Open Problems in Protection of Life-Giving Infrastructures and Supply Chains

Dana Procházková*
Czech Technical University in Prague, Faculty of Transportation Sciences, Praha, Czech Republic
**Corresponding author: prochdan@fd.cvut.cz*

DOI: 10.2478/v10158-012-0032-1

ABSTRACT: Based on the concept of safe community there are followed couplings created in the human system by life-giving infrastructures and supply chains. The assessment of harm caused by their failures and the level of management of these failures reveals open problems in the followed domains and these were used for formulation of requirements for future research.

KEY WORDS: Security, safety, life-giving infrastructures, critical supply chains, failure, requirements for future research.

1 INTRODUCTION

The present time characteristics consists in note that: demands of humans on life quality increase; it increases the human vulnerability connected with number of humans and with human dependence on new technologies; it is lack of resources in densely populated areas; and new way of management "JUST IN TIME" limited stocks and reserves and introduces the dependence on early supplies and early services. The security, economic prosperity, and social well-being of humans depend on the safe and reliable functioning of the increasingly complex and interdependent infrastructures that make up the system of systems - hereafter "SoS" (Procházková, 2009). Highly efficient, complex, and interdependent infrastructure systems, including electric power, telecommunications, transportation, water utilities, food distribution, housing and shelter, public health, finance, banking and public governance, are the foundations of modern societies. In the new economy, these interconnected infrastructures have become increasingly fragile and subject to disruptions that can have broad regional, national, and global consequences.

The paper summarizes the results of assessment of failures of life-giving (vital) infrastructures and of the level of management of these failures in Europe, where special attention is paid to failures of supply chains.

2 NATURE OF LIFE-GIVING INFRASTRUCTURES AND SUPPLY CHAINS

Infrastructures assure the quality of human life, enable protection for humans and their survival in critical situations. They represent large technological facilities, the technological systems, which are more than just a set of technical equipment parts and components. They reflect the organizational structure, management, operating rules and culture of design organizations that created them and are usually also reflections of the society in which they were created (OECD, 2002; Procházková, 2009, 2011a; Procházková et al., 2008). Accidents are often

blamed on operator error or equipment, without distinction of industrial, organizational and managerial factors that caused the errors and the shortcomings in question to become unavoidable. The causes of accidents are often, if not almost always, rooted in the organization - in its culture, management and structure. All these factors are critical to the safety of technical systems. Analysis of the causes of past accidents shows that the issue is very complicated and its solution requires a high professional perspective and a genuine desire to solve problems, both in the management and in the engineering disciplines (Procházková et al., 2008).

In terms of exact sciences, each technology sub-system consists of the controlled object and the control system. The controlled object is usually a complex nonlinear system: it consists of numerous elements, where each one is uniquely described by a finite number of measurable variables. Interactions between elements are clearly formulated. Dynamic properties of the controlled object can be described by differential equations, the solution of which is the state vector. The state vector allows determining the state of the system at any point in time using the minimum number of variables. The control system must maintain specified physical quantities at predetermined values. In the process of regulation, the control system changes the state of the technological system by affecting the action variables in order to achieve the desired state. When managing the control system (according to the recent concept that places the highest emphasis on safety) the priority order of features such as: safety (level of compliance with the conditions of operation and non-creation of harmful (unacceptable) impacts on the system itself and its surroundings); functionality (level of performance in execution of required acts); operability (level of performance in execution of the required actions depending on normal, abnormal, and critical conditions); operational stability (level of compliance with the conditions of operation at the time); and inherently built-in resilience to possible disasters (Ellul, 1980).

The human system like any other system is described by the basic elements (assets), links among elements (physical - material, territorial, cyber, logical) and flows that make more or less important couplings, which in some cases fundamentally determine the behaviour of the human system (Procházková, 2011a). With regard to the uneven spread of humans and unequal distribution of food and other resources, the quality of the supply chain is highly significant for human life. Events in recent years, such as the interruption of oil supplies to Central and Western Europe due to disagreements between Ukraine and the Russian Federation, have shown the high vulnerability of selected commodities and they led to the consideration of a new problem that the EU must solve for its security and development. The present research specifies some security problems of supply chains.

