairly and consistently without regard to economic or social circumstances and territorial location,
- ensures that citizens are included into the response management system not only as potential victims,
- ensures that citizens know emergency plans, content of plan of response to disasters, way of reaction and it's justifying at emergency situation origination etc.
- ensures that emergency management system is transparent also for citizens and it is adjusted to the local conditions,
- ensures that the emergency management system is legitimate and acceptable and it is based on systemic approach,
- ensures that the critical infrastructure safety (inherently including the critical infrastructure protection) is the matter of both, the private sector and the public sector.

For decision support system profiting the continuity of critical infrastructure at response and renovation of property in a territory affected by disaster is quite basic concept for determination of critical elements, critical processes, critical functions, critical infrastructures and critical technologies in a region. This concept leans on the risk analysis methodology and on actual terms of safety management in a region. It is possible to summarise that this process is determined by:

- way of assessment (acceptation) of risk, judgement and governance of risk,
- methodology of risk analysis and operation research,
- tools of safety management including tools of crisis management,
- specific particularities of cyber infrastructure,
- threat of conventional and unconventional terrorism,
- way of determination of priorities of system vulnerability,
- population awareness and by properties of postmodern society.

Reasons, why the critical elements, critical processes, critical functions critical infrastructures and critical technologies in the region are determined, are given by demand on reduction of risks in the human system from the view of its safety and development in the broadest sense. It is a matter of reduction of vulnerability (resilience increase) of key elements of human system that are basic for the society being on all levels of organisation and state administration, ensuring the functionality of life-giving systems and rational protection of critical infrastructure [2].

Regarding to the above given facts we can conclude that it is necessary to consider that the safe critical infrastructure we can ensure by two ways. The first one is more or less ideal and it consists in the construction of critical infrastructure on the "green field", i.e. from the beginning we create safe systems system (each partial infrastructure is also resistant against to failure of the others). For this case we need criteria, limits, standards and norms for removing the interdependences and spots with inconvenient risk potential. The other way, more realistic, consists in an application of site-specific measures ensuring the inherent mitigation of impacts of each individual infrastructure failure on the other parts of critical infrastructure; e.g. the others start independently to work in an insular regime.

At critical infrastructure protection during the whole life cycle we need to consider external and internal hazards including the social hazards covering the human factor and especially those humans that cause the organising accidents.

Up to now we have been mostly concentrated to technical domain, the research of which shows that

in practice it often comes up to failure of critical infrastructure from so called internal causes. Therefore, it is necessary to consider technical level, conditions and durability of a given infrastructure (35 – 40 years; max. 50 years), and the reality that through this time interval there need to be ensured the return ability of investments and that the human security needs not to be threaten. The longer time interval for which it is planned the infrastructure performance, the more modern (timeless) solution needs to be used. Each variant needs to be financially acceptable and needs to be also acceptable from the viewpoint of accessible technologies and of qualify human sources. At decision making on infrastructure renovation it is necessary to consider expenses and their return ability. Usually it is used a criterion that says "when expenses for infrastructure renovation do not return, e.g. after natural disaster to 10 years, so it is better to build new one". From the public interest view it is necessary to remove or to limit interventions of politics into decision making on the infrastructure in the territory because their targets are usually another than long-term safety including the functionality and reliability of infrastructure in the region without regard to a politic party in a power.

In the frame of ensuring the human system security and sustainable development, it is necessary permanently to perform the measures that reduce an infrastructure criticality in a region. By building the new infrastructure it is necessary to ensure suitable number and regional distribution of objects of important infrastructure that are sufficiently resistant to expected disasters in a given region, and by that systematically to reduce infrastructure criticality.

Expenses for critical infrastructure are not only costs for its design and building but they also include costs for its operation, maintenance, repair and modernisation. Therefore, the risks connected with each infrastructure need also to include the risks from just given domains and the region management needs to know how to deal with them. It is necessary to assess the risks from disasters that can be denoted as financial market failure because with them it is connected failure of finances for maintenance, operation, repair and modernisation of objects of critical infrastructure. It is caused by the fact that critical infrastructure criticality increases if not good maintenance and good repair are performed (which cause the vulnerability increases).

