Critical Infrastructure Safety Management

D. Procházková*
Institute of Security Technologies and Engineering, Faculty of Transport Sciences, Czech Technical University, Prague
** Corresponding author: prochazkova@.fd.cvut.cz*

DOI: 10.2478/v10158-010-0022-0

ABSTRACT: Critical infrastructure is a set of mutually interconnected networks, i.e., the systems of various sectors of a human system. An interconnection of systems means their mutual dependence. Therefore, in connection with safe critical infrastructure and with sustainable development potential, it is necessary to solve several problems, namely the safety of partial infrastructures and the safety of a set of mutually dependent infrastructures. With regard to present knowledge we know that the optimum safety of the set of infrastructures is not the set of optimum safeties of partial infrastructures, and, therefore, we must search for a solution in a different way. The work shows a possible approach for solution acquisition. The paper searches for the principles for safety management of critical infrastructure by logic analysis and the synthesis of present findings and experiences.

KEY WORDS: Critical infrastructure, interdependences, safety, dependability, vulnerability.

1 INTRODUCTION

From the societal viewpoint critical infrastructure represents mutually interconnected networks and systems that include the identified sectors and institutions (including humans and procedures) that provide the reliable flow of products and services substantive for defensive and economic safety, which is understood as the state's capability to compete on global markets, while being on an acceptable level of real public income, and the public administration functioning on all society levels (Moteff et al. 2003). This means that the critical infrastructure is a set of partial infrastructures from different sectors of a human system (see e.g., act No. 183/2006 Col.), that are composed of physical elements and of processes that used these elements for the fulfilment of the tasks of each partial infrastructure. The functionality of this set of partial infrastructures predetermines the human system safety (Prochazkova, 2007a). It is caused by the fact that to economic safety are joined other ones (Moteff et al. 2003), the physical safety that is connected with risks caused from disasters of all kinds, and the cyber safety that is connected with disasters affecting computer networks. Individual items of each infrastructure, according to this work, are subdivided into elements and typical processes according to the distribution, storage, payments, recycling, data transfer, transport, etc.

Critical infrastructure and critical technology in the human system ensure services in a territory, i.e., a certain quality and hierarchy of public services. A measure of the level of services in a territory consists of a judgement of the different sorts of services that have

a different importance from the viewpoint of life and the security of humans in an integral sense. In reality there are different sorts of services are ensured by different partial infrastructures that are dependent because, among them, there are interdependences. This fact always manifests during severe disasters (beyond design disasters) when the beyond standard preventive measures are only implemented in special cases in harmony with the legislative demands, and also protective systems, built into the frame of emergency and crisis managements, are only created for selected protected interests (human lives and health, property). Vulnerabilities of partial infrastructures induce cascades of phenomena that cause the failure of other infrastructures, i.e., when the loss of services in territory has secondary impacts on humans and property, so-called interdependences are shown, e.g., in the workplace (Prochazkova, 2007b). This means that in human system safety management the links going across the individual partial infrastructures and across the critical infrastructure and across the human system have not yet been sufficiently considered. For the security and sustainable development of humans it is necessary to solve this problem, and, at least, to remove or to reduce to an acceptable level the secondary and higher order impacts in impact chains that are connected with the start of the occurrence of real disasters (Prochazkova, 2007b). For this reason in practice significant features of critical infrastructure have been followed, understood as a system created by the connection of partial infrastructure systems, that predetermined its functionality and that are mutually dependent. Only with the application of measures that consider the above-given facts is it possible to ensure the quality governance of public affairs in the territory and to fulfil the age-old human dream, i.e., the security and sustainable development of territory and of human society. All of the above-mentioned, and to be mentioned, facts for critical infrastructure are also valid for critical technologies.

In other words, critical infrastructure is the physical (technical and material), cyber, and organisational subsystems of a human system that is necessary for ensuring the protection of human lives, health and security, property and the minimal development of the economy and the administration of the state. The subsystems of critical infrastructure and their number have not been stable in the world (Prochazkova, 2007b). With regard to the documents accepted by the Safety Board and Government of the Czech Republic in 2002 critical infrastructure includes such items as: the energy supply system, the water supply system, sewer system, transport system, communication and information systems, the banking and finance system, emergency services (police, fire rescue service, medical rescue service), basic services (food supply, waste liquidation, social services, funereal services), industry, agriculture, state and regional administrations. Each of the given items is a system with elements, links and flows determined by infrastructure nature. In further text we use a recent concept that the critical infrastructure safety includes both the functionality and the reliability of critical infrastructure.

