MEST Journal
DOI 10.12709/mest.07.07.02.04

CRITICAL INFRASTRUCTURE PROTECTION SPECIFICATIONS IN THE TRANSPORT SECTOR

Zdenek Dvorak
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

Bohus Leitner
University of Zilina, Faculty of Security Engineering, Zilina, Slovakia

David Rehak
VŠB – Technical University of Ostrava, Faculty of Safety Engineering, Ostrava, Czech Republic

JEL Category: **R41, R42**

Abstract

Contemporary society is more sensitive to new threats than 20 years ago. More than 15 years modern democratic countries developed support for the most important objects and services as are named critical infrastructure elements. Critical Infrastructure (CI) and Critical Infrastructure Protection (CIP) have become a phenomenon of this era. (Act no. 45/2011), (European 2008/11/ES. 2008) The countries and their governments are preparing different measures to improve the security level of critical infrastructure networks. According to the current level of knowledge, the most important (critical or key) infrastructure networks include drinking water resources and water infrastructure, electric power generation sources, large power stations and high voltage transmission lines, gasholders and gas distribution systems, oil pipelines, refineries and pipeline network, important transport junctions and transit European corridors in road, rail, water and air transport. These infrastructure networks were originally built several decades' ago and are being gradually upgraded. The New Critical Infrastructure networks include computer networks, telecommunication nodes, and large data centers. At present, these major infrastructure networks are mostly threatened by natural and anthropogenic threats. The natural threats include especially all kinds of floods and extreme storms. The anthropogenic threats include especially intentional or unintentional attacks by employees, less frequently failures of technical and technological origin. Terrorist attacks on infrastructure networks are exceptional. According to the latest scenarios, the consequences of threats are critical, particularly from the point of view of further development of the society and are important for environmental, economic and social impacts. The paper presents key results of current research activities. At the time of writing this publication, the authors worked at two faculties. In the Slovak Republic, it was the Faculty of

Address of the corresponding author:
Zdenek Dvorak
Zdenek.Dvorak@fbi.uniza.sk

Security Engineering of the University of Zilina and in the Czech Republic, it was the Faculty of Safety Engineering of VŠB - the Technical University of Ostrava.

Keywords: *Best practices, central and eastern Europe, infrastructure, risk.*

1 INTRODUCTION

The Faculty of Security Engineering of the University of Žilina (hereinafter FSE UNIZA) is a higher education and scientific research institution with a wide scope of activities. In the last 20 years was adapted from the military study programs to civil study programs. In October 2015 the Accreditation Commission of Slovak Republic accredited four study programs "Crisis management", "Security and protection of critical infrastructure", "Security management" and "Rescue services". In this academic year, we will graduate the first study group in study program Security and protection of critical infrastructure. (Documentation, 2015)

2 SECURITY ANALYSIS OF CRITICAL INFRASTRUCTURE ELEMENT

The goal of the security analysis is to evaluate the conditions and influences of the environment that have significance for the security of a critical infrastructure (next CI) element and its assets (security environment). It identifies the existence of relevant security risks of the external and internal environment of the CI element, their causes or sources. It assesses their significance, probability of origin (activation) of the risk, its consequences, as well as the level of adequacy of measures accepted for lowering or preventing its impacts.

Security environment analysis for elements of the CI element is a systematic, purposeful process of acquiring, collecting and processing of information about demographics, socioeconomic, social, psychological, criminalistic and criminological, or other peculiarities of the environment, which may represent a source of security risks or potential threats. It consists of an analysis of the external environment and analysis of the internal environment of the protected object.