Supply chains are multistage systems that are comprised of suppliers, manufacturers, distributors, retailers and customers and in where among the individual levels in both directions there run flows of materials, finances, information and decision. Material flows include flows of raw materials, intermediate products and finished products from suppliers to customers. Conversely, there are oriented flows of products for repair, recycling or disposal. Financial flows include various types of payments, loans, cash flows arising from the ownership, etc. Information flows linking the system with information about orders, supplies, plans, etc. The decision flows are sequences of decisions of participants affecting the overall performance of the chain, i.e. among the final contractor and all sub-contractors who are involved in the completion and delivery of the supply according to the contract between the final supplier and the delivery customer. The supply chain can contain more levels of co-operation stages and it always relates to the performance of one supply. Mutual relations among the co-operative stages are based on a contractual basis.

The supply chain includes all transport and activities related to transport and procedures, starting from the production plant and ending at the cargo destination, i.e. it is a network of autonomous or semiautonomous business entities collectively responsible for procurement, production and distribution activities associated with one or more related manufacturers.

The theory of the supply chain involves the planning, implementation and control of operations applied to the supply chain as efficiently as possible. Supply chain management encompasses all the movement and storage of raw materials, inventory and movement of finished goods from the point of origin to the point of consumption. In theory and in management a specific term, "outsourcing", is used (Zemánek, 2008). Outsourcing is the division of labour, the purchase of semi-finished products, financial loans and almost all other activities at the store. All the outsourcing issues are contained within the problem of deciding whether to "make or buy" (make vs. buy) or "to own or rent" (own versus lease). In the domain of information sharing one of the many questions is raised when considering the possibilities of outsourcing, the question of safety. Safety can be further divided into two categories. One is data security, i.e. ensuring data from loss (backup). The second category is to protect data against unauthorized abuse, i.e. defence against intrusion into the system and transfer of the information stored in the information system to third parties by employees.

It is a question of both who ensures that the information stored in the system will not be abused by the company that governs (administrates) the system and how this is ensured. A possible answer is the look to statistics, but it is necessary to consider that the amount of penalties that a company may apply to the company's own employees (insiders) is, as a rule, lower than the possible financial penalty of an outsourced company. The security aspect is managed by a contract in which this domain may be a part of the contract on outsourcing or it may be included in a separate agreement on confidentiality.

The Supply Chain Management (SCM) is turbulently evolving discipline that uses concepts that were developed in various other disciplines such as logistics, marketing, financial and operational management, information systems, economics, dynamics of systems and operational research. Quality of governance (management) of the supply chain is considered to be the key to its future competitiveness, and, therefore, it raises considerable interest with managers and researchers. Modelling the supply chain is a frequent topic of conferences and professional communication.

Supply chain management deals with the mutual relationships among supply chain components, i.e. among suppliers, carriers, customers, vendors, managers for waste management, including those who work with products after the end of their lifespan. These interactions are likely to change in the chain up and down depending on what the subject of interest of an organization in the supply chain. It is clear that effective communication can strengthen co-operation, reduce the potential for misunderstanding and influence the measures taken by organizations in the supply chain.

In a modern operating company it is necessary that the company's management is capable of managing the supply chain very efficiently. An important component of these chains is an understanding of subcontracting or also of the outsourcing domain, which is used by almost every company today. Firms must know which activities should be delegated to external institutions specialized in the implementation of these operations. An optimal decision on what operations and to what extent to delegate leads to a reduction in costs or to the possibility of focusing on more important tasks related to the firm's competitiveness.

Every company is trying to assert itself on the market, to define its mission, the so-called company mission. From this mission targets are determined, i.e. objectives, which the company may achieve in a particular market in a certain timeframe. Based on these stated objectives a corporate strategy is then formed, i.e. the determination of the procedure, the means and methods with which to meet those objectives. Together with this, the question arises of the necessity of "correction" of the strategy outlined or its new creation, with the view of changing the scope of the dominant factors affecting the company both internally and externally. In most cases, vicinity factors are simply the main cause of the prosperity or decline of a company.