The aim of the paper is to summarize present knowledge and experiences on critical infrastructure, to judge the role of technical factors and to apply logic methods for the derivation of principles for critical infrastructure safety management from the viewpoint that critical infrastructure is protected against internal and external disasters, and, simultaneously, does not threaten its vicinity and correctly fulfils the expected functions for territory.

2 ASPECTS CONNECTED WITH CRITICAL INFRASTRUCTURE SAFETY

From the above-given description of critical infrastructure it follows that the critical infrastructure is a system composed of mutually interconnected systems. In this coherence it is important that mutual interconnection means dependence. The safety of each system,

understood as the set of measures that ensure the safe infrastructure that can sustainably develop depends, of course, on the infrastructure nature. The system safety inherently includes the system protection. The safety of the system that is a set of mutually dependent subsystems is predetermined not only by the safety of the individual subsystems, but also by the character of mutual interconnections.

According to the work (Stein et al. 2003) the interconnection means the dependence of at least two subsystems. By means of this interconnection the condition of one subsystem influences or correlates with the condition of other subsystem. The given definition can be extended by the condition of mutually sharing the several physical elements or processes with those elements or processes that can be situated in a given territory. Therefore, the mutual dependence in the territory may be physical, cyber, logical and regional.

It simultaneously holds:

1. Partial infrastructures are physically mutually dependent if the condition of one of them is dependent on a material output of the other.
2. Cyber mutual dependence means that the condition of one infrastructure depends on information from the other. Cyber mutual dependence requires the existence of information infrastructure.
3. Infrastructures are regionally and mutually dependent if the events in a region can change the conditions of partial infrastructures.
4. Logical mutual dependence means that the condition of one partial infrastructure depends on the condition of the other with the fact that a mechanism of interconnections is not physical, cyber or regional. It takes the dependences transferred through flows created by rules, finances, legislative etc., e.g. finance markets.

In the work (Stein et al. 2003) there are characteristics of partial infrastructures completed by other items when there are the types of malfunctions and failures (cascade and escalation malfunctions, defect for one cause – e.g., natural disasters), the operation conditions (normal, abnormal, critical), the measure of the tightness of relations and interconnections (free, tight, complex) and the critical infrastructure characteristics (time, spatial, organisational, proprietary and institutional).

As a consequence of mutual dependence the defect or failure of one partial infrastructure causes the defect or failure of the other. This fact contributes to the criticality of the system, called in the following case as the critical infrastructure that is the set of subsystems. Therefore, it does not suffice to ensure the safe subsystems separately, but instead it is necessary to systemically ensure the whole set of subsystems, which in practice means to search for the solution to a problem called the systems system safety (Prochazkova, 2008).

The reality is that each partial infrastructure and the whole set of such infrastructures is a complex dynamic system with a given level of adaptability. For ensuring its stability and functionality the threshold value must be known – the criticality that determines the condition at which the system does not ensure expected functions within a required time, a site, and in a required quality. The criticality of each partial infrastructure can be approached from two viewpoints, teleological and systemic (Eda, 2005):

1. From the teleological viewpoint it follows that the criticality is a result of the role and function of partial infrastructure in the society. This concept enables one to work with non-network and non-technical objects and processes.
2. Partial infrastructure criticality from the systemic viewpoint is a result of its position in the system or of its link to another partial infrastructure.

From both approaches it follows that the partial infrastructure criticality also influences the system that is a social partial infrastructure created by public administration, business subjects, educational and research institutions, and civic clubs.