The security analysis has a written form. It is possible to divide it into four parts by content:

1. Analysis of the CI element.
2. Analysis of the external security environment.
3. Analysis of the internal security environment.
4. Security risk analysis. (Project OKI. 2010)

2.1 Analysis of the critical infrastructure element

It is executed for the purpose of identification of protected interests (assets) and the level of their protection. It is based on:

1. Description of the CI element, which contains mainly basic data about:
   - functions (purpose) of the object,
   - line of business the company is in,
   - number of persons (employees, management, etc.),
   - operational, production or technical devices, on storage concept, solution for internal transportation and spaces for service, maintenance, and repairs,
   - organization structure (organization order),
   - sensitive information and activities,
   - the company and other users of the object,
   - urbanistic, architectonic and construction technology solution of buildings of the protected object, their construction parts, and used building materials,
   - the working mode in the object (work order), etc.
2. Characteristic of protected interest of the CI element – usually represented by:
   - human resources,
   - material immovable property (buildings, constructions, estate, rooms, zones of the estate),
   - material movable property (machines, vehicles, IT, communication technologies, works of art and other valuable property),
   - immaterial property (licenses, patents, software, information) and others.
3. Consequence criteria for endangering of the CI element, usually being:
   - casualties and damages to the health of persons,

- destruction of property or its part,
- failure of management functions,
- the leak of sensitive information,
- operational and significant financial losses,
- pause or limiting of operation,
- loss of good business name, etc.

The correct determination of criteria shall allow the creation of an order of importance of individual elements of a protected interest.

4. Evaluation of protected interest in CI element and its prioritization. The goal of the evaluation is to assess and determine the order of significance of individual assets according to their importance. The evaluation is carried out through the value matrix to lower the subjectivity of approach as much as possible. It examines the relationship between individual elements of protected interest and the chosen criteria. Each element of protected interest is evaluated individually, for example by the point method (with the possible use of expert evaluation determined by a client's expert). Similarly, each criterion is assigned a weighting coefficient in the range of the listed amount of the relevant criteria. It is also appropriate to use for example the Fuller's triangle method. The criterion with the largest amount of points has the highest significance. In case of equal values of the weighting coefficient, the relevant criteria are joined into one criterion and are assigned to the order from the highest to the lowest weighing coefficient. (Hromada & Lukas, 2012a)

For the reason of higher transparency, the results are processed graphically using for example by Pareto chart. Together with the Lorenz curve, it may allow achievement of transparent order of protected interest according to the priority or dividing it according to its significance. For example, when protecting a human factor, the highest priority is usually given to the protection of management, or when protecting immovable property (buildings and constructions), it is given to the property containing technological devices, raw materials, storages and other entities necessary for the object of business, etc.

The importance of the division of protected interest according to achieved significance and priority allows to correctly identify security risks and to set out matching security measures. (Simak & Ristvej, 2009)

2.2 Analysis of the external security environment

This analysis should allow identification of sources of security risks and threats, located in micro- or macroenvironment.

External security macroenvironment:

1. Geographical characteristic – its importance lies mainly in the unambiguous determination of:
   - the geographical location of the protected CI element within the geographical space,
   - position relative to other objects (e.g. urban area, rural area, mountain area, area threatened by floods, border area).
2. Hydrometeorological characteristic – significantly influences work environment if the work activities are carried out in exterior. It increases requirements not only on the physical attributes of the employees but also on their psychological resistance. From the viewpoint of the position type, precipitation, climatic conditions (high temperatures, low temperatures in winter), hydrometeorological situation (snow calamities, an object located in the area of flood activities), possible fire hazards due to high temperatures and low precipitation are significant factors. Based on the results of the hydrometeorological characteristic, we may be able to identify potential risks (floods, snow calamities, fires, etc.).
3. Demographic characteristic consists of statistic data about the status (number) and structure (sex, average age, nationality, marital status, natality, mortality, migration) of citizens of the area the object is located in. It may be accompanied by indicators of economic development (employment rate, unemployment rate, monthly salary, industry, transportation, production economic activities, etc.).
4. Characteristic of antisocial activities consists of social statistical data about criminality and infractions. The data on crime is acquired from Criminal statistics evidence system

administrated by the Police Force or based on the data provided by the Office of Statistics of Slovak Republic. (Vidrikova, Boc, Dvorak, & Rehak, 2017)

