Identification and Management of Risks of System of Systems

Dana Prochazkova
Czech Technical University in Prague
Praha, Czech Republic

Abstract—**The human system, critical infrastructure, environment, human society, human etc. are represented by system of systems, i.e. they consist of several systems of different nature and of different sitting, that are mutually interconnected with aim to provide given operations and activities. The systems of systems have specific properties as non-linearity, different steady states (attractors), catastrophic behaviour, chaotic behaviour etc. that are the cause of cross-section risks that disturb the security of a given system of systems and the security of system of systems vicinity. To ensure safe systems of systems and their safe vicinity we must know to negotiate with cross-section risks, i.e. to identify them and to manage them by suitable way. The paper presents the proposal of tool for identification of cross-section risks and outputs of its tests on real data.**

Keywords-system of systems (sos); risk management; co-existence of systems

I. INTRODUCTION

Throughout its existence the human society has been faced natural disasters, which have been threatened its existence. Therefore, with the development of its intellect and its technologies began to reduce step by step the impacts of disasters on the human lives and health and on the property. At first, human society only defended itself and with the development of knowledge it is step by step creating stable and oriented management system according to All Hazard Approach [1], aimed at minimizing the impacts of disasters on human lives, health and security, public welfare (i.e. the state of human society), property, the environment and on critical technologies and infrastructures.

In order to ensure timely defence and protection against disasters and their impacts, tool called SMS (Safety Management System) is used, integral part of which are emergency and crisis managements [2,3]. The safety management system ensures the system security and the system vicinity security. The SMS is based on the analysis, evaluation and management of risks from potential disasters of all kinds [1], which may affect the monitored real object (the territory, organization, business, infrastructure, etc.) and it provides a systematic application of measures and activities of engineering disciplines, by which objectives of serious risks management for the benefit of the public interest are achieved [4]. As the most effective preventive measures are finical on knowledge, the availability of necessary technologies, economic resources and skills of staff, the advanced countries use higher quality safety management tools based on trade-off with risks, which enable them to provide a higher level of human security in comparison to poor countries.

Because the systems which humans manage in practice are diverse by nature, author at framework of tools for identifying and managing the SoS risks chose a pragmatic approach, which relies on findings from solving the complex problems and on experiences from good engineering practice and which allows compiling a sensible and effective SMS for the SoS safety management.

II. THE NATURE OF CONTROLLED SYSTEMS AND THEIR SMS

Clear model of the safety management system (SMS) has been established based on current knowledge [2, 3, 5, 6], Figure 1. It must be noted that this SMS model applies to systems with not very complex structure and with clearly defined relationships and flows among the elements of the system. Even here, however, considering the diversity of systems that are object of management, it is necessary to elaborate each particular SMS in accordance with concept that respects the individual structure and specifics of a system, by which we replace the object that we want to manage. By such concept we also determine risks that we follow and the way of their consideration, i.e., if process of decision making is based on evaluation results of partial, integrated or integral risks. It should be emphasized that only the integral ones include cross sectional risks that are associated with internal dependencies among interconnected assets of system or among interconnected individual systems in case of system of systems (SoS - System of Systems) [7].

According to current knowledge, real systems like the human system, critical infrastructure, environment, human society, human body etc. are complex systems that consist of several systems of different nature and different locations that are interconnected and aimed to ensure certain operations and activities in a specific place and time and in a certain quality. It is necessary to note that there is a fundamental difference between the complex system which we have been monitored and managed for several decades, and the SoS, which we have systematically examined in recent times [7-10].