Adopting the findings from the systems' system safety management (Prochazkova, 2010) the set of partial infrastructures in a region is a critical one if it is only capable of ensuring activities at which the only assurance is human survival in the region. For this purpose the analyses of sectors to which individual partial infrastructure belong have been performed in the world and they have followed the dependences among sectors, and the safety management that respect both the conditions for the functionality of individual partial infrastructures and the conditions for the functionality of a set of infrastructures; aggregated (critical) infrastructure. The term "criticality" was first used in connection with the nuclear reaction, where it denoted the threshold after which the spontaneous chain reaction followed. In connection with partial infrastructures and with critical infrastructure (the set of infrastructures) the criticality is, according to sources given in (Prochazkova, 2008), most competently expressed by the following definitions:

1. Criticality is a relative measure of impacts of frequently occurring defects and failures.
2. Criticality is expressed by conditions that describe a transition between quality changing conditions.
3. Criticality is a condition of extensive urgency.

From the given criticality definitions it is possible to derive that criticality is a threshold value that may be designed and that can relate to an event, process / function parameter, type of defects and/or resistance.

The determination of criticality is consistently related to the size of impacts caused by loss of the functionality of each infrastructure in the society. For criticality determination the following must be considered:

1. Concentration of humans and assets (protected interests).

2. Sectors of economy (sector analysis).

3. Types of mutual dependences among the partial infrastructures / sectors:
   i. On which item the assets of a given sector are dependent?
   ii. What is the mutual dependence of assets among sectors?

4. Types of services for the public:
   i. How long has the renovation of services furnishing taken?
   ii. Which compensation / substitutes can be accessible and available?

5. Public confidence in the public administration institutions:
   i. Can the defect of assets / public services result in a drop in the morale of citizens, a loss of national prestige, panic, rebellion, or civic disorder?
   ii. Can the defect of assets induce some impact / changes in the environment?

The determination of criticality in the service of territory can include the hazard assessment for disasters possible in a given region, considering the vulnerability of partial infrastructures in a given region, the mutual interconnections of partial infrastructures in a given region, i.e., theoretically the same principle as in the analysis and assessment of risks in a region, at which several protected interests are considered.

Therefore, the criticality determination process is the following:

1. Characteristics of assets (protected interests that are considered physical, cyber and human assets).
2. Determination of criticality (hazard analysis and consideration of the assets vulnerability in a site).
3. Assessment of impact on assets (concentration of humans and assets, economic impact, mutual dependences, reliability).
4. Assessment of consequences of losses, victims, damages and harm to assets.
5. Determination of priorities according to the given rules.

Analysis of data in literature, provided in the list and summarised in the works (Prochazkova, 2007b, 2008), showed that most of the procedures correspond to the above-mentioned general procedure, and the criticality is mostly determined by scoring, i.e., with a decision making matrix (Highway, 2002).

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

- "high vulnerability and high importance of service" the condition of the infrastructure / technology / set of infrastructures is precarious, i.e., critical for a given region and from the viewpoint of security and sustainable development the situation must be solved through back up and enhancement of the given infrastructure,

- "lower vulnerability and lower importance of service" the condition of infrastructure / technology / set of infrastructures is satisfactory and it is necessary from time to time to perform a check-up of conditions in a given region,

- "high vulnerability and lower importance of service" the condition of infrastructure / technology / set of infrastructures is conditionally satisfactory and it is necessary to ensure preparedness for a sophisticated response in the case of infrastructure / technology / set of infrastructures failure and prevention to concentrate on preventive and mitigation measures leading to the reduction of infrastructure / technology / set of infrastructures vulnerability against possible disasters that can cause the failure,

- "lower vulnerability and high importance of service" the condition of the infrastructure / technology /set of infrastructures is conditionally satisfactory and it is necessary to ensure the preparedness for a sophisticated response in the case of infrastructure / technology / set of infrastructures failure and the prevention to concentrate on a reduction of the criticality of the infrastructure / technology / set of infrastructures in a region or to build redundancies of being objects of infrastructure / technology / set of infrastructures.

It is true that above-described procedure shows that the assessment of infrastructure / technology / set of infrastructures according to two criteria, namely the measurement of vulnerability and measurement of the importance of the service in a region is not a result of an objective computation of process analysis but rather the result of subjective estimations which is only tolerable in the case of the determination of a basic frame. The determination of criticality for some processes can be more complex.

When scoring the vulnerability and importance of a service it is necessary, in harmony with the work (Highway, 2002), to consider the following items:
- duration of renovation of infrastructures and technologies,
- impact of failure of infrastructures and technologies on human lives and security,
- caused detriment, harm and loses,
- impacts on environment,
- induced adverse interest.