2.3 Analysis of the internal security environment

The goal of the analysis of the internal security environment of the CI element is the acquirement of a basic overview of the current status and structure of the protection. The structure of the protection is given by securing of the protected interest by:

- guarding,
- regime and organizational measures,
- technical security devices, mainly:
    - mechanical barriers,
    - alarm systems, consisting of the following elements - electronic security system (hereinafter "ESS"), closed-circuit television (hereinafter "CCTV") security system, access control and management system. (Lovecek & Nagy al, 2008)

Some of the listed elements may be absent. For the purpose of achieving the goal, it is not necessary for all listed elements to be present in the security system protecting the protected interest. However, it is important to know, which elements are used for the protection of protected interest and in what quality or quantity.

1. The content of guard analysis is determination of the number of entry/exit points in an object and their character (personnel, vehicle, combined, etc.), form and intensity of the object control (permanent guarding during work time, after work time, and during holidays, checks continuously within patrol activity by a guard or through CCTV devices).
2. The analysis of mechanical barriers, consists of the examination of the status of used mechanical barriers used for:
    - perimetric protection ensures security around the protected object and signalizes violation of the object perimeter; content of its analysis consists of the evaluation of a fencing type (classic, security), mechanical state and construction of the fencing, level of passive security of barriers, type of mesh (square, nodal, welded wire), mesh material (steel from wavy wire, welded corrugated mesh, razor wire, etc.), barriers against digging under (plates, solid wall footing, steel grates), protection at entry/exit points for vehicles (gates – sliding, rotary, extensible), bars, nail barriers or spike strips, used security devices at personal entry/exit points (gates, turnstiles, safety outlets), etc.
    - room protection provides protection of space inside the protected object (communication rooms, rooms with concentration of material or mental values) and signalizes events with character of security risk or threat; it consists of a system of detectors that evaluate movement inside the protected space (PIR, AIR, dual, ultrasound, microwave detectors, etc.),
    - shell protection prevents any violation of entry units of the object. It consists of elements of mechanical shell protection of each partial object (i.e. opening fillings, walls, floors, ceilings, roofs). Their mechanical breach resistance depends on used material, its firmness, and construction (light or reinforced building). The individual elements of shell protection are evaluated independently. The opening fillings, which consist of windows and doors (STN 74 6481, 2000) are evaluated separately as entry opening doors (their construction and used material), windows and balcony doors (firmness and frame docking, shutters, means of ventilation, glass quality, used security elements – bars, blinds, security foils, etc.). Light constructions have low passive security. These are constructions mainly of drywall, hollow-brick masonry, partition concrete walls without reinforcement, etc. Reinforced building constructions are for example buildings, whose external walls consist of solid burnt bricks of 300 mm minimal thickness or concrete walls with static reinforcement at 150 mm minimal thickness, or from steel construction, etc. ; a part of shell protection is also the electronic alarm signalization (e.g. mechanical or magnetic contacts of opening fillings, glass break

detectors, alarm foils, wallpapers or decals),
- item protection supplements the security of shell and perimetric protection. It is an independent securing of selected entities within the object. It consists of storage units, which may be mobile or immovable. Among those, there are safes (built-in, strongrooms, cabinet safes, and furniture safes), safety cabinets, safe walls, archiving cabinets, security panels, etc. Among the technical elements of item protection, the most used are mainly sensors that evaluate the change of mass of a suspended object (painting sensors), mechanical or magnetic contacts, infrared gates, PIR detectors with special optics that modifies the detection characteristic (type “curtain”), capacitance or pressure sensors or tread mats.

3. Analysis of the electronic security system provides the overview of used technical security devices for the purpose of detection of violation of the protected space. Within this analysis, the following aspects are evaluated:
   - introduction of ESS,
   - description of technological level the and level of security,
   - ESS elements – disposition, purpose, and character of used detectors,
   - elements of the alarm transfer system – method of leading out the intrusion signal (local, autonomous, remote).