Enterprises are increasingly confronted with global competition, which is caused by increasingly demanding customers. In order to succeed, they try to control the efficiency of their operations that create and provide products for the attention of end users within the supply chain. In recent years, supply chain management is becoming more important for firms as a competitive advantage. Fierce competition in today's global markets, marketing of products with shorter life cycles, rising customer expectations, forcing companies to focus their attention on the supply chain influence the situation.

The aim of supply chain management is to ensure the safety of all participants of supply chains to which they belong: participants' prosperity; fulfilment of tasks for which they were established; a harmonious relationship with the state on whose territory they perform the activities (Procházková, 2011a).

3 DATA AND METHODS OF SPECIALISED RESEARCH

For the investigation of infrastructure and supply chain failures and of their management published original data were used, e.g. on blackouts in the US, Italy, Switzerland, Czech Republic; disruption of oil and gas from Russia to Central and Western Europe (EU, 2012a); and a simulation of failures of networks which create the basic part of infrastructures (Procházková, 2009). The outputs described in the next paragraphs were created by pure scientific methods, i.e. analysis and synthesis of obtained published results on disasters; specific investigation of disasters by analytical and heuristic methods. Heuristic methods were first tested on real data to see if they are suitable for security tasks solution; specific investigation of the level of disaster management with the help of a special questionnaire; and specific investigation for the identification of critical items in territory management from a viewpoint of human survival performed by special logical tools specially tailored for the FOCUS targets (Procházková, 2012a).

Table 1: Form of questionnaire.

Protected asset		**Problems**	**Proposal of countermeasures**
Lives and health of humans			
Human security			
Property			
Public welfare			
Environment			
Critical Infrastructure	Energy supply (electricity, heat, gas)		
	Supply of water drinking / utility		
	Sewage		
	Transport network		
	Cyber infrastructure (communication and information networks)		
	Banking and financial sector		
	Emergency services (police, fire fighters, paramedics)		
	Essential services in the area (food supply, waste disposal, social services, funeral services), industry, agriculture		
	Local government		

The sources of risks connected with supply chains were derived by considering the all hazard approach (FEMA, 1996), the list of disasters (Procházková, 2011a) and by application of the What, If method (Procházková, 2011b) in the form shown in Table 1.

The detailed study on failures and failures´ management in the EU (2012a) was concentrated on ten domains the outputs of which are concisely summarized in papers (EU, 2012; Procházková & Kopecký, 2012; Procházková & Říha 2012; Procházková et al., 2012). The work (EU, 2012a) also obtains results of a theoretical study dealing with the form of an EU security concept: it must be based on systemic (holistic) thinking, a typical feature of which is the focusing on the whole view of systems and on the research of relations among their individual parts; a proactive approach; an all hazard approach (FEMA, 1996); respecting the co-existence of overlapping systems (Procházková, 2012b). For its realisation sophistically managing the failures that damaged the security of community and its assets is necessary, i.e. to apply measures and activities of prevention, preparedness, response and renovation. For practical purposes good technical solutions are necessary based on recent findings and experiences and correctly aimed governance of public affairs supported by a legislative with a sufficient legal force, finances, qualified human personnel and material base.

4 RISKS OF SUPPLY CHAINS

The synthesis of data from quoted publications and simulations performed by the described What, If method revealed that there are two broad categories of risk that must be controlled in the case of supply chains:

- The risk that is the cause of a lack of co-ordination of requirements and supply;
- The risks associated with the failure of normal operation, which is caused by disasters of all kinds, i.e. natural disasters, technological accidents, terrorist attacks, power failures, strikes, etc.

According to the analysis in EU (2012b) there are particularly important strategic risks, financial risks, operational risks and risks associated with threats according to the approach followed by the All Hazard Approach (FEMA, 1996). According to ISO 28000:2010 (ČSN, 2010) major damage in supply chains causes: physical failure (e.g. failure of the equipment, intentional physical damage); operational failure (technical failure, human error); natural disasters (e.g. floods, storms); external threats (e.g. failure of outsourced activities or externally ensured activities); and threats from interested parties (e.g. the State – the failure of complying with legal and other regulations).