From the viewpoint of human system safety (i.e., the security and sustainable development of human society) it is necessary to ensure the quality services in a region that are conditioned by the operational dependability of the critical infrastructure, understood as the systems system.

3 PROPERTIES INFLUENCING THE DEPENDABILITY OF PARTIAL INFRASTRUCTURES AND OF CRITICAL INFRASTRUCTURE

The dependability of partial infrastructures, and also a critical infrastructure, is the element that humans can influence. System dependability means that the system fulfils the given demands and its operation satisfies the given conditions. This aggregate property is not very practical for analytic purposes, and, therefore, it is broken down into two basic properties, as the vulnerability and the resistance are in the sense of the resilience. The following dependences are in force:

Vulnerability = f *(exposure, perception / sensitivity)*
Vulnerability = f *(sensitivity, dependability, life cycle)*
Resilience = f *(life cycle, ensuring, functional capability, operational readiness, adoption capacity)*

To reach a given level of dependability of partial infrastructures and a critical infrastructure both following points must be considered- the vulnerabilities against possible disasters (in the case of critical infrastructure including interdependences induced by mutual interconnections) and the human capabilities and opportunities to ensure a certain resilience. It is necessary to understand that the resilience is a certain functional capability of critical infrastructure to fulfil the tasks also during abnormal and critical conditions. To reach this condition it is necessary that critical infrastructure might attain a certain adoption capacity.

The dependability is a designed property and it is related not only to normal conditions, but also to abnormal and critical conditions at which, through the adoption capacity of critical infrastructure or critical technology, ensures the required reactions also during certain types of critical conditions. Usually, the critical conditions expected are considered in the sitting, designing, building, and operating of the infrastructure or technology, i.e., the foreseeable impacts which would be highly unacceptable (i.e., it is considered the precaution principle). Nevertheless, would be critical conditions could happen that are either unforeseeable or the result of a relevant fault of the operator and these can pass to inconvenient / unacceptable conditions, i.e., crisis conditions (Prochazkova, 2008).

The crisis potential can be expressed as a contemporary action of a trigger factor (trigger factors) and of non-steady conditions of a critical infrastructure setting, i.e.:

Crisis potential = trigger factors * non-steady conditions of setting

Likewise at the risk there is evaluated the occurrence probability, so also at crisis potential it is evaluated the crisis condition occurrence probability, namely including the assessment of impacts that are mentioned as the relevant disruption of functions of elements and processes of the critical infrastructure.

From the dependability it follows that the critical infrastructure, the system which plays a key role in a society, as it affects the decision making cycle of public administration and political and social solidarity, and supports the removal of physical and psychological harms, is very complex, and thus vulnerable. Therefore, in assessment three basic properties of critical infrastructure could be described and characterised, namely: resilience; vulnerability; and adoption capacity.

For the reason that today starts to approach the critical infrastructure as a complex socially-technological system (including mass flows, energy flows, information flows and reverse links including recycling) in the frame of societal metabolism, so the following definitions are:

1. *Resilience:*

Resilience is the capability of a system to adsorb and to use the deviations and changes so that it lives through them without the chance that quality changes of its structure might originate (Holling, 1973).
Resilience is a measure of such an extent of deviations that the system may absorb before the transition from one condition to another (Gunderson & Holling, 2002).
Resilience is a measure of a system's return rate to the balance condition (Gunderson & Holling, 2002).
Resilience is an extent of deviations that a system may absorb without a change to its stability (Gunderson & Holling, 2002).
Resilience determines the reactions remaining in a system and it is a measure of a system's capability to absorb condition changes (Franklin & Downing, 2004).
Resilience is a measure of the rate of a system's recovery from deviations (Adger, 2000).

2. *Vulnerability:*

Vulnerability is expressed as a relation between the exposure to hazard from an external activity and the capability of risk reduction in a certain time (Langeweg & Espeleta 2001).
Vulnerability is a measure of experiences of a system, subsystem or an element with damages that may occur with exposure to harmful phenomenon that induces a stressor (disaster) or deviation (Science, 2000).
Vulnerability expresses a measure between the system exposure to unforeseen phenomena and the load and the difficulty that is connected with their defeating (Chambers, 1990).
Vulnerability expresses a system capability of reacting to the occurrence of a harmful unfavourable event (Watts & Bohle, 1993).
Vulnerability is a result of a combination of exposure, resistance and elasticity (Dow, 1991).