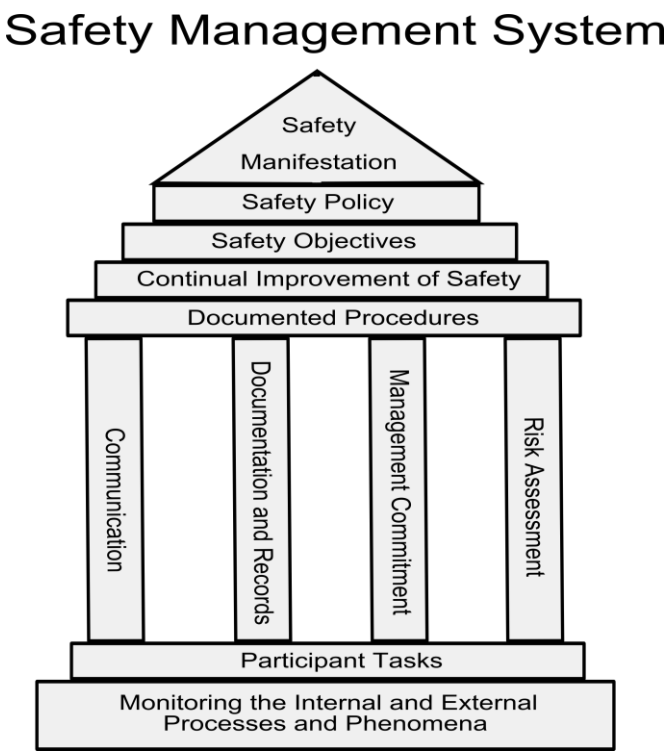

Figure1. A general model of the safety management system of real objects

A complex system is a set of interconnected systems which have closed architecture. This model nowadays represents foundation for management of power [11], gas, heat, and water, supply systems etc. According to the nomenclature of engineering disciplines focused on safety [4], the aim of such systems is to ensure system security, whereas no attention is paid to the system surroundings or to neighbouring systems. Therefore, e.g. in case of black-out of electricity supply system, the electricity distribution management system only deals with technical problems associated with the restoration of electricity supply and it does not address issues of impact of such power failure impacts on lives of people, on running businesses, etc., i.e. on public assets [12].

On the other hand, the current SoS concept is understood as a set of interconnected systems which have open architecture, i.e., different elements are connected as long as they fulfil the conditions of interoperability and user requirements [13]. With regard to the above-mentioned public assets, the aim of SoS safety management is to ensure not only safe SoS as such, but also its safe surroundings, i.e. its goal is not just a system security, but also requirement that the system does not threaten its surroundings, i.e. it goes on the integral safety management [7,14]. In other words, the SoS safety management system takes into account requirements of surroundings, e.g. such as demands of electricity users etc. From the above it is clear that the concept of SMS for SoS is different than these for complex systems now commonly used in practice.

Qualified SMS for the SoS safety management are currently being looked for. They must deal with internal dependencies among systems and appropriately resolve conflicts among systems of different nature, Figure 2. Conflict resolution with aim to ensure the SoS safety in the real environment means finding a consensus among aims of individual systems and among ways of their reach; priority target for SoS safety is coexistence of partial systems [20].

The biggest challenge for SoS safety management systems are the identification, understanding and appropriate management of cross-cutting risks which cause or can cause different cascades of failures of SoS functionality, which deplete the SoS assets. For their discovery and strategic management it is necessary to analyse internal dependencies among SoS individual systems, across entire SoS and between the SoS and its surrounding. Available professional works [8-10, 15] show that the general analysis of SoS is very difficult, e.g.: due to diversity of different elements of SoS, different types of interdependencies among partial systems of SoS (there are physical, cyber, spatial and logical interdependences that predispose the SoS criticality, types of faults and failures). Application of theoretical methods based on network models [16] fails just on the fact above. Published examples from books [9, 10] show good solutions obtained by studying the specific SoS in a region. The same is shown by site specific prevention systems, and site specific response systems, which form the foundation of plans for protection of public assets [17].

Systems of systems have specific properties such as nonlinearity, different steady states (attractors), catastrophic behaviour, chaotic behaviour, etc., which are the cause of cross-cutting risks that disturb both, the followed SoS security and the SoS vicinity security [6]. In order to ensure safe SoS and safe SoS vicinity, we must be able to cope with the cross-cutting risks, i.e. to identify and appropriately manage them.

We must realize that for SoS risk management it is valid basic knowledge of risk management domain [7], i.e. it is not enough to know the risk size, but it is necessary to know its specific causes, their localisation in a controlled system and the particular vulnerabilities of assets in a given allocation. For identification, analysis and assessment of risks, there are many classical methods, tools and techniques [5]. Unknown are the tools, methods and techniques for identifying, analysing and managing the cross-cutting risks.