Because nothing is out of defects, it needs to be prepared the plan for renovation of each infrastructure, namely critical one. This plan needs to be proactive, properly assessed; it needs to contain transparently managed risks and answers to questions as: What to do?; How to do?; In which time interval?; Do not risks for other protected assets increase?; etc.

Because the critical infrastructure is a set of mutually connected (i.e. dependent) infrastructures, it is necessary to pay high attention to internal dependences study because analogy based on study of simple technological systems indicates that for critical infrastructure failure there are much more important links and flows that interconnect subsystems mutually. From the author's inspection experience it follows that couplings triggering the individual infrastructure failures and critical infrastructure failures often seem to be a random nature started by combination of several momentary weaknesses. For correct results we need in-depth analysis of sufficient number of critical infrastructure failures in connection with circumstances that were in their origin time.

The critical infrastructure protection means the ensuring of the continuity preservation of economic and social life of state and providing the response in case of danger or disruption of the basic conditions of life, services and systems, the continuity of which is fundamental for the State functioning. The main tasks in the field of critical infrastructure from a manager' point of view on the level of state are:

- to conduct the analyses of the vulnerability of critical infrastructure towards the possible disasters and attacks,
- to involve the legal, employee and citizens in the system of critical infrastructure protection,
- to elaborate a plan about removing of the biggest vulnerabilities of critical infrastructure,
- to elaborate a continuity plan for the individual critical infrastructures,
- to ensure the system of the detection of disasters and attacks (their possible scenarios) on critical infrastructure,
- to ensure the plan and realization of a response (its possible scenarios, means for its execution) to the functionality loss of critical infrastructure,
- to prepare the renovation plan for critical infrastructures,
- to provide education, awareness and collaboration of the public administration, private owners, employee and citizens in the issues of the critical infrastructure protection,
- to provide research and development for the needs of the functionality and protection of critical infrastructure,
- to provide intelligence analyses for the need of the critical infrastructure protection,
- to ensure the international cooperation at the protection of critical infrastructure,

- to ensure the legislative and financial demands for the need of the protection of critical infrastructure.
- the fact of the matter is that the major owners of critical infrastructure are the private subjects. Therefore, it is necessary that the critical infrastructure protection was an issue of both of the state and private sector. Until the effective mechanisms of management are not found, it will be necessary to use the tool of cooperation. We still have to look for a platform, on which the common way of funding the research will be sought and the way of funding the realization of relevant measures. If the State does not ensure the know-how, i.e. for example the monitoring of critical infrastructure, practice database for its operation and protection, units for its protection and relevant research, assessment and development of the approaches in protection and the relevant international cooperation, the private sector will cooperate with it because they don't have an easy access and possibilities of the creation of these tools [2].

For the ensuring of the reliable function of critical infrastructure, the relevant management [3,4] needs to respect the following principles:

- to always concentrate the activity on the fundamental aspects,
- to consider the early warning of citizens, employees, visitors before the up-coming disaster as a basis of success, as a basis of the reduction (or better the prevention) of the casualties,
- to set the target of management in a way that the sustainable development is ensured and that it would be far-sighted, i.e. so it would prefer the protection of lives, health and security of humans by paying the primary attention to the reduction of the system vulnerability,
- to always pay attention to the subsystem, which is the most vulnerable,
- to focus on the needs and priorities at dealing with emergency situations, while the basic priority is the protection of humans and the protection of critical sources and systems, on which the existence of society depends,
- to support the safety culture and to pay the maximal attention to prevention,
- to include the ensuring of preparedness on the emergency situations handling to the programme of the area development,
- citizens have the right to help (assistance service) and the help must be rendered consistently without regard to the economic and social circumstances and the area setting,
- citizens belong to the system of response to emergency situations not only as potential victims but also as the active elements of the response,
- to arrange, so as the citizens knew, what the crisis plans and response plans on emergency situation are and what do they bring about, what is their responsibility, how can they help in the prevention of the disaster or emergency situation emergence, how should they react and why, etc.,
- both, the system of safety management and crisis management need to be transparent even for citizens and must be adjusted to the local conditions,
- both, the system of safety management and crisis management need to have legitimacy, need to be sustainable and acceptable and need to be based on the systematic approach.