According to the EU documents, shown in Dequae (2012), the supply chain must adhere to the following sub-categories of risk: construction and design and technological risks; credit risks, market risks, external risks, operational risks, and risks associated with management and decision-making. Analysis and evaluation of these risks are required when applying for the European Union's projects (Procházková, 2011b). Construction, technological and design risks include: construction and design risk; site risks, and the risk of erroneous technologies, networks and related services. Construction and design risks that include the risk associated with the design documentation (good/bad, error); risk connected with construction; risk connected with exceeding construction costs; risk connected with the pollution of the site/site vicinity during the project's realisation which is caused by public administration; risk connected with the pollution of the locality/neighbourhood during the project, which is caused by the supplier; the risk associated with the impact

of the project on the environment during the project's life that is caused by bad decisions of public administration; and risks connected with the project's impact on the environment during the project's life that were caused by the contractor and operator). The risk of a given site includes the risk associated with the current entity; risk associated with the availability of site; risk associated with ownership of the site; risk associated with the state of a site; risk associated with networks (utilities) located on the site (construction site); risk associated with the land-use plan; risk associated with a construction permit; risk associated with cultural/ archaeological heritage; and risk associated with the protected landscape area. The risks associated with faulty technologies, networks and related services include: risks associated with a defect during the implementation of the project; risk associated with a defect within the lifetime of the project; risks associated with using the wrong technology; risks associated with technological insufficiency; the risk associated with an unexpected disruption of power supply, loss of services and support systems provided by the private sector; and risk associated with an unexpected disruption of energy supply, loss of services and support systems provided by public administration. Credit risks include: liquidity risk; and risk of default/i.e. the availability risk, which is further divided into: risk associated with availability (default by the private sector); risk associated with the failure of counterparty and with the loss for public administration; risk associated with the failure of the counterparty and loss for the supplier; risk associated with concentration (for all deliveries there is only one supplier); and risk associated with rejection of partnerships (public administration does not support the project). Market risks include: demand risk in the case that the contractor is a public administrator; demand risk if the supplier is a private entity; the risk that the benefit is for rival; and other market risks such as: currency risk; inflation risk; and interest rate risk. External risks include: political risks; force majeure; and other external risks. Political risks include: risk associated with the national or international situation; risk of government default; and supranational political risk associated with the duties of the state in the EU and NATO. The risk associated with force majeure includes: risk associated with natural disaster with the size of catastrophe; risk associated with terrorism; and the risk associated with war. The item "other external risks" includes: the risk of legal/tax of a general nature associated with changes in legislation/taxes; risk of legal/tax of a specific nature; the risk associated with the need for additional authorizations; and the risk associated with the situation in the sector (strikes). Operational risks include: risks related to the equipment; the risks associated with people; and risks associated with human negotiation. Risks associated with the device include: the risk associated with the device inputs (material); risk associated with maintenance, repairs, modifications and adaptations; and the risk associated with small amortized cost. Risks associated with humans include: risks associated with inadequate labour; risk associated with non-replaceability; risk of scarce human resources; risk associated with labour-legal disputes; and risk associated with human error. Risks associated with human negotiation include: risks associated with fraudulent negotiations; risk associated with illegal negotiation; risk associated with the safety of technological systems; and risk associated with derogation and theft.

Risks associated with management and decision-making include: contractual risks and other risks associated with management and decision-making. Contractual risks include: risks associated with the responsibility to third parties; risks associated with the change of contract; and the risk associated with the violation of generally binding regulations. Other risks associated with governance and decision-making include: risks associated with strategic decisions; and the risk associated with reputation. The definitions of partial risks in the financial sectors are given in Procházková (2011b).

The risks of supply chains according to work (EU, 2012b; Minárová & Dejnega, 2009) and performed simulations provide the following phenomena: traditional property risks - fires, natural disasters, power system outages and downtime of devices; theft, violence and terrorism; political instability and risks, fluctuations in exchange rates, supply interruptions due to political problems in the country of the supplier; fraud and some consequences of centrally planned economies; failures of computer and telecommunication networks; very demanding customers requiring fast and precise delivery; short product life cycles as a result of the diversity of products, their substitutability and emphasis on their continuous innovation and flexibility; complete conformity of the products according to the laws of individual countries; and failures in communication with suppliers. The risks associated with supply chains are very serious, and therefore, they are the subject of current research and investigations (Kinder, 2012). The overall objective of risk management of the supply chain is to identify current sources of risk in supply chains, to perform a distribution of risks according to the size of damage that could be caused their occurrence, and to find a suitable trade-off with risks so that the operational organizations may be safe and no adverse impacts on public interests may occur.