III. RISKS AND THEIR TYPES

Risk is a measure of violation of monitored system security, which is a subject of possible disaster occurrence monitoring. It goes on measure of disaster potential to disrupt security and sustainable development of monitored system. The most concise definition of risk is to use the expected loss, damage and harm on assets in a certain standardized way in order to ensure comparability (e.g., converted to area unit and time unit [7], which is used in materials for strategic management). In dependence on the specific needs [7] we

determine either the risk of one disaster or for a set of all disasters, which can affect the real object reference.

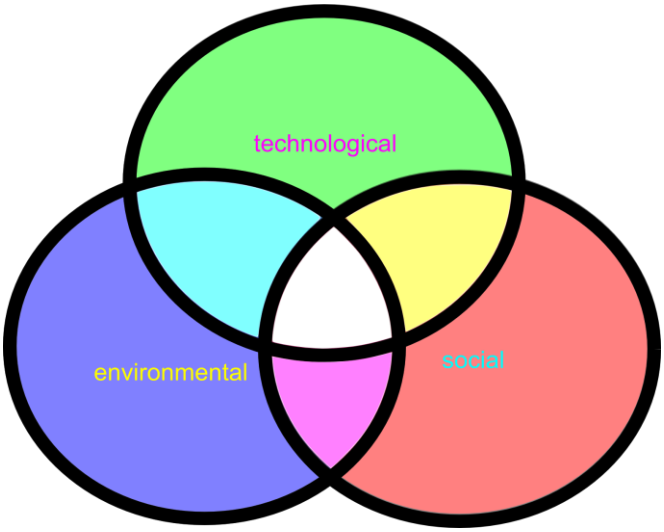

Figure2. Sample of systems, the conflicts of which are the subject of SMS solution for SoS

In determining the risk either one asset is considered and partial risk is determined, or complex assets are considered and integrated or integral risk is determined. Integrated risk only represents a certain aggregation of partial risks, which is usually determined by norms or standards. The integral risk includes both, the risks associated with individual assets and the cross-cutting risks that are associated with links among assets and with the couplings among the assets realized by flows (energy, information, instructions, commands, responses to them from top to bottom and vice versa), i.e. it represents a complex risk the qualified management of which provides the integral safety.

In the SMS concepts we consider two cases, namely either the risk realisation is still substantially the same or it is significantly different. In the first case, we consider from safety reasons either the worst case (such approach is found in standards based on a deterministic approach to safety provision) or we admit random uncertainties resulting from momentary local and temporal conditions of assets and as a representative variable for risk management we use mean value obtained by evaluating the possible alternatives (arithmetic mean, median, median + σ, where σ is the standard deviation, the probable mean value). The other procedure is now commonly considered in the preparation of documents for strategic management (there are determined alternative scenarios for the risk realisation and their occurrence probabilities; and the mean and its dispersion are derived from them by clear mathematical approach); we can find it in the norms and standards based on a probabilistic approach.

Based on the knowledge of the past decade, it is necessary to admit when considering the risk realisation, that in addition to random uncertainties, there exists also knowledge (epistemic) uncertainties, i.e. vagueness in the data. By admit the other uncertainty type existence we de facto admit the existence of significant changes in the process of risk realisation, which go significantly beyond simple effects of random changes. Thus in recent years, approaches of theory of possibilities, i.e. Dempster - Shafer theory [18, 19] have been introduced into practice for modelling the safety and reliability. It assumes that the available data and our knowledge have vagueness, i.e. they contain knowledge (epistemic) uncertainties in addition to random uncertainties. Using this theory, the variants corresponding to different processes are modelled, which are possible due to knowledge shortcomings. Of these, optimum variant is selected. For selecting the options service of experts is used and calculations are combined with the best practices. The practice has shown that one expert is not enough, but that it is necessary to combine knowledge of several experts. Such a combination can be ensured by analytical methods or heuristics, such as DELPHI, panel discussion [16].

IV. THE CONCEPT OF TOOL FOR IDENTIFYING, ANALYSING, ASSESSMENT AND MANAGEMENT OF CROSS-CUTTING RISKS

When preparing the concept of tool by which is possible to reveal critical items from the safety viewpoint in which it goes on security and sustainable development of the SoS, i.e. with which it is possible to estimate cross-cutting risks in SoS, that we do not know to control, we come out from well-known fact, that the risk is locally specific; and this fact we also generalize to cross-cutting risks. As the point approximation is unrealistic, we define the reference point as a circle with certain radius (e.g. for the 5 km area) circumscribed around a reference point, or as a square with certain side length (e.g. 5 km), and in this we define possible losses, damages and injuries, according to the presence and amount of assets and according to their vulnerabilities to a given disaster [16].