It is rational that it is not possible to include in the critical infrastructure all the facilities and all the networks of the observed sector, but only the priority ones. This priority facilities and networks are ensured specially. Each element of critical infrastructure consists of several different elements that are fundamental for its functionality. These are: the critical constructions composition (objects, networks); critical structures; critical machines and means of production and service; critical materials, critical parts of I& C; and critical personnel.

It is necessary to determine those elements and links that are important for the ensuring of the survival of humans and for the protection of their lives and health. This special protection requires finances, material sources and educated personnel. The analysis of real situations [5,16] often shows that the most important is usually the qualification of the top management, which controls the area and the personnel, which executes the measures in the area. Because the sources are limited everywhere, only the priority elements are being protected. It is also the truth that the easily attackable structures, based on the complicated technical accesses, are often replaced by the flexible and simple technical solutions that are able to work in the difficult conditions of critical situations [2].

Methods of the choice of priorities are usually very expensive. In practice, the method of multicriterial assessment, based on the evaluation of the vulnerability of the individual elements in system proved useful. At the selecting, the variants meaning the big vulnerability at individuals and little vulnerability at society are preferred [2]. At the assessment, it is necessary to classify rather complicated system of links, in which it is not possible to quanti-

fy the effect of the individual factors. Therefore, the total evaluation is relative and can be influenced by the subjective approach of single evaluators. On that account, it is worthwhile, if the evaluation is conducted by several mutually independent experts. The results of the evaluation count only for the evaluated system and it is not possible to compare them with results of the evaluation of different systems assessed separately. Therefore, in the USA and several other countries the expert methods are codified for these complicated evaluations, e.g. the multistage Delphi method [2].

At the determination of critical infrastructure and technologies in area, many factors need to be considered and between the most important; there are: operating and maintenance expenses for the lifetime period; and preventive service and repair measures expenses during the response and renovation.

For each of the elements, the criteria need to be defined for the assessment of the physical conditions (respecting both the character of critical infrastructure and demands for the physical infrastructure), capacities and demands for services and for functionality assessment. On the basis of these criteria, the state of element is quantitatively assessed by a verbal scale containing levels from "very good" to "bad" and "critical (i.e. very bad)". The five-level scale is appropriate:

- very good state: the element is in a perfect physical state and it fulfils the intended functions. The expenses for maintenance are in accord with standards and norms. The element is new or recently renovated. Requirements for operation correspond to the project, there are no operational problems. The whole programme is being fulfilled efficiently and effectively,
- good state: the element is physically in a good state and it fulfils the intended functions. The expenses for maintenance are in accord with standards and norms but they are growing. The element is approximately in a half of its lifetime period. Requirements for operation correspond to the project, occasionally there are operational problems. The whole programme is being fulfilled acceptably,
- acceptable state: the element shows the signs of wastage and lower efficiency than it was intended. Some parts are already insufficient. The expenses for maintenance overcome the sums set by standards and norms and they are growing. It was used for a long time and it is in the last phase of its lifetime period. Requirements for operation correspond to the project, the operational problems are frequent. The whole programme is largely being fulfilled but the ineffective and inefficient ways of fulfilment occur,
- bad state: the element shows the significant signs of wastage and it fulfils the intended functions on a low standard. Many parts are insufficient. The expenses for maintenance overcome significantly the sums from standards and norms. The element comes near the end of its lifetime period. Requirements for operation overcame the data in project, the operational problems are apparent. The whole programme is being fulfilled only in a very limited range,
- critical state: the element is in a bad state and it does not work as it should be. There is a high probability of its failure. The expenses for maintenance are absolutely unacceptable in comparison with standards and norms; renovation is not cost-efficient. The replacement is necessary. Requirements for operation overcame significantly those in the project; operational problems are serious and continual. The set program is not being fulfilled.