3. *Adaptation:*

Adaptation is related to an unplanned reactive response to events or to conditions with the aim to avoid the unacceptable impacts through anticipating reactions (Glantz, 1992).
Adaptation includes changes in a system as a result of reaction to the manifestation of external forces or deviations (Smithers & Smit, 1997).

For designing the infrastructures and technologies we have been solving up to now the problem of safety of individual infrastructures, i.e., individual subsystems. From the present viewpoint before us there are minimally two following tasks:

1. To solve the problem of safety (including the functionality) of a set of mutually interconnected (dependent) infrastructures (i.e., systems system) for normal, abnormal and critical conditions.

2. To find the systems system critical conditions that are foreseeable or are a consequence of a significant mistake of the operator, and that under certain conditions can pass to high unfavourable and high unacceptable conditions, i.e., into the condition at which alone the human being is threatened which we usually denote as a crisis.

Therefore, we must today judge the critical infrastructure resilience, vulnerability and adaptation capacity considering that:

- *critical infrastructure resilience* is a measure of the critical infrastructure to absorb the changes of condition caused by a possible disaster (including the possible interactions),
- *critical infrastructure vulnerability* is a measure of a critical infrastructure's inability to react to a possible disaster (including the interactions) occurrence,
- *critical infrastructure adaptation* is a measure of a critical infrastructure capability to modify the structure of elements, links and flows of critical infrastructure in a way that the impacts of a disaster (including the interactions) are not unacceptable for the critical infrastructure.

4 CRITICAL INFRASTRUCTURE SAFETY

In the above-mentioned safety concept the critical infrastructure safety is a set of measures and activities that, when considering the critical infrastructure nature (systems system) and all possible risks and threats that are directed to ensuring the safety of elements, links and flows by way in order that their failure might not happen. In the situation of international dependence and the interconnection of sectors, the failure of the critical infrastructure in one country can affect more countries, and therefore, for critical infrastructure safety (inherently including the critical infrastructure protection) the following are both required - the sharing of responsibilities with the private sector and the exchange of information between the public administration and other relevant organisations; and secondly international co-operation (Prochazkova, 2007b). For ensuring critical infrastructure safety the following are used:

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

The critical infrastructure systems are multiplex owing to their nature and the conditions of functionality in the human system. Therefore, the critical infrastructure safety problems (inherently including the critical infrastructure protection problems) are multidisciplinary and interdisciplinary, namely in technical, managerial, and organisational domains

on different levels - legal, financial, personal, knowledge, international, etc. For the solution of problems of critical infrastructure safety it is necessary to understand the targets and roles of critical infrastructure in the human system. The process model ensuring critical infrastructure safety is based on the method of safety engineering (ESRIF, 2009). All relevant disasters are assessed – the so-called "all hazard approach" (FEMA, 1996). In order that the problem might be understandable and transparent it is necessary to use further ranking of the primary disasters: technological accidents (internal) of critical elements, links and flows in the critical infrastructure system. It is necessary to take into account material defects, aging, insufficient maintenance etc.; errors or failures of control systems; human errors; natural disasters or technological accidents (external) of other systems; and terrorist attacks, criminal acts or war.

In the theoretical domain it means the delimitation of integral risk and its partial components, with regard to protected interests (assets) and possible disasters in a given region and the specification of measures and activities leading to an increase in a region's safety in the real world; it is not expected to ideally solve technological problem but to be for the protection, conservation, and development of basic protected interests, i.e., an optimal interconnection of measures directed towards human lives and security. The basic strategic approach for critical infrastructure safety is: nothing is absolutely safe; and elements and networks of critical infrastructure can fail sooner or later, and, therefore, it is necessary to establish sophisticated regional safety management. Effective and efficient safety management must be supported by present knowledge and on the right assessment in a context that is valid for a given region. Therefore, the basic role belongs to the research that at present solves:

- impacts of interdependences among the critical infrastructure subsystems and the human system subsystems on the systems system safety,
- procedures and targets for ensuring the critical infrastructure safety from a managerial view on the level of state,
- 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 of reaching an optimal position for the public and private sector),
- requirements on the personnel of the critical infrastructure and technology owners,
- tasks of security components at defeating the emergency situations, induced by the extensive,
- outage of the critical infrastructure,
- general frame for critical infrastructure safety.

