MEST Journal
DOI 10.12709/mest.02.02.02.15

CRITITAL INFRASTRUCTURE PROTECTION FROM THE VIEW OF TECHNICAL STANDARDS

Mária Lusková
University of Žilina - Faculty of Special Engineering, Žilina, Slovakia

Zdeněk Dvořák
University of Žilina - Faculty of Special Engineering, Žilina, Slovakia

Ladislav Novák
University of Žilina - Faculty of Special Engineering, Žilina, Slovakia

JEL category: **H54**

Abstract

Protection of critical infrastructure is an important issue of modern civilisation. Critical infrastructure systems include facilities and assets publicly or privately owned that are so vital that their destruction or incapacitation would disrupt the security, economy, safety, health, or welfare of the public. In the European conditions, they usually include from six to ten sectors. Transportation systems, energy and information networks belong to the very important sectors. At present, in the Slovak Republic, the attention is given especially to the sectors of transportation and energy. In the last years the researchers of the Faculty of Special Engineering of the University of Zilina participate in the research project focused on the issues of the critical infrastructure protection in transportation sector. There was also accredited study program Security and Protection of Critical Infrastructure for the bachelor and master degrees.
In the paper the authors are dealing with protection of critical infrastructure objects in the context of the technical standards. They include especially standards related to the risk management and quality management (ISO 31000:2009, ISO 9001:2008, ISO/IEC 27001). In the paper there are published partial results of the research oriented on the effect of implementation of the above mentioned standards on the situation in critical infrastructure protection.

Keywwords: *Critical infrastructure protection, ISO standards, security, risk management.*

Address of the corresponding author:
Mária Lusková
Maria.luskova@fsi.uniza.sk

1 INTRODUCTION

Critical infrastructure protection (next CIP) is the phenomena of the last decade. After the attacks on the Twin Towers in New York on 11 September 2001, the legal rules for increasing protection and security of important entities – the critical infrastructure elements (next CI) were progessively developed (Act No. 45/2011, 2011).

Within the EU member states first the issues of objects identification and their including among the European critical infrastructure elements and national critical infrastructure elements were solved. Some countries specified also elements at the regional critical infrastructure level.

Enhancing protection of specified critical infrastructure elements was the next task. In this context various methods, metodologies and processes were defined (Dvořák, Soušek, Sventeková, Leitner, & Čižlák, 2010).

In regard to the scope of the issues and miscellaneousness of the critical infrastructure elements it is necessary to investigate the issues in detail within the specific branches. In last time the attention is concentrated especially on transport and energy sectors and information and communication technology (ICT) sector at the European and national levels (Voeller, 2005).

The researchers of the University of Zilina in cooperation with foreign colleagues are dealing with the issues of CIP very intensively. Since year 2011 they are solving project entitled Critical infrastructure protection in sector transportation supported by the Slovak Research and Development Agency. In years 2011-2013 also the project, entitled Integration of quality management and risk management, that brought new viewing angle on the solved issues, was solved at the University of Zilina. Since year 2014 the researchers of the University of Zilina will also participate in FP7 research project entitled Risk Analysis of Infrastructure Networks in response to extreme weather.

The aim of this paper is to present the results of the research in the field of critical infrastructure protection. The paper is also dealing with common issues of standards for quality assurance and risk management. Within application of the mentioned standards it is advisable to specify the fields where the respective standard will be implemented.

2 EXPERIENCE WITHIN USING METHODS DEALING WITH CRITICAL INFRASTRUCTURE RISK ASSESMENT

The whole risk management process in critical infrastructure consists of several partial activities. The first step, identification of hazard sources, is followed by risk analysis. Realization of these two basic activities requires selecting the most suitable methods. Identification of hazard sources can be done either by detailed statistical data for given system or expert evaluation. Risk analysis is a basic step in the risk assessment process. The basic classification of usable methods is given by the expression of values used in risk analysis as follows:

- qualitative,
- quantitative,
- semi-quantitative.

At the beginning risk analysis and assessment were connected with use of qualitative methods that generally assessed the subsystem with conclusion that some measures are needed to be accepted or not.