In the real case, we consider the variability of disaster scenarios in time in a given place; the risk assessment is performed as indicated below.

Let k is the number of possible disaster scenarios for the object / location / area, p_i is the occurrence probability of the i-th disaster scenario, i = 1,2,..., k, c_i is the overall impact of the i-th scenario disaster, i = 1,2, ..k. to the assets, then the risk associated with the disaster with respect to the assets in a given place is determined by relationship

$$R = \sum_{i=1}^{k} p_i \; c_i \; .$$

If we relate the risk to just one asset, i.e. human life and we consider that today's acceptable probability of human casualty is 10^{-5} in case of individuals and $10^{-3} \cdot N^{-2}$ in case of group of persons, where N is the number of affected individuals [7].

In the selection of specific measures and actions to ensure the safety objectives we are considering contemporary targets, which means to achieve likelihood of occurrence of human

casualties at 10^{-6} at individuals 10^{-4} N^{-2} at groups of people, where N is the number of affected individuals [7]. Number of vulnerable people is calculated according to formula

$$N = S \cdot h \cdot f_s ,$$

where *S* is the affected area in ha, *h* is the density given by the number of persons per ha, f_s is the correlation factor when only part of the territory is inhabited.

In terms of risk as a proportion of total damage to assets to the total values of the assets the risk is a dimensionless quantity (a number between 0 and 1 or between 0 and 100, depending on the chosen scale) related to the chosen time unit. On the basis of representative set of empirical disaster scenarios and corresponding calculations of losses and damages in a particular area it is possible to calculate the average total risk associated with disaster in a given area [7].

There exists large number of tools and methods for the identification, analysis, assessment and management of risks of not very complex systems, described in [7] and in works that are cited in it. It is not so in case of the SoS, and therefore on the basis of recent knowledge and years of experience in solving the complex practical tasks, in which it was necessary to use the best practices of good engineering, the author has prepared a draft of instrument for identification and management of risks of the SoS . In order to promote its application in practice, results of tests based on real data are provided.

From a methodological point of view the SoS risk management represents coordination of a number of disparate processes that take place simultaneously in different domains and some of their results are mutually inter-dependent, i.e. the processes are in some way dependent on each other, i.e., the procuration of tasks connected with safety ensuring is determined by targeting the measures and activities in various parts of the SoS. From the perspective of the given objective it is necessary that each governing body of SoS understood each problem in the existing context and sought an effective solution in these conditions with regard to other systems, while acting rationally with regard to costs and available resources in their respective domains. These requirements are the basic principle of SMS for SoS.

Based on the knowledge and experience in designing systems for decision support [7] a comprehensive tool for identifying, analysing, evaluating and managing the risks, including cross-cutting ones, which guarantees the survival and continuity of critical assets during critical disasters was designed using the logical synthesis of data and experience. Since at the SoS normal condition it is difficult to identify cross-cutting risks, so well-known fact was used, i.e. the cross-cutting risks are manifested by secondary and higher impacts on the SoS assets in the occurrence of disasters the sizes of which exceed the level of design disasters (i.e. the size of the disaster up to which systematic preventive measures are taken to avoid or mitigate potential impacts of disasters on assets) [7]. With the help of specific approach, which requires processing of extreme disaster scenarios, atypical disaster scenarios should be identified that do not occur under normal conditions and are therefore not revealed at normal risk analysis [10].

The proposed tool de facto introduces the compilation of site specific scenarios that in case of individual disasters represent both, the local disaster impacts (i.e. actions) and the human reactions. By analytical way there are revealed weaknesses in human reactions to possible disasters, namely in domains of prevention, preparedness, response and renovation, by specific technique applications there are determined the individual weakness relevance and by help of good engineering practice rules there are proposed improvements in human reactions with aim to upgrade safety. The tool consists of 4 parts:

1. The SoS screening.
2. The SoS risk assessment.
3. Screening the existing measures and activities for SoS risk management and for SoS safety increasing and for evaluation of level of trade-off with risks.
4. Identification of critical items of SoS risk management and proposal of solution of gaps associated with survival or continuity of assets during critical disasters.