For ensuring the continuity of critical infrastructure is considered [2-4] it is necessary the answer on the following questions is being sought:

1. What is the concept, on the basis of which the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area are determined?
2. Why the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area are determined in that way?
3. How is the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area executed in practice and to whom it serves?
4. Where is the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area used?
5. What are the requirements (data/equipment/intellectual potential etc.) necessary for the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area?
6. Who conducts the determination of the critical elements, critical processes, critical functions, critical infrastructure and critical technologies in area?
7. What are the advantages and disadvantages, weak points in the determination of critical elements, critical processes, critical functions, crit-

ical infrastructure and critical technologies in area?

The existing concepts [2-14,16] show that the word "critical" is used either for the indication of the condition (state) of element / property / process etc. or with regard to the importance of element / property / process etc. for the area functioning. In the area of management, the word "critical", e.g. in a phrase "critical disaster" means a disaster that is fundamental for the process of management functionality. In this concept, also the term "emergency management critical function" is used, which is applied in the response plans on emergency situations that are compiled in the USA [9].

On the basis of the critical analysis of information in professional literature, stated in [2-4], and experience from practice, the scale is proposed this way:

- level 0: the losses on infrastructure or technology do not have any impact on the safety and development of the area,
- level 1: the losses on infrastructure or technology have low impact on the safety and development of the area,
- level 2: the losses on infrastructure or technology have a medium impact on the safety and development of the area,
- level 3: the losses on infrastructure or technology have a significant impact on the safety and development of the area,
- level 4: the losses on infrastructure or technology have a serious impact on the safety and development of the area,
- level 5: the losses on infrastructure or technology have a fundamental impact on the safety and development of the area; they bring about its collapse.

In view of the area functionality, it is also necessary to assess the time period, in which it is possible to repair or replace the damaged infrastructure or technology. For the verification in practice, in [2-4], it is proposed to assess according to the following value scale:

- level 0: the damaged infrastructure or technology can be repaired or replaced in a time interval of 0-5 days,
- level 1: the damaged infrastructure or technology can be replaced in a time interval of 6-30 days,
- level 2: the damaged infrastructure or technology can be replaced in a time interval of 31-90 days,
- level 3: the damaged infrastructure or technology can be replaced in a time interval of 91-180 days,
- level 4: the damaged infrastructure or technology can be replaced in a time interval longer than 180 days,
- level 5: the damaged infrastructure or technology cannot be replaced.

It is necessary to get into practice the consciousness that the failure of critical infrastructures need to be evaluated at the risk assessment of enterprises / area / state, because the losses brought about by their failure deeply affect both the activity of every enterprise and its further existence. The systematic tool is the continuity plan that should be elaborated for the priority structures and networks of critical infrastructure [2-4]. I.e. it is necessary to introduce, both to the practice of public administration/ organizations and enterprises, the system:

- analysis of the impacts of the relevant natural and other disasters on enterprise / area / organization / structure / network etc.,
- assessment of risks and the ensuring of the sophisticated risk management,
- defining the management strategy of the continuity of both business and life in area, in case of unacceptable risks that remained, for some reasons, after the application of the measures of risk management,
- defining the emergency response and emergency activities for the case of natural or other disasters occurrence, i.e. if the realization of risks,
- processing and the implementation of the continuity plans of business and of crisis plans (for the case when the continuity plans fail),
- ensuring the consciousness and training of participants,
- actualisation and practising the existing plans,
- preparation and practising the crisis communication
- connection to offices and bodies outside of business/ structure/ network/ area etc.

The total investigation that is necessary to conduct for the ensuring of safety and development of critical infrastructure and technologies of organization / enterprise / structure / area / region / state/ community under the tools of safety management has also a general framework [2-4], which consists of the answers to the 14 following questions:

1. ***What natural or other disasters*** can appear in infrastructure location and what impacts do they have?
2. ***Where*** can natural and other disasters in infrastructure location appear and ***in what way*** are their impacts placed in infrastructure?
3. ***In which conditions*** can natural and other disasters in infrastructure location appear and what

conditions can cause the escalation of their impacts?