At present high degree of using information – communication technologies and expert systems development bring the need to use semi-quantitative and quantitative methods. These methods use broad knowledge basis, present expert systems enable so called data mining from other information systems and internet sources. So very detailed structured information sources are necessary for semi-quantitative assessment. Applying quantitative methods is often connected with problems of needed data absence. In that case the expert estimation is usually applied to assign required values.

2.1 Methods applicable for critical infrastructure risk assessment

There are many methods and techniques dealing with risk that are used almost in all spheres of human activity with effect. The attention is oriented especially on effort to affect existing risks and their impacts in economy, industry or other field. Risk

management is a systematic and logical method of determining the connections, identification, analysis, evaluation, treatment, monitoring and reporting risks connecting with any activity, function or process in such a way that organizations are able to minimize their losses and maximize opportunities (Sventeková & Dvořák, 2011).

In the Slovak Republic risk management is introduced and defined by standard STN ISO 31000 "Risk Management. Principles and Guidelines". In accordance with this standard, figure 1 presents the key steps of the risk management (STN ISO 31000:2011, 2011).

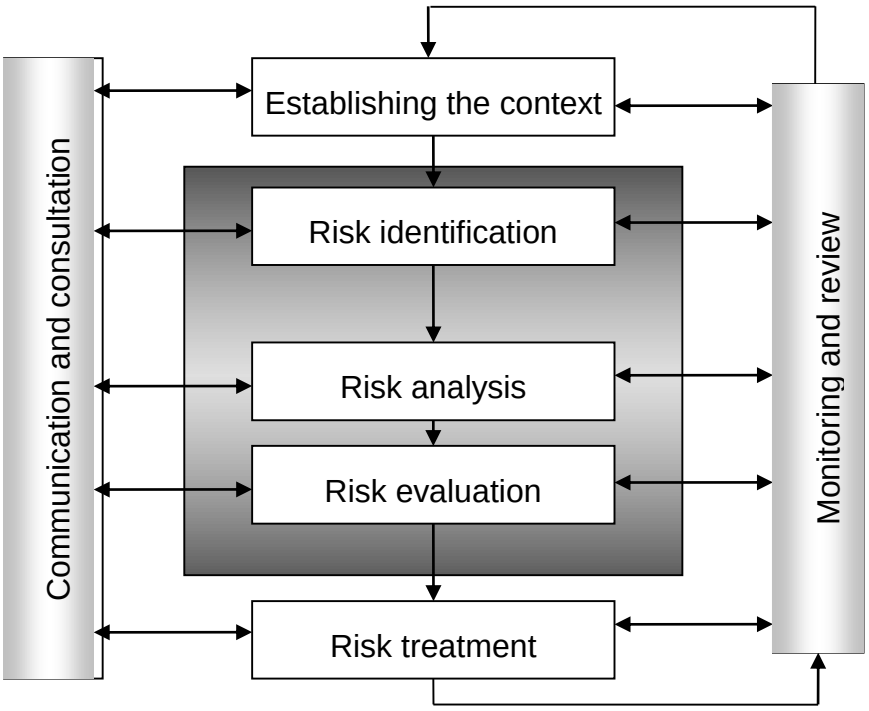

Fig. 1 Risk management key steps (STN ISO 31000:2011, 2011)

The single parts of standard STN ISO 31000 are necessary to be approximated into critical infrastructure protection.

In introduction the context should be established, that means defining those parts of the CI that will be the subject of investigation. Strategic and organization context and risk evaluation criterions should be defined, too.

Within the second step – risk identification – complex assessment of the CI threats is necessary to be done. Answers to questions what, how and why can happen are needed to be found.

Possible results with criterions defined in advance are compared within risk evaluation. Further the risk importance sequence is defined. Then assessing the risk acceptability is realized.

Within the risk treatment possible corrective measures are defined. It is necessary to evaluate their economic justness and possibilities of real implementation. Then to select and plan specific measures to be realized in proper sequence.

Communication and consultation as well as monitoring and review are feedback aimed at continuous enhancing risk management process. The whole risk analysis process depends especially on used methods. Appropriate methods should be used in all steps. Because the risk management is not strictly bound to certain system or activity, it can be used also for CI in combination with other needed and appropriate methodologies.