In the first step screening of SoS is carried out , which consists of the following parts:

- determination of the SoS characteristics (in the case of territory the characteristic in the range of land planning documentation, as it is required by land-use planning),
- classification of SoS (in the case of territory - industrial area, agricultural area, forest ...),
- application of ALL HAZARD APPROACH to the SoS documentation it is specified a set of disasters which can have on SoS conditionally acceptable or unacceptable impacts, i.e. they are dangerous for the SoS,
- identification of SoS vulnerabilities (e.g. using the SWOT analysis there are identified weaknesses, strengths, risks and opportunities of management mechanism of SoS).

In the second step, the SoS risks associated with all the disasters identified as hazardous in the first step are evaluated. With regard to the existence of random uncertainties and knowledge uncertainties in the data:

- alternative scenarios are elaborated for the risk realisation in SoS for each dangerous disaster (e.g., by linking the modified form of the „What, If“ method [7,16] and targeted methods of case studies [16]); with regard to knowledge the disaster scenarios are created for normal, critical and extreme size of disaster; in these there are separately monitored impacts on individual assets of SoS the within the predefined time intervals (e.g. at territory level the simulations proved successful for time periods measured from the disaster origin at 0h: 0h, 3h, 6h, 24h, 3 days, 14 days, 1

month); experts are asked to fill tables the prototypes of which are in annex 1,

- for each dangerous disasters the secondary and higher impacts on assets of SoS are evaluated, as observable in times of 3h, 6h, 24h, 3 days, 14 days, 1 month, especially in scenarios for critical and extreme disasters and points of cascading failures and possible cascade effects are revealed,
- vulnerable items of SoS are determined by overall evaluation of the data obtained for the disasters identified as dangerous for the SoS,
- failure rates of individual vulnerable items of SoS are determined with regard to disasters identified as dangerous for the SoS,
- the criticality matrix for SoS is compiled (for individual vulnerable items of SoS it is scored failure frequency and failure severity that is estimated by size of losses on SoS assets) and according to the appropriate value scale highly critical, moderately critical and commonly critical items of SoS are determined.

In the third step on the basis of existing documentation for SoS safety management, which currently means that there are considered measures and activities of risk management for the individual systems and there are performed the evaluations of their effectiveness in risk management of SoS - for individual items of risk management (acts of management, technical area, knowledge area, financial area, personnel area, responsibility) it is:

- performed the screening of existing measures and activities for risk management of partial systems of SoS and it is evaluated its suitability for improving safety of SoS,
- performed the evaluation of level of trade-off with the risks for all disasters that have been identified as dangerous for SoS, especially for highly and moderately critical items of SoS; and for SoS safety management needs, the level should be classified according to suitable scale,
- compiled responsibility matrixes and their level is assessed in terms of the appropriate competencies at the level of individual systems and the whole SoS; responsibilities for SoS safety management must be logically prime,
- examined procedures and regimes of SoS management that originate by aggregation of processes and regimes of management of partial systems; attention is focused on the detection of conflicts and gaps at implementation in practice and on reality how they are procured by knowledge, material, technical means, finance sources and personal,
- assessed adequacy and accessibility of resources, forces and means with regard to cope with the medium and highly critical items of SoS with acceptable losses and damages,
- assessed effectiveness of specific procedures such as warning, capability to respond to warning instructions, etc.

Finally, areas where the risk of SoS is managed poorly or not at all are identified.

In the fourth step, aimed at identifying critical items of SoS risk management and proposal of solution of gaps associated with survival and continuity of assets during critical disasters there are determined interfaces, leading to decay and dissolution of any of the assets or entire SoS are identified. The procedure is as follows:

- it is judged the relevance of the domains where the SoS risks are managed poorly or not at all and for domains highly significant from the public interest perspective there are proposed realistic measures and actions against decay and extinction of any of the assets or the entire SoS, there is processed implementation plan (mostly long-term) and it is ensured its realisation in all aspects,
- on the basis of a critical view on extreme and critical scenarios of potentially dangerous disasters with regard to basic public interests (human lives and health, good living conditions and the possibility of development) there are re-examined possible measures and activities for survival or continuity of public assets in order to avoid overlapping the threshold of criticality of conditions of their existence.