4. ***How often*** can natural and other disasters in infrastructure location occur?
5. ***From what size*** do natural and other disasters in infrastructure location have undesirable and unacceptable impacts that cause damage on protected assets?
6. ***What is the maximal possible (expected) size of natural or another disaster*** in a given infrastructure location?
7. ***What damage*** on protected assets can cause the maximal possible or maximal expected natural or another disaster determined on the specified level of credibility in infrastructure location and what are its greatest possible impacts on infrastructure location and especially on the human society?
8. ***What we can do to avoid the undesirable and unacceptable impacts of natural or other disasters*** in infrastructure location in the section of land-use planning, designing, construction and operation of both public and private infrastructures or possibly in other fields, such as monitoring, inspection, education etc. so that we could avoid the disasters, which can be avoided or so that we avoided undesirable and unacceptable impacts, or at least, so that the undesirable and unacceptable impacts were reduced by preventive measures, preparedness, suitable response on a disaster and renovation, at which the prevention of losses and targets of suitable development will be respected?
9. ***What measures towards the real natural or other disasters*** in infrastructure location in the technical, organizational, financial, social, legal, educational and training section are desirable?
10. ***What unacceptable and remaining risks*** (i.e. the unacceptable impacts with the probability of occurrence higher that the set limit) with regard to possible natural or other disasters in infrastructure location remains, if the rational measures are executed that can the state/ public administration/ organization ensure in the technical, organizational, financial, social, legal, educational and training section?
11. ***In what way to execute the response on natural or another disaster***, what are its priorities, critical points etc.?
12. ***How to execute the renovation*** of infrastructure after natural or another disaster, so that the sources, forces and means were used rationally and so that other losses were prevented, the resistance increased to possible other disasters and the further development was started in infrastructure with all the elements of the human system (humans, environment, property, infrastructure, technologies etc.) that form it.
13. ***What form of the management*** and executing of the renovation of infrastructure and protected affaires after natural or another disaster in infrastructure is suitable and how it can be executed?
14. ***How to create the potential and financial reserve*** of infrastructure organization for the rational renovation of the infrastructure after natural or another disaster?

The up-stated results show that the domain of critical infrastructure is vivid and that there exist many unresolved problems. Therefore, it is necessary to continue the research and to prepare the application of its results into practice.

The gathered knowledge shows that the problem of critical infrastructure protection is a complex problem. The basic concept of protection needs to be based on the area planning and on the following activities. Because it is not possible to put out the entire existing critical infrastructure by a single act and replace it by the modern one, which fulfils all the ideal requirements and demands, many tasks exist also in the section of response. Therefore, these have an important place: special plans of response for critical infrastructure that are processed by the proprietor/ keeper/ holder of the licence of critical infrastructure; continuity plans from the side of the proprietor / keeper/ holder of the licence of critical infrastructure that ensure survival / minimal functionality of critical infrastructure for the fulfilment of the demands of area, the services of which depend on this infrastructure; continuity plans from the side of the guardian of area and the protector of the public welfare and public assets, that is the public administration ensuring the safety and development of area; and crisis plans from the side of the proprietor / keeper / holder of the licence of critical infrastructure that ensures the survival of his business and will not cause unacceptable impacts on the protected assets, especially the human health and lives.

This means, that the basic concept of the critical infrastructure protection needs to be processed on the basis of the philosophy of safety management (integral / complex, i.e. not integrated / aggregated) and from it, we need to deduce the requirements for the response and renovation management for the case, where critical infrastructure is affected by unacceptable impacts caused by natural or another disaster. Only from this concept, it is possible to deduce the way of participation of executive units and their tasks.