2.2 Selected methods of CI assessment

There are many methods dealing with risk assessment and the most widely known and used methods survey is published in „Review of 62 risk

analysis methodologies of industrial plants". Majority of methods given in Table 1 are derived from the most widely known and used methods. Single methods have different use, they provide different kinds of results and have different time and working demands (Tixier, Dusserre, Salvi, & Gaston, 2002).

Table 1 Survey of the basic and the most used traditional methods for risk assessment usable in CI

Method	Short
As Low As Reasonable Practicable/ Achievable	ALARP/ALARA
Hazard Analysis	HAZAN
Check List Analysis	CLA
Cause Consequence Analysis	CCA
Hazard Tree Analysis	HTA
Fault Tree Analysis	FTA
Event Tree Analysis	ETA
Failure Modes And Effects Analysis	FMEA
Safety Audit	SA
What if Analysis	WFA
Globalement Au Moins Aussi Bon	GAMAB
Human Reliability Assessment	HRA
Relative ranking / Hazard Indices	RR / HI
Routine Tests	RT
Rapid Ranking	RR
Hazard and Operability Study	HAZOP
Preliminary Hazard Analysis	PHA

ALARP ALARA (As Low As Reasonable Practicable / Achievable) – introduces the principle to lower the risk on such a level that is achievable (executable) in practice. The effort is concentrated on achieving the lowest risk value and in situations when the risk reduction on required level is not possible to achieve, this risk value can be accepted (but cannot be too high) if it is proved that this value is not able to be reduced by reasonable way. This principle is used especially in Great Britain. In the Slovak Republic this method is used in connection with radioactive materials

Hazard Analysis - HAZAN is one of the variants of the failure tree analysis. There is required to decide if it is necessary to do some changes to reduce this danger. The basic requirements for decision making are: frequency of failures occurrence and their probable consequences including acceptability criterions.

Check List Analysis – CLA uses check records of items or steps. Complete check list contain data "yes", "no", "is not suitable" and "other information are not needed". Check lists are often used to find out conformity between regulations and standards. This method is important as the way that enables to analyse important problems and compare them with in advance prepared record. It is also suitable for detecting the problems that already have arisen.

Cause Consequence Analysis – CCA is method integrating FTA and ETA analysis. Description of possible accident results is the result.

Hazard Tree Analysis - *HTA* - principle for assembly of hazard tree is selection of some general type of accident adequate for covering problems we want to solve. These accidents types are in detail categorized and present the opening stage in risk analysis.

Fault Tree Analysis - FTA is so called deductive method. This method is used for searching accidents or system failures and determining the causes of these negative events. Evaluation is

made by graphical model of system failures various combinations including human factor failures that can result in so called top event, i.e. principal system failure (accident).

Event Tree Analysis - ETA enables graphical presentation of possible accident results following from the initiatory events. The result is graphical and numerical presentation of possible accident scenario with quantity of failures and errors leading to top events, i.e. accident. The basis of this method is development of certain negative event through other affecting factors to result impact – accident.

Failure Modes and Effects Analysis - FMEA assess possible equipment failures and their impact on technological process at various levels. It is used for identification of failure kinds on single equipment and systems.

Failure Modes, Effects and Criticality Analysis – FMECA extends FMEA method. It includes characteristics of failure existence frequency or their probability.

Safety Audit – SA – this audit is understood in relation to existing operations and includes systematic and critical assessment of selected aspects of transport technology operation or single transport equipments. It presents inspection rounds that can have character from informal visual inspection to formally finding that takes more time. Assessment is made by team of people of various professions.

What if Analysis - WFA – the aim of security assurance by this method is identification of dangerous situations in technological process. With help of typical questions beginning with traditional „What happen if“ are detected causes for accidents and measures for increasing security are proposed. There can be expressed any objection concerning security and may not be expressed as question.

Human Reliability Assessment - HRA - the aim of this method is to identify possible human mistakes, their effect and reasons. It presents systematic evaluation of factors affecting the action of operators, technicians, maintenance men and other personnel in transport. It systematically names the mistakes that can occur in the course of standard operation of technologies or in emergencies.

*Relative Ranking/Hazard Indice*s means assessment of process seriousness on the base of physical-chemical properties of substances, technical-security parameters, their quantity, process thermodynamics and other characteristic events. These methods do not allow monitoring causal dependences cause and effect.