Based on the documented statistics (Kinder, 2012) the following five most frequent risks to the supply chain are: failure of suppliers; production interruption; logistical difficulties; IT failures; and the rising prices of oil and energy. These risks are predictable, their trade-off is essential for a safe organization, and hence, organizations pay critical attention to their management.

The international supply chain has many participants and covers a huge amount of goods. The vulnerability is double: on the one hand there is a large risk of failure for the origination due to a terrorist attack, and on the other the goods are used for a means of attack. At the same time there is vulnerable to the economy of the countries, which directly depends on the reliability of the supply chain. International supply chains also suffer from the consequences of abduction (Kommerskollegium, 2008). Therefore, internationally and within the EU there are extensive programs for the protection of the international supply chain, especially transport shipment, sea freight, air, rail and automotive (Kommerskollegium, 2008). An important role in the international scale of safety is played by a non-profit organization TAPA (TheTransportedAssetProtectionAssociation) that was founded in 1997 in the USA; in Europe it started to be active in 1999 and in Asia in 2000.

In practice it holds the generic standard for the management of security systems, ISO 16125, which deals with security systems related to all forms of threats to organization by fraudulent, malicious, dishonest or intentionally negligent individuals or entire organizations. To ensure safety it means to establish, implement and maintain an adequate level of protection and measures against such threats. The purpose of the document is to provide a security team of organization the systematic approach and guide for the assessment and management of security risks with the target of reaching an overall safe level for the operation of the organization and other stakeholders.

The detailed guidance annexed to this standard states that threats are specific for different sectors, and it gives solutions in line "with good practice" that can be applied in the security policies, procedures, infrastructure, systems and tasks in order that it may be possible to face individual risks. A generic document builds on the existing ISO standards relating to safety and adds them, as e.g. standards that specifically deal with information, information technology, intellectual property and the safety of supply chains (ÚMNZ, 2011).

The logistics of the supply chain is based on information sharing between enterprises based on electronic technologies with reality that the technologies used and their applications

are different. From a technological standpoint, these are systems of Supply Chain Management - Supply Chain Management (SCM) based on standard principles characteristic for the implementation of relations company with company, a Business-to-Business (B2B), i.e. on electronic data interchange (Electronic Data Interchange - EDI), applications based on XML technology and standards (eXtensibleMarkupLanguage) and on web applications. Functionality for APS (AdvancedPlanning and Scheduling) is based on transactional applications (e.g. ERP-type - EnterpriseResourcePlanning), possibly in combination with applications and tools for business intelligence. Under the term APS it is understood as a system ensuring production planning whilst considering all possible restrictions of the production system, such as material, labour capacities etc.

Support for supply chains in the EU focuses on support of the so-called intermodal transport logistics, which is a key element of European transport policy. It aims to create a technical, legal and economic framework conditions and innovative concepts for the optimal integration of different modes for services provided by the "door to door" method. In particular it goes on to ensure that modes that are more environmentally friendly may be integrated into the transport chain, such as rail, inland waterways and maritime transport for short distances. The EU adopted a number of regulations and directives in order to create a single European transport market. The legal basis for this Title V of the EC Treaty, in particular Article 71 (Treaty of Lisbon: Title VI, particularly Article 91 of the Treaty on the European Union).

Supply chains according to standard (ČSN, 2010) include all interconnected components of the delivery process, starting from collecting the raw materials and ending with the delivery of the product to the consumers (end users). The low professional level within the EU is highlighted in the work (Burian, 2003) according to which it is necessary "to improve co-operation and communication between Member States on a multidisciplinary approach. In this area it will be necessary to create a set of equivalent methodologies for the evaluation of safety and vulnerability in specific areas".