SMS for SoS is therefore composed of a safety management system that controls and determines the cross-cutting risk and defines objectives of safety management systems for individual systems of SoS (Fig. 1). This means that SMS of each SoS partial system will change as follows:

- input item "monitoring of internal and external processes and phenomena" is changed to "monitoring of internal and external processes and phenomena, and guidelines for the management of partial system from the perspective of SoS safety management,
- Output item "safety manifestation" is changed to "manifestation of safety and possible impacts on the surroundings, i.e. on further SoS systems."

Input SMS entry for SoS is "monitoring of internal and external processes and phenomena and behaviour of individual partial systems". Output item is a "SoS safety manifestation."

V. EXAMPLE OF APPLICATION OF METHOD FOR IDENTIFYING, ANALYSING, EVALUATING AND MANAGING THE CROSS-CUTTING RISKS

The above described method for identifying, analysing, evaluating and managing the cross-cutting risks has been successfully tested on the SoS, represented by territory. 123 different surveys for the different areas were performed, namely: rural settlements, urban development, industrial region, agricultural region, and wooded areas; and 77 disaster types possible in the ČR were considered [4]; annex 2. The investigation was carried out with help of experts from different areas, namely: master and doctoral students from

technical universities; the academic staff of universities in the field of safety engineering, safety technologies, crisis management and planning; scientists from research institutes dealing with technologies and their safety; public administration workers; designers; safety engineers from industry; inspectors from different departments of safety (nuclear safety, fire safety, chemical safety); policemen and fire-fighters; and activists from several selected areas of the environment and health.

The quality of the data obtained was variable. Dependence of data quality on a practical operational experience was dramatically demonstrated and a clearly visible was certain blindness of designers and safety engineers in operation, who are firmly convinced that compliance with the norms and standards guarantees safety and that nothing dangerous can happen when they comply with norms and standards for safety (they do not recognize data variability and uncertainties in our knowledge).

It was, therefore, necessary to combine data for similar areas together, and to add some new investigations in specific areas in order to reduce the uncertainties in the data and to increase the representative capability of the data file. Methods of mathematical statistics were used to delete random uncertainties. For vagueness (epistemic uncertainty) removal in the data file there were considered specific variants obtained by case study methodology and results were set with help of 5 experts.

The analysis of results provided following facts for the Czech Republic:

- there exists awareness of natural disasters, although systematic prevention aimed at increasing the resilience of buildings and technology is not always at necessary level,
- in social area: in many cases not enough care is given to prevent human errors in processing plants and public affairs governance; there is not sufficient protection against bullying and similar phenomena in schools and workplaces; and there is not sufficient protection against misuse of CBRNE and IT technologies,
- in the technology area there is a clear demonstration of pragmatism and technical education of the population - a clear promotion of innovation and new technologies, and support for government efforts enforcing the use of secure and high-quality technologies,
- in the environmental area there is insufficient protection against contamination of air, water and soil; and low quality of waste treatment,
- in areas related to internal dependencies in the human system inadequate care in following areas was observed (sorted by highest priority according to data from the respondents'), which causes: failures in management of human society for the benefit of the public interest, i.e. the lack of fight against: corruption, abuse of power and the disintegration of human society into intolerant communities; failures in services for citizens (health, education, social assistance ....); failures in flows of raw materials and products; failures of energy flows; failures in money flows; failures in information flows; failures in public transport,
- politicians and public administration workers are not responsible for the quality of their decisions in favour of the public interest,
- professional accountability of public administration workers for decision-making in the public interest support is not required,
- public administration does not use tools for identification, analysis and management of risks in the public interest (mainly because of ignorance and because of the lack of enforcement of the legislation), i.e., it is making ad hoc decisions,
- there is no sufficient control of use of public resources, forces and means,
- good work in the public interest is not fully appreciated and the interests of different lobbying and political groups are preferred,
- the education and healthy development of the population is not supported.

From the facts above it is clear which areas are critical and unresolved and to which it is to pay necessary substantial attention in order to create safe community.