Rapid Ranking – RR enables rapid ranking of danger through inflammability, explosiveness and toxicity indexes. Inflammability and explosiveness indexes are determined on the base of material factor and degree of so called general and specific danger (risk sources) of process. Technological process or transport units are classified in one of three categories according to the resulting value of mentioned indexes.

Preliminary Hazard Analysis - PHA – this hazard analysis provides very quickly survey of operational hazards that can be start base for detailed analysis. This way can be also applied in early stage of planning when only very general purposes and technological schemes are to disposal.

The first step, selection of appropriate methodology, is the most important step for the complete risk assessment of the CI. Because not every method is usable for risk assessment in relation to CIP, selection of appropriate method is affected and conditioned especially by:

- results we want to achieve considering the reality that each methodology has its limitations,
- availability of needful information about examined system that are necessary for application of selected methodology.

2.3 Case study for railway risk assessment

Selection of methods depends on specific sector or subsector of CI. Within the above mentioned project we focused on subsector railway transport. The most often used methods for railway risk assessment are as follows:

- IAEA-TECDOC-727,
- CPR 18E - Purple Book,

- TRA,
- ARAMIS,
- Common Safety Method.

Method IAEA-TECDOC-727 presents so-called screening method that enables classification and determination of social risk sources priorities. This methods allows classification of danger from mobile sources (road, railway, water flows), completion of accidents consequences assessment with probability aspect based on historical data from accidents in the past.

Method according to the CPR 18E - Purple Book was elaborated and issued by TNO organization. It allows quantitative risk assessment for transportation of dangerous goods. The specific process of risk assessment for transportation of dangerous goods is second part of document CPR 18E-Purple Book and start from analysis of reports dealing with former accidents.

Method according to the Guideline for Chemical Transportation Risk Analysis - TRA elaborated by Center for Chemical Process Safety - American Institute of Chemical Engineers (AIChE). The security study elaborated according this methodology present risk measure in relation to transport operations of dangerous goods by qualitative, semi-quantitative or quantitative approach. In quantitative and semi-quantitative approaches are in principle used the same methods as in methodology Chemical Process Quantitative Risk Analysis – CPQRA.

Methodology Accidental Risk Assessment Methodology for Industries in the framework of the SEVESO II directive - ARAMIS uses two existing methods and principles for risk assessment. I tis based on created reference accidental scenarios according to:

- types of equipment,
- present dangerous substances,
- conditions of running processes.

This methodology was developed within research projects of the European Union. The risk assessment is based on assignment of risk measure through integration of three independent partial indexes:

- assessment of accidental scenarios importance, so called S-INDEX,
- assessment of effectivity of risk management, so called M-INDEX,
- assessment of vulnerability of the risk source environment, so called V-INDEX.

Experiece with application of various methods for CIP assessment lead to the future integration of these methods with some standards, detailed described in chapter 3.

3 INTEGRATION OF QUALITY AND RISK MANAGEMENT STANDARDS

At present many organizations have adopted or are adopting except ISO 9001 also other management system standards such as ISO 14001 Environmental management systems, ISO 31000 Risk management, ISO/IEC 27001 Information security management systems, ISO 22000 Food safety management systems, ISO/TS 16949 Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations, OHSAS 18001 Occupational health and safety management systems and others. With respect to increasing pressure and requirements of their internal and external stakeholders, adopting several management systems have become a necessary condition of their existence and sustainability. However the integration process is not standardized and each organisation must find a way how the processes within the management systems can be best integrated to achieve significant integration benefits and meet business needs (Luskova, 2013).

Quality management and risk management belongs to the key factors of performant management. It can be said that the risk and quality are two sides of the same coin: quality is the measure of satisfying the requirements, and risk measures the weight of unfavorable situations, deviations from the requirements. These two dimensions are not mutually exclusive but complement each other, being components of the indicators system that measure the performance of the organization (Popescu & Dascălu, 2011).

Although in the ISO 9000 family of standards there is no specific reference to risk management, their philosophy is based on the principle of risk prevention. Analysis of these standards

demonstrates that they indirectly refer to risk management in many cases.

The ISO 9001:2008/Quality management systems. Requirements, for the first time explicitly emphasizes that the design and implementation of an organization's quality management system is influenced by its organizational environment, changes in that environment and the risks associated with that environment.