The work (Setola, 2009) shows that in the EU countries, in terms of global risk, insufficient attention is paid to threats to the food chain, to which drinking water belongs. According to experience it is necessary at the supply chain management level to pay attention to organized crime, which in recent years has become an economic threat. With theoretical considerations a global perspective is necessary and in practice it is necessary to pay attention to the protection of insured partners along the whole chain, as insurance is one of the basic tools for the trade-off with risk (Procházková, 2011b). The present style of management called “Just in Time” (Procházková, 2011a) facilitates the situation to enterprisers and businessmen on one side – they do not pay attention to reserve resources, however, on the other hand it causes a strong dependence on early perfect supply chains.

5 DEFICITS REVEALED IN THE MANAGEMENT OF THE PROTECTION OF LIFE GIVING INFRASTRUCTURES AND SUPPLY CHAINS

The results of a study of the level of management of infrastructures’ and supply chains’ failures documented in detail in works (EU, 2012a, 2012b; Procházková, 2009, 2012b; Procházková & Říha, 2012; Procházková et al., 2012) are summarized in Table 2.

Table 2: Deficits at failures' management from the viewpoint of the safe community concept (EU, 2012b).

SECURITY ITEMS	RESEARCH RESULTS
Security challenges that can be considered to have a big impact in the 2035 time frame and currently are not sufficiently addressed in the planning of research	The list of followed disasters is necessary to supplement with: ▪ Disuse of research infrastructure. ▪ Disuse of educational infrastructure. ▪ Disuse of social infrastructure. ▪ Disuse of supply chains for terrorist attack. ▪ Disuse of supply chains as a political attack.
Most severe security challenges that should be addressed by research planning in the 2035 time frame	The disaster order with regard to impact severity is: ▪ Mid-term failure of social infrastructure (disintegration of human society into intolerant groups). ▪ Failure of public administration infrastructure due to corruption, disuse of power and non-respect for the public's interests. ▪ Long-term outage of electrical infrastructure. ▪ Long-term stoppage of drinking water supply. ▪ Long-term shortage of basic foods.
Challenges for future security research for prevention, preparedness, response and renovation	It is necessary to establish norms and standards for infrastructures that will: ensure their sufficient capacities; enhance their robustness and resiliency. To create an effective system for response, especially in case of failure of finance infrastructure and in the case of failures of critical supply chains. To create a system for renovation (recovery) after critical infrastructures' failures.
Related main vulnerabilities to be addressed for future security research	The massive collapse of the financial market. Long-term outage of electrical energy supply. Long-term stoppage of drinking water supply. Long-term shortage of food supply. Long term failure of critical supply chains. Lack of technical resources, inadequate knowledge and training of managerial staff, poor response management and lack of finances.
Related main knowledge gaps to be addressed for future security research	Methods used are based on deterministic and stochastic approaches and on the assumption that each system is steadily in a steady (stationary) state or close to it, which is not always true. In practice it is necessary to include non-linear thinking and a way to live with risks connected with interdependences. E. g. lessons learned from the Fukushima accident (Procházková, 2012b) show that it is necessary to improve the methods associated with the determination of terms of references for the design, construction and operation of technological buildings, equipment and infrastructures.

	An effective strategy for the robustness and resilience of critical supply chains.
Proposed type of future security research	System of management of territory, entities, sectors, infrastructures and chains of critical resources, goods and needs. Integral risk management – because procedures applied so far do not consider cross-cutting risks, which are the cause of cascading failures of complex systems. Respect for public interest and principles for integral safety management.
Expected most needed topics of future security research	Strategic, proactive and systemic management of territories, sectors, infrastructures and chains that respect public interest and the principles for integral safety management.

6 CONCLUSION

Current practice requirements require in order that each system may be safe under all conditions, not only to themselves but also for their surroundings (i.e. they do not endanger their surroundings through their failure). Therefore, it is necessary to base their management on current knowledge, see, for example, the application of the theory of possibilities in practice (Procházková, 2012b), and especially complies with the principles of good management (governance), which except the responsibility and respecting the public interest, includes early recognition of emerging risks and timely application of corrective measures and actions. To ensure safety in both domains, the critical infrastructure and the supply chains, it is necessary to determine, introduce and keep an appropriate level of protection and countermeasures against real risks.