Methodology for the critical infrastructure safety management (inherently containing the critical infrastructure protection) relies on keeping the further given procedure (ESRIF, 2009, Prochazkova, 2007b, 2010), i.e., the management:

- is always directed to essential aspects,
- considers that the development must be sustainable and far-sighted (i.e., there must be balance between the economy, environment and social domain) and the primary target is the reduction of vulnerability,
- pays attention to the aspects that are the most vulnerable,
- ends emergency situations and when doing so it is directed to the needs and priorities
- regarding the basic priorities of human protection and the protection of critical sources and systems on which the community's existence depends,
- supports a prevention culture, programmes for the prevention and the preparedness to defeat emergency situations and it insures that these items are included in the territory development programme,

- ensures that the citizens have right to just 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 in the response management system not only as potential victims,
- ensures that citizens know emergency plans, content of plan of response to disasters, way to react and to be able to justify the origination of an emergency situation, etc.
- ensures that the emergency management system is also transparent for citizens and it is adjusted to the local conditions,
- ensures that the emergency management system is legitimate and acceptable and that it is based on a systemic approach,
- ensures that 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 renovation of property in a territory affected by a disaster is quite a basic concept for the determination of critical elements, critical processes, critical functions, critical infrastructures and critical technologies in a region. This concept relies 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 properties of post-modern society.

The reasons why the critical elements, critical processes, critical functions, critical infrastructures and critical technologies in the region are determined are given by the demand of the reduction of risks in the human system from the view of its safety and development in the broadest sense. It is a matter of the reduction of vulnerability (resilience increase) of key elements of the human system that are basic for society being at all levels of organisation and state administration, ensuring the functionality of life-giving systems and the rational protection of critical infrastructure (Prochazkova, 2007b,2010).

5 PRINCIPLES FOR CRITICAL INFRASTRUCTURE SAFETY MANAGEMENT

Regarding the above-given facts it is necessary to take into account that we can ensure the safe critical infrastructure in two ways. The first one is more or less ideal and it consists of the construction of critical infrastructure on a “green field”, i.e., from the beginning we create safe systems system (each partial infrastructure is also resistant to the failure of the others). The other, more realistic, way consists of 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.

In practice the failure of critical infrastructure often comes from so-called internal causes. Therefore, it is necessary to consider the technical level, conditions, and durability of a given infrastructure (35 – 40 years; max. 50 years), and the reality that through this time interval the ability for a return on investment must be ensured and that human security must not be threatened. The longer the time interval for which the infrastructure performance is planned, the more modern (timeless) solution must be used. Each variant must

be financially acceptable and must also be acceptable from the viewpoint of accessible technologies and of qualified human sources. For decision making on infrastructure renovation it is necessary to consider expenses and their return ability. Usually a criterion is used that says "when expenses for infrastructure renovation do not return, e.g., after natural disaster within 10 years, it is better to build a new one". From the public interest viewpoint it is necessary to remove or to limit the interventions of politics into decision making on the infrastructure in the territory because their targets are usually different to the long-term safety, including the functionality and reliability of the infrastructure in the region without regard to the political party in power.

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

Expenses for critical infrastructure are not only the costs for its design and building, but they also include the costs for its operation, maintenance, repair and modernisation. Therefore, the risks connected with each infrastructure must also include the risks from just given domains and the region management must know how to deal with them. It is necessary to assess the risks from disasters that can be denoted as financial market failures because of the connected failure of finances for the maintenance, operation, repair and modernisation of objects of critical infrastructure. This is caused by the fact that critical infrastructure criticality increases if no good maintenance and good repair are performed (which causes the vulnerability to increase).