Without enforcing the logical procedure and connection of activities, all the processional models created with the best intentions will represent the solution of the problem by a method ad hoc or differently defined as the method of the immediate idea/ impulse/ inspiration etc. All the publications cited in the lists of sources and that describes methods and principles suitable for the processional analysis conduction and for the seeking of critical links among the individual elements of critical infrastructure are based on causes, i.e. on disasters or inner links, that go across the individual infrastructures or across several infrastructures (electricity, informational technologies, anthropogenic management, financial flows) and not on the states, i.e. emergency situations.

The processional analysis is done in this way:

1. Concept of safety management is applied with the assessment of the whole process connected with the existence of critical infrastructure, i.e. the placement, designing, projecting, construction, operation and changes.
2. The processional model is compiled for the entire process connected with the critical infrastructure existence and only then, there are selected the models for the partial tasks or the very detailed models for the parts being a subject of a special interest are created.
3. The All Hazard Approach is used. This means that the protection against all the relevant disasters is ensured according to the laws, norms, standards and approaches of established practice for the area planning, choice of places, designing, projecting, construction, operation, repairs, maintenance, changes and renovations
4. The suitable methods of safety engineering are being used and that both for the determination of the risks' size and for the determination of the priority risks that contributes the most to the vulnerability of a given infrastructure.
5. Risks are understood as losses, damage and harms on the protected assets in a concrete area, i.e. not as numbers of no clear expression of the negative potential. At existing infrastructures, the existing risks are found out, the risks that contribute the most to the vulnerability of a given infrastructure are determined and to them the inner emergency plans, plans of continuity and possibly also the crisis plans are prepared.
6. For the critical links searching between the individual elements of critical infrastructure the decision matrixes are used the most often. Because the practice, time to time, also requires the resolving of the special tasks, for which the application of the criticality matrix (i.e. the decision matrix for the critical infrastructure) is a too broad tool, the more precise methods are used, based on the theory of graphs; and that e.g. the method of critical path (so-called CPM), method of the optimization of resolving the problem in time and space (so-called PERT) and method of the modelling of processes in a network (so-called Petri net).
7. For the ensuring of the critical infrastructure functionality in time and space, the specific control lists are used. This method is common mostly in the public administration and the inspectorate bodies.

So that the State could fulfil its function i.e. to ensure the protection of protected affaires, for which he was created in antiquity, it has to have the functioning critical infrastructure and technologies. This means that in the normal, abnormal and critical conditions the basic elements, links and flows in the state system must be in function that are the basis of the state ability to reach stability at any situation and to start the further development [2-15]. This means that the protection of critical infrastructure needs to belong among the objects, which are the subjects both of the safety management of area and crisis management [2-4].

The Conference "Critical Infrastructure Protection and Resilience Europe" [17], which held in Milan on October 14 -16, 2019 included serious information, such as:

1. Today, in time of using the advanced automation and remote-control systems of technical devices, the critical infrastructure elements are attacking from space. A number of attacks were presented – e.g. an attack from a satellite: on an equipment that checks employees when they arrive at work at a nuclear facility – the attack caused the employees could not enter in the facility, and therefore, shifts could not be replaced; on the company's management centre caused the centre to be overwhelmed by a large number of queries and the subsequent interruption of the production process; from the satellite knocked out the equipment measuring water in the boiler and caused the boiler to overheat; etc. The term "new risks from space" began to be used. Additional risks are expected when quantum computers are introduced into widespread use – the number of cyberattacks will increase.
2. In the vast majority of reports, there was a recommendation on the need to use a systemic approach using multi-criteria methods based on DSS (decision support system) and finding that only a proactive approach can provide critical infrastructure protection. E.g.: very popular are

smart grids, and yet when put into practice, the risks associated with them are not addressed (there are no plans for response in case of their failure); analyses of criticality of energy infrastructure revealed 28 critical elements for that need to be upgraded; and many risks are associated with the "Internet of thinks" network – interconnected chains are created where it is not easy to identify the originator of a malicious message (e.g. damage to the good will of the critical infrastructure manager), and therefore, the principles for response plans for the implementation of cyber risks need to be drawn up.