Among the important supply chains belong: the Food Chain; and the plan of the necessary supplies, and, therefore, in the EU and the Czech Republic a considerable amount of attention should be paid to their safety. Generally speaking, in the EU the issues associated with supply chains are not completely solved and it is necessary to make some major modifications.

REFERENCES

Burian, P., 2003. *Management of Supply Chains– SCM of Industrial Enterprises by Help of Multi-agent Systems*. Praha: VŠCHT.

ČSN, 2010. *ČSN ISO 28000: 2010. Specification for Safety Management Systems for Supply Chains* [online]. [cited 2013-04-21]. Retrieved from: http://www.aecsro.cz/informace/info18.pdf (in Czech)

Dequae, M., 2012. Managing Supply Chain Risks. *Risk-Management.cz* [online]. [cited 2013-04-21]. Retrieved from: http://www.risk-management.cz/

Ellul, J., 1980. *The Technological System*. New York: The Continuum Publishing Corporation. ISBN 0-8264-9007-4.

EU, 2012a. *FOCUS project, Deliverables D5.1, D5.2, D5.3* [online]. [cited 2013-04-21]. Retrieved from: www.focusproject.eu

EU, 2012b. *FOCUS project study* [online]. [cited 2013-04-21]. Retrieved from: http://www.focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c46959712 f8a

FEMA, 1996. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA.

Kinder, A., 2012. Management of Supply Chains Minimises the Losses. *System Online* [online]. © 2001 - 2013 CCB spol. s r.o. [cited 2013-04-21]. Retrieved from: www.systemonline.cz/it-pro-logistiku/rizeni-rizik-dodavatelskeho-retezce-minimalizuje-ztraty.htm (in Czech)

Kommerskollegium, 2008. *Supply Chain Security Initiatives: A Trade Facilitation Perspektive*. Stockholm: National Board of Trade, pp. 124. ISBN 978-91-977354-3-8.

Minárová, A., Dejnega, O., 2009. *New Factors of Risk in Supply Chain*. In *Sborník Konference MendelNet PEF 2009*.

OECD, 2002. *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD. 191 p.

Procházková et al., 2008. *Hazardous Chemical Substances and Chemical Preparations and Industrial Incidents*. Praha: PA ČR. 420 p. ISBN 978-80-7251-275-1.

Procházková, D., 2009. Critical Infrastructure Safety Management. In *Reliability, Risk and Safety. Theory and Applications*. Leiden: CRC Press / Balkema, pp. 1875-1882. ISBN 978-0-415-55509-8.

Procházková, D., 2011a. *Strategic Management of Safety of Territory and Organisation*. Praha: ČVUT. 483 p. ISBN 978-80-01-04844-3.

Procházková, D., 2011b. *Analysis and Management of Risks*. Praha: ČVUT. 405 p. ISBN 978-80-01-04841-2.

Procházková, D., 2012a. Results of Selected Methods Evaluation. *SPEKTRUM*, 11 (2), pp. 47-51. ISSN 1211-6920, ISSN 1804-1639.

Procházková, D., 2012b. *Critical Infrastructure Safety*. Praha: ČVUT. 308 p. ISBN 978-80-01-05103-0.

Procházková, D., Kopecký, Z., 2012. Problems of Bank Sector. In *Požární ochrana 2012,* Ostrava: SPBI, pp. 250-252. ISBN 978-80-7385-115-6.

Procházková, D., Říha, J., 2012. Selected Security Problems of Supply Chains. In *Požární ochrana 2012*, Ostrava: SPBI, pp. 266-269. ISBN 978-80-7385-115-6.

Procházková, D. et al., 2012. Management of Disasters Connected With Technologies and Infrastructures. In *Požární ochrana 2012.* Ostrava: SPBI, pp. 246-249. ISBN 978-80-7385-115-6.

Setola, R., 2009. Security of the Food Supply Chain. In *31st Annual International Conference of the IEEE*. Minneapolis: EMBS.

ÚNMZ, 2011. *ISO 16125 – Generic Norm for Management of Security Systems*.

Zemánek, O., 2008. *Development of Supplies in Small and Medium Enterprise*. Brno: Fakulta podnikatelská, Ústav ekonomiky. 68 p.