Since nothing is perfect, a plan for renovating infrastructure, especially for critical situations, needs to be prepared. This plan must be proactive, properly assessed; it must contain transparently managed risks and answers to questions such as: what to do?, how to do it?, in which time interval?, do risks for other protected interests increase? etc. Because the critical infrastructure is a set of mutually connected (i.e., dependent) infrastructures it is necessary to pay great attention to the study of internal dependences, because analogies based on the study of simple technological systems indicate that for critical infrastructure failure there are much more important links and flows that mutually interconnect subsystems.

6 CONCLUSIONS

The critical infrastructure safety is a basic problem of the present days. The problem today is very broad as we must solve, not only individual infrastructure securities that depend on the technical aspects of individual infrastructures and on respecting human factors, but also aspects connected with the safety, dependability and functionality of a set of individual infrastructures in a given territory from the viewpoint that the critical infrastructure is protected against internal and external disasters and simultaneously does not threaten its vicinity (humans, environment, and property) and correctly fulfils the expected functions for the territory. At present we try to find a solution that also enables human survival in a territory during catastrophes. For this case the paper summarized the principals for critical infrastructure safety management. The conclusions were verified for electric infrastructure and now collected data exist for the judgement of transport infrastructure and for its integration into regional critical infrastructure, as, from the reasons given above, many of critical infrastructure problems are site specific.

7 REFERENCES

Adger, N.W., 2000. *Social and ecological resilience*. Progress in Human Geography 24, (2000) No 3.

Chambers, R., 1990. *Vulnerability, coping and policy*. IDS Bulletin. 20, No. 2.

Dow, K., 1991. *Exploring differences in our commnon future*. Geoforum 23, No. 3.

Eda, 2005. *Workshop on critical infrastructure protection and civil emergency planning-dependable structures, cybersecurity, common standard*. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch

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

FEMA, 1996. *Guide for all-hazard emergency operations planning*. State and Local Guide (SLG) 101.

Franklin, S. &. Downing, T., 2004. *Resilience and vulnerability*, GECAFS Project, Stockholm Environment Institute.

Glantz, M., 1992. *Global warming and environmental change*. Global Environmental Change. 2.

Gunderson, L. & Holling, C. S., 2002. *Panarchy: understanding transformation in human and natural systems*. Washington, Island Press.

Highway, 2002. *A Guide to highway vulnerability assessment for critical asset identification and protection*. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation–Transportation Policy and Analysis Center, Vienna.

Holling, C.S., 1973. *Resilience and stability of ecosystem*. Annual Review of Ecology and Systematics, 4, No 1.

Langeweg, F. & Espeleta, E. E., 2001. *Human security and vulnerability in a scenario context*. HDP Update 2.

Moteff, J., Copeland, C. & Fischer, J., 2003. *Critical infrastructures: what makes an infrastrucuture critical*. Report for Congress, 2003, CRS Web, Order Code RL31556.

Prochazkova, D., 2007a. *Strategy of safety and sustainable development management of territory* (in Czech). ISBN 978-80-7251-243-0, PA ČR, Praha, 203p.

Prochazkova, D., 2007b. *Problem of critical infrastructure protection* (in Czech). Indikace a reflexe rizik společenské praxe jako teoretický základ pro rozvoj policejních sluțeb. PA ČR v Praze, Praha, ISBN 80-7251-229-3, 219-245.

Prochazkova, D., 2008. *Critical infrastructure safety from the viewpoint of systems system* (in Czech). Riešenie krízových situácií v špecifickom prostredí. ISBN 978-80-8070-846-7, FŠI ȚU, Țilina 2008, 605-610.

Prochazkova, D., 2010. *Critical infrastructure and principals for its safety* (in Czech). Manațérstv o ți votného prostredia. ISBN 978-80-89281-34-3, Strix et VeV, Țilina 2010. 301-366.

Science, 2002. *Framework for vulnerability analysis in sustainability science*. Proceeding of National Academy of Science 100 (14).

Smithers, J. & Smit, B., 1997. *Human adaptation to climatic variability and change*. Global Environmental Change 7 (2).

Stein, W., Hammerli, B, Pohl, H. & Posch, R. (eds), 2003. *Critical infrastructure protection – status and perspectives*. Workshop on CIP, Frankfurt am Main, www.informatik2003.de

Watts, J.M. & Bohle, G.H., 1993. *The Space of Vulnerability*. Progress in Human Geography 17, No. 1.