Application of method for identifying, analysing, evaluating and managing the cross-cutting risks on SoS, which represents the critical infrastructure, is currently being processed. Due to large diversity of infrastructure interdependencies that make up the critical infrastructure of the area and that are also different in nature, it is necessary to compile separately several different areas, because the interfaces of infrastructures comprising the critical infrastructure are not yet regulated by norms and standards. Infrastructures are physically interdependent (if condition of one of them is dependent on the material output of the other), cyber interdependent (if condition of infrastructure depends on information from other infrastructure; i.e. the existence of information infrastructure is assumed), territorially interdependent (if the phenomena and events in territory may change the infrastructure conditions) and logically interdependent (if condition of infrastructure depends on the condition of other infrastructure, and the coupling mechanism is not physical, cyber, or territorial; it is results of dependence transferred by flows, which are regulations, finance, legislation, etc.). Qualified professional data collection is, therefore, very exigent on knowledge and it is time consuming, because it is necessary to study the documentations for a specific territory and its real infrastructures. Only after collecting a representative data set it will be possible under the rules of logical synthesis to find out the general features determining criticality of the monitored SoS.

VI. CONCLUSION

The proposed method for identifying, analysing, evaluating and managing the cross-cutting risks is based on the experience and the principles of good engineering practice. Although, it does not make extensive use of highly sophisticated methods of application [16], and could be time consuming due to its requirements for high-quality data, the collection of which is always challenging as for the expertise and time, it is characterized by a pragmatic and transparent approach, and it provides good results which practice needs for management of objects which belongs to the SoS.

ACKNOWLEDGMENT

The research was supported by the Czech Technical University, Faculty of Transport Science (Institute for Security Technologies and Engineering), by the EU – project FOCUS, grant No 261633 and by the Ministry of Education of the Czech Republic, grant No 7E11072. Thank you for support.

REFERENCES

[1] FEMA,"Guide for All-Hazard Emergency Operations Planning". State and Local Guide (SLG) 101. FEMA, Washinton 1996.
[2] OECD, "Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes Related to Chemical Accident Prevention, Preparedness and Response." OECD, Paris 2002, 191p.
[3] D. Prochazkova, " Strategy of Management of Safety and Sustainable Development". ISBN 978-80-7251-243-0, PA ČR, Praha 2007, 203p.
[4] D. Prochazkova, "Procedures and Methodologies of Engineering Disciplines Directed to Safety". ISBN 978-80-01-04946-6, SPBI, Ostrava 2011, 2 parts – book – 176p. + CD ROM – 164p.
[5] D. Prochazkova, "Protection of Peoples and Property". ČVUT, Praha 2011, ISBN 978-80-01-04843-6, 246p.
[6] E. McGuinwess, I. B. Utne and M. Kelly, "Development of a Safety Management System for Small and Medium Enterprises (SME's)". In: Advances in Safety, Reliability and Risk Management. CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-415-68379-1 – Hbk, pp 1791-1799.
[7] D. Prochazkova, "Analysis and Management of Risks". ISBN 978-80-01-04841-2, ČVUT, Praha 2011, 368p.
[8] R. Bris, C. G. Soares and S. Martorell (eds), "Reliability, Risk and Safety. Theory and Applications". ISBN 978-0-415-55509-8, CRC Press / Balkema, Leiden 2009, 2367p.
[9] B. Ale, I. Papazoglou and E. Zio (eds), "Reliability, Risk and Safety". Taylor & Francis Group, London 2010, ISBN 978-0-415-60427-7, 2448p.
[10] Ch. Bérenguer, A. Grall and C. G. Soares (eds), "Advances in Safety, Reliability and Risk Management". CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-203-13510-5 – eBook - CD ROM, 3035p.
[11] ČEPS, "Control of Czech Electric Distribution Net. Safety Documentation". Archives, ČEPS Praha.
[12] CR, Act No. 458/2000 Col.
[13] R. Filippini and A. Silva, "Modelling Language for the Resilience Assessment of Networked Systems of Systems". In: Advances in Safety, Reliability and Risk Management. CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-415-68379-1 – Hbk, pp 2443-2450.
[14] UN, " Human Development Report". New York 1994, www.un.org
[15] D. Prochazkova, "Real Problems of Critical Infrastructure Threatening the Region Safety". In: Reliability, Risk and Safety – Ale, Papazoglou & Zio (eds), Taylor & Francis Group, London 2010, ISBN 978-0-415-60427-7, 2387-2394.
[16] D. Prochazkova, "Methods, Tools and Techniques for Risk Engineering". ČVUT, Praha 2011, ISBN 978-80-01-04842-9, 289p.
[17] D. Prochazkova, "Security Planning (Land-use, Emergency and Crisis Planning)". ISBN 978-80-86708-80-5. VŠERS o.p.s., České Budějovice 2009, 200p.
[18] G. A. Shafer, " Mathematical Theory of Evidence". Princeton University Press, Princeton 1976, 292 s.
[19] A. P. Dempster, "Upper and Lower Probabilities Induced by a Multivalued Mapping". In: The Annals of Mathematical Statistics, 38 (1967), No 5, pp 325-339.
[20] H. Bossel, "Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme". Books on Demand, Norderstedt/Germany, 2004 (ISBN 3-8334-0984-3) (www.libri.de).