The ISO 9004:2009/Managing for the sustained success of an organization. A quality management approach, emphasizes that an organiazation's environment is ever changing and uncertain, and to achieve sustained success it is necessary for its management to identify associated short and long-term risks and deploy an overall strategy to mitigate them.

The risk approach method is also an integral part of the standards ISO 14001:2004/Environmental management systems. Requirements with guidance for use and OHSAS 18001:2007/Occupational health and safety management systems. Requirements. Organizations should identify and assess each of the risks they‘ve been faced. Infrequent risks with minor effects should be only controlled. Significant risks with severe consequences should be managed in such a way to eliminate them completely or reduce the frequency of their occurrence and severity of consequences (Avanesov, 2009).

Industry Quality Management Systems

In the world there are a lot of quality management systems for industry branches dealing with specific management systems. Requirements of these industry quality management systems are more demanding than the ISO 9000 family of standards requirements.

QS-9000 Quality System Requirements

The QS-9000 is an international quality management system standard for the automotive industry originally developed by and for the 'Big Three' of the American auto industry, namely, Daimler Chrysler Corporation, Ford Motor Company, and General Motors Corporation.
The main weakness of the QS-9000 is the fact that it is based on the ISO 9001:1994, which has been obsoleted and replaced by ISO 9001:2008 and so automotive companies are using the ISO/TS-16949 as the new standard for the automotive industry's quality management systems (SiliconFarEast.com, 2007).

VDA6 Verband Der Automobilindustrie/VDA Automotive standard

VDA is the German Association of the automotive industry that consists of about 600 member companies, who have come together to research and produce clean and safe auto-mobility for the future. The VDA 6.X regulations are designed for organizations in the automotive supply chain to provide a holistic quality management (VDA, 1999).

Upon introduction of the ISO 9000 in 1987, a VDA working group responsible for the standardization of technical norms recognized the necessity to integrate and adapt the general ISO standards to the particular context and environment of the automotive industry. The VDA quality management series VDA 6.X was introduced in 1991. Since August 1, 1997 the VDA quality standards are administered by the VDA Quality Management Centre that is responsible for the continuous update and translation of standards set by the ISO to the specific context of the German Automotive industry (Clarke, 2005).

ISO/TS 16949:2009

ISO/TS 16949 is the international quality management system standard for the automotive Industry based on ISO 9001. Subscribers to the standard include BMW, Chrysler, Daimler, Fiat, Ford, General Motors, PSA, Renault and Volkswagen. The introduction of TS 16949 has resulted in substantial improvements in all aspects of quality, delivery and overall efficiency throughout the supply chain and It has also reduced the requirement for multiple audits of manufacturers. This standard is applicable to any organisation within the automotive supply chain that manufactures and/or adds value to parts for supply to the automotive industry (NQA, 2013).

OHSAS 18001 Occupational Health And Safety Management Systems

OHSAS 18001:2007 are an Occupation Health and Safety Assessment Series for health and safety management systems. They are intended

to help organizations to control occupational health and safety risks. They were developed in response to widespread demand for a recognized standard against which to be certified and assessed. The OHSAS specification is applicable to any organisation (OHSAS 18001, 2007)

ISMS Information Security Management System

Information Security Management System (ISMS) is part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. Requirements for Information Security Systems are set in the Information Security Standard, originally published by the British Standards Institution. The Standard is published in two parts:

- ISO/IEC 27001, Information Security Management Systems – Requirements,
- ISO/IEC 27002, Code of practice for Information Security Management (Risk Analysis Consultants, 2013).

AQAP Allied Quality Assurance Publication

AQAP Allied Quality Assurance Publication is the management system for suppliers to the military industry developed by the NATO. Organization that is interested in cooperation with NATO countries (especially military branch) has to have introduced specific standard to prove its ability to meet all its specific requirements.

The main NATO objective in quality management of supplies is to implement such a system where particular countries would be able to produce and supply a safe, reliable and economical product for military purposes. In order to achieve this objective all parties involved are responsible for the product quality. It refers to User, Purchaser, Supplier and Government Quality Assurance Supervising Staff throughout the life cycle of a product (ZSJZ, 2013).