3. In several reports there was a complaint about the poor-quality work of software processors – they do not give a deliberately thorough description of the software + instructions with corrective measures in case of failure – it was suspected that in this way software companies procure themselves work for the future. Even several specialists have stated that the same practice occurs in the design and construction of technical elements of critical infrastructure.
4. Based on an analysis of security events in critical infrastructure, the UK specialists have shown the following breakdown of causes: cyber-attack 42%; insider attack 28%; terrorist attack 15%; failure of human factor 14%; natural disaster 1%; and attack CBRNE 1%.
5. For increasing the safety and reliability of critical infrastructure, it is necessary in terms of references of critical infrastructure elements and whole to use the disaster sizes with a return period of more than 100 years. Another mistake is that during the design, it is only carried out the protection of elements and objects only for individual listed disasters, i.e. other some possible and unnamed disasters are not considered – it is necessary to use the application called "All Hazards". As critical infrastructure provides vital functions for humanity, care needs to be taken to ensure the continuity of operations, for which resilience is important. The idea of resilience is portrayed as the intersection of three circles, Figure 5. Resilience means continuously increasing both, the safety and the security while addressing potential conflicts that arise in practice; E.g. in present automobile industry [18].

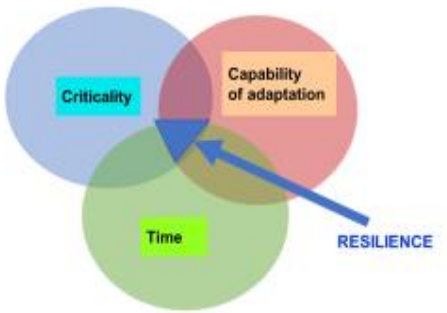

Fig. 4. Critical infrastructure parameters that are important for resilience.

References:

[1] KERTIS, T., PROCHÁZKOVÁ, D. Problems of Safety of Automation of Car Control (in Czech). In: *Řízení rizik procesů spojených s technickými díly*. ISBN 978-80-01-06656-0. Praha: ČVUT 2019, pp. 65-75. http://hdl.handle.net/10467/ 85587

[2] PROCHAZKOVA, D. *Challenges Connected with Critical Infrastructure Safety.* ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.

[3] PROCHAZKOVA, 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

[4] PROCHAZKOVA, D. *Safety of Complex Technological Facilities.* ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244p.

[5] HAYS, W. (ed.) *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters", Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards", Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters*. Washington: ASCE 2001.

[6] EMA. *Critical Infrastructure Emergency Risk Management and Assurance*. Handbook Emergency Management Australia, 2003, www.ema.gov.au

[7] FEMA. *Promoting Critical Infrastructure Protection by Emergency Managers and First Responders Nationwide*. Washington: FEMA 2005. www.usfa.fema.gov

[8] EU. *Green Paper on European Programme for Critical Intrastructure Protection*. Brussels: EU 17.11.2005, COM(2005) 576.

[9] US. *Critical Infrastructure Conception*. Washington: Government 2001.

[10] ESRIF: *ESRIF Final Report*. Brussels: EU 2009, 311p.

[11] US. *Federal Response Plan*. Washington: FEMA 1999, 304 p.

[12] US. *Emergency Management Plan*. State of Texas 2000.

[13] US. *The Tennessee Emergency Management Plan*. State of Tennessee 1995.

[14] FEMA: *Interim Assessment Guide for Hazardous Facilities*. Washington: FEMA 1999.

[15] GUSTIN, J. F. *Disaster: Recovery Planning: a Guide for Facility Managers*. ISBN: 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn: The Fairmont Press, Inc. 2002, 304p.

[16] CLOAKE, T., SIU, L. K. *Standardized Classification System to Assess the State and Condition of Infrastructure in Edmonto*n. In: *Conference INFRA*, Montreal 2002.

[17] IACIPP. *Critical Infrastructure Protection Proceedings.* Milan: CIP Association 2019, www.cip-association.org