ANNEX 1.

Impacts of monitored disaster in the territory in the disaster origin time (0h). Distinguish three variants: V - standard disaster size, C - critical disaster size and E - extreme disaster size. In times 3h, 6h … measured from disaster origin distinguish primary and secondary impacts; secondary ones are caused by failure of infrastructures and technologies.

Protected interest / asset		**Impacts**
Possible impacts on lives and health of people		
Possible impacts on people security		
Potential impacts on property		
Potential impacts on public welfare		
Possible impacts on the environment		
Possible impacts on infrastructure and technology	Failure of energy supply (electricity, heat, gas)	
	Failure of water supply drinking utility	
	Failure of sewage	
	Failure of the transport network	
	Failure of cyber infrastructure (communication and information networks)	
	Failure of the banking and financial sector	
	Failure of emergency services (police, fire fighters, paramedics)	
	Failure of essential services in the area (food	

	supply, waste disposal, social services, funeral services), industry, agriculture	
	Failure of state and local government, i.e. the management of territory and human society	

ANNEX 2. LIST OF DISASTERS

1. Disaster types being results of processes in and out of the Earth:
   - natural disasters: avalanche, earthquake , floods, drought, windstorm (strong wind, tornado, hurricane), volcanic eruptions, land slide, rock slide , dyke damages, forest fire, hot humid summer days, excessive precipitations (water, snow), gas emanation from Earth's interior, sandy storm
   - epiphytic
   - epizootic
   - land erosion
   - desertification
   - fundament liquefaction
   - ocean spreading
2. Disaster types being results of processes in human body, behaviours and in human society separated to:
   - unintentional: illnesses, epidemic, involuntary human errors
   - intentional: vandalism & unlawful adventure, robbery, assaults, illegal access, unauthorised use of property / facilities, theft, fraud, intimidation and extortion, disruption, sabotage, killing, victimization, religious and other intolerance, riots, criminal acts, terrorist attacks, mass migration, local and other armed conflicts
   - disused technologies: mining the information from social (face book, twitter etc.) and other cyber nets directed to psychological pressure on human individual, intent CBRNE scatter
3. Disaster types connected with human activities (separate chemical, nuclear and bio technologies):
   - incidents
   - near miss
   - accidents
   - infrastructure failures
   - technology failures
   - loss utilities
4. Disaster types being results of processes that are reactions of Planet or environment to human activities:
   - man-made earthquakes
   - disruption of ozone level
   - greenhouse effect
   - fast climate variations (climate change)
   - contaminations of air, water, soil and rock
   - desertification caused by human bad river regulation
   - drop of diversity of animal and vegetal variety
   - fast human population explosion
   - migration of great human groups
   - fast drawing off the renewable sources
   - erosion of soil and rock; land uniformity
5. Disaster types being results of processes connected with inside dependences in human system and its surrounding separated to:
   - natural: stress and movements of territorial plates, water circulation in environment, substance circulation in environment, human food chain, planet processes, interactions of solar and galactic processes
   - human established: human society management failure as: corruption, authority disuse, human society disintegration into intolerant groups; flows of raw materials and products (material and product supply chain) failure; flows of energies (energy supply chain) failure; flows of information (information supply chain) failure; flows of finances (finance supply chain) failure; flows of waste and waste water (waste handling) failure; flows of water (water supply chain) failure; transport failure.