NUSS Nuclear Safety Standards

The IAEA is the world's centre of cooperation in the nuclear field. It was set up as the world´s "Atoms for Peace" organization in 1957 within the United Nations family. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies (IAEA, About the IAEA, 2013).

Nuclear Safety Standards are dealing with all aspects of nuclear safety. The five Codes of Practice deal with the topics (IAEA, 2013):

- governmental organization for the regulation of nuclear power plants (NUSS-50-C-G),
- safety in nuclear power plant siting (NUSS-50-C-S),
- design for safety of nuclear power plants (NUSS-50-C-D),
- safety in nuclear power plant operation (NUSS-50-C-O),
- quality assurance for safety in nuclear power plants (NUSS-50-C-QA).

HACCP Hazard Analysis and Critical Control Points

HACCP is a process control system that identifies where food safety hazards may occur in a food production process and puts into place stringent controls to prevent the hazards from occurring. By strictly monitoring and controlling each step of the process, there is less chance for hazards to occur and in this way a food business is able to assure the safety of the food products they produce.
Effectively implemented HACCP controls biological, physical, chemical and allergen hazards within a food operation. HACCP can be implemented as a separate risk management system or as part of a certification to ISO 9000 (Standards.org, 2011).

4 CONCLUSION

In conclusion we would like to present some important conclusions and recommendations.

For the first we underline improving the vocabulary and its correspondence with international standards. Some fields of the research of the critical infrastructure protection specific elements are still not sufficiently solved also thanks to insufficient vocabulary. Recommendations in the field of standardization are one of the results of our research. Within our research we meet with different approaches to risk analysis and assessment in various fields.

Another important aspect is application of modern information – communication technologies (ICT) within the critical infrastructure protection. At present physical and object security and safety without ICT application is not possible. Except the

real attackers, who want to destroy the specific object, the great risk is represented also by internet attackers who want to take control of management and information systems.

Important aspect is also inspection of performing the measures defined by the laws and regulations. Every critical infrastructure element must have always elaborated security plan. Its implementation has to be checked and verified. In case realization of the protection is in accordance with security plan than the security level is evaluated as very well. In case the tasks of the security plan are not fulfilled, some activities are evaluated as insufficient and other corrective measures are needed.

WORKS CITED

Act No. 45/2011. (2011, 02 08). *Zakon o kritickej infraštruktúre.* Retrieved 03 05, 2014, from zbierka.sk: http://www.zbierka.sk/ ; http://www.zbierka.sk/sk/vyhladavanie?filter_sent=1&_filter_predpis_aspi_id=45%2F2011+Z.z .&q=

Avanesov, E. (2009). Risk management in ISO 9000 series standard. *International conference on Risk Assessment and Management* (p. 11). Geneve: Economic Commission for Europe. Retrieved 02 14, 2013, from http://www.yumpu.com/en/document/view/15319840/risk-management-in-iso-9000-series-standards

Clarke, C. (2005). *Automotive production systems and standardisation.* Heidelberg: Springer.

Dvořák, Z., Soušek, R., Sventeková, E., Leitner, B., & Čižlák, M. (2010). *Riadenie rizík v železničnej doprave (eng. Risk Management of Railway Transport).* Pardubice. Retrieved from http://edis.uniza.sk/publikacia/5985/Riadenie-rizik-v-zeleznicnej-doprave/

IAEA. (2013). An overview of the Nuclear Safety Standards (NUSS) Programme. *IAEA BULLETIN, 21*(2/3), 13-17. Retrieved 02 12, 2014, from http://www.iaea.org/Publications/Magazines/Bulletin/Bull212_3/212_302001317.pdf

IAEA. (2013, 02 14). *About the IAEA*. Retrieved from IAEA: http://www.iaea.org/About/about-iaea.html

Luskova, M. (2013, 07 15). The contemporary trends in integration of management systems. (Z. Čekerevac, Ed.) *MEST Journal, 1*(2), 71-79. doi:10.12709/mest.01.01.02.06

NQA. (2013). *All NQA Services What is ISO/TS 16949:2009?* . Retrieved from NQA: http://www.nqa.com/en/atozservices/what-is-ts-16949.asp

OHSAS 18001. (2007). *OHSAS 18001 Occupational Health and Safety Zone - The Health and Safety & OHSAS Guide. [cit. 2014-03-05*. Retrieved 03 05, 2014, from OHSAS Health & Safety Standard: http://www.ohsas-18001-occupational-health-and-safety.com/index.htm

Popescu, M., & Dascălu, A. (2011, 03 31). Considerations On Integrating Risk And Quality Management. *Annals of "Dunarea de Jos" University of Galati, XVII*(1), 6. Retrieved 03 05, 2013, from http://www.ann.ugal.ro/eco/

Risk Analysis Consultants. (2013). *ISMS: ISO/IEC 27001 and ISO/IEC 27002 standards*. Retrieved 03 05, 2014, from Risk Analysis Consultants: http://www.rac.cz/rac/homepage.nsf/EN/BS7799

SiliconFarEast.com. (2007). *QS 9000*. Retrieved 03 05, 2014, from siliconfareast.com: http://www.siliconfareast.com/qs9000.htm

Standards.org. (2011). *HACCP Hazard Analysis Critical Control Point*. Retrieved 03 05, 2014, from Standards.org: http://www.standards.org/standards/listing/haccp

STN ISO 31000:2011. (2011). Manažérstvo rizika. Zásady a návod (eng. Risk Management). In *Slovenský ústav technickej normalizácie* (p. 40). Bratislava.

Sventeková, E., & Dvořák, Z. (2011). Human activity as a risk in railway transport. *Transport means 2011, Proceedings of the 15th international conference* (pp. 50-53). Kaunas, Lithuania: Kaunas University of Technology.

Tixier, J., Dusserre, G., Salvi, O., & Gaston, D. (2002). *Review of 62 risk analysis methodologies of industrial plants. [cit. 2014-03-05*. Retrieved from ScienceDirect: http://www.sciencedirect.com/science/article/pii/S0950423002000086

VDA. (1999, 04). *Quality Management in the Automotive Industry - Basics for Quality Audits.* Retrieved from MBA lib: http://doc.mbalib.com/view/5f7c3756b9ad3808a98b6fa921087c0dd.html

Voeller, J. G. (2005, 03 05). *CIPP - Critical Infrastructure Protection Priorities. [cit. 2014-03-05.* Retrieved 03 05, 2014, from The Construction Sciences Research Foundation, Inc.: http://www.csrf.org/pubs/cipp.html

ZSJZ. (2013). *AQAP - Introduction.* Retrieved 03 05, 2014, from ZSJS: https://www.zsjz.pl/en/Certification/AQAP.html

ACKNOWLEDGEMENT

This paper was supported by projects:

APVV 0471-10 *Critical Infrastructure Protection in Sector Transportation*

and

Innovation and internationalization of education – tools of quality enhancement of the Zilina University in the European Education Area. 2013-2015, CODE ITMS: 26110230079

Received for publication: 31.01.2014
Revision received: 23.05.2014
Accepted for publication: 23.06.2014

How to cite this article?

*Style – **APA** Sixth Edition*

Luskova, M., Dvorak, Z., & Novak, L. (2014, 07 15). Critical infrastructure protection from the view of technical standards. (Z. Čekerevac, Ed.) *MEST Journal, 2*(2), 139-148. doi:10.12709/mest.02.02.02.15

*Style – **Chicago** Fifteenth Edition:*

Luskova, Maria, Zdenek Dvorak, and Ladislav Novak. 2014. "Critical infrastructure protection from the view of technical standards." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 2 (2): 139-148. doi:10.12709/mest.02.02.02.15.

*Style – **GOST** Name Sort:*

Luskova Maria, Dvorak Zdenek and Novak Ladislav Critical infrastructure protection from the view of technical standards [Journal] // MEST Journal / ed. Čekerevac Zoran. - Belgrade : MESTE, 07 15, 2014. - 2 : Vol. 2. - pp. 139-148.

*Style – **Harvard** Anglia:*

Luskova, M., Dvorak, Z. & Novak, L., 2014. Critical infrastructure protection from the view of technical standards. *MEST Journal,* 15 07, 2(2), pp. 139-148.

Style – **ISO 690** Numerical Reference:

Critical infrastructure protection from the view of technical standards. **Luskova, Maria, Dvorak, Zdenek and Novak, Ladislav.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, 07 15, 2014, MEST Journal, Vol. 2, pp. 139-148.