In case that the protection by ESS is not provided, the requirements for, e.g. number of persons providing guarding service, increase. (Velas, 2010)

4. Analysis of a CCTV security system consists of the evaluation of:
   - location and purpose of use,
   - type of CCTV system – digital, analog, etc.,
   - method of data transfer – cable, wireless (short range – uses Bluetooth technology for data transfer, medium range – uses Wi-Fi technology, far range – uses satellite or multichannel or multipoint distribution system /MMDS/ or mobile technologies /GSM, GPRS, EDGE/ for data transfer),
   - type, description, and utilization of CCTV cameras,
   - method of video signal recording,
   - display units and their resolution.

5. Analysis of access control and management systems, similarly as with the CCTV system, lies in the evaluation of:
   - location and purpose of use,
   - level of integration with CCTV and ESS,
   - entry devices - terminals.

If the access control system is used, then it significantly increases the control and overview of persons that enter or move around the protected object. It is then possible to timely detect the movement of unauthorized persons (not identified or not authorized) in a protected area or zone without increasing the number of guards.

6. Analysis of regime and organizational measures contains the evaluation of:
   - entry and exit regime of persons and monitored vehicles (entry/exit control of employees, clients, visitors and vehicles in/out of an object or it's part – determination of conditions for entry into the object based on authorizations, IDs and in a certain time),
   - movement regime of employees in an object (determination of zones – parts of an object with the limited entry for employees, labeling of affiliation of employees for certain workplaces, shops, zones, etc.),
   - material and expedition regime (process for receiving, storage, expedition, and transfer of material),
   - operational regime (ensuring of fluency and security of operation in an object, actions during crisis situations or emergencies),
   - key regime (method for labeling, assigning, turning in and storing of keys, procedures for exchange and repairs of locks and their mechanisms in important parts of the object, as well as sealing of rooms, in which sensitive information or material are located,
   - organizational measures (e.g. statute of the organization, organization order, guidelines for protection of property, guideline for protection of object – basic

regulation that sets goals, principles and scope of protection of the object, guideline for emergency and crisis situations, guideline for entry/exit of persons and entry/exit of vehicles),
- fire statute, fire alarm directives, fire evacuation plan,
- guidelines specifying the principles for processing and security of personal information according to the Act on the protection of personal data (Act 122, 2013), e.g. while processing the personal information in information system connected to the public computer network,
- guidelines for the protection of classified information created according to Act on the Protection of Classified Information (Act 215, 2004),
- guidelines for crisis management, etc.

Organization and regime measures have to be accepted by the employees of the protected object and they should identify with them. Their compliance with them is checked and enforced by the employees charged with the execution of guarding.

2.4 Security risk analysis

Identification and evaluation of security risks is a precondition and basis for their effective management. The purpose of security risk management is decreasing the risk level of occurrence negative event or phenomenon on to an acceptable level. An acceptable level is understood as a zero or low probability of its occurrence (e.g. probability of fire caused by lightning is at worst once per ten years, thus the probability of its origin in one year is on average 10 %; however, storm activity is typical for spring to autumn months of year, i.e. during 9 months, which represents 75% of year; then the probability of fire caused by lightning per year is 0.10 * 0,75 = 0.075 = 7.5%). (Vidrikova, Boc, Dvorak, & Rehak, 2017)

The goal of security risk identification is the determination of:

- all significant types and sources of security risks and threats related to a protected CI element or interest and security environment,
- preconditions of origin of each security risk.

The content of the identification of a security risk is the creation of a risk registry. The registry lists all suitable risks that have or may have a causal relationship to the protection of evaluated protected interest (or CI element). Identification of security risks is based on the analysis of the protected object and its security environment, which prove their existence objectively. Only those risks, whose existence has been objectively proved by the occurrence of negative event or phenomenon, or can be realistically assumed, should be identified. Identification of security risks has to be process-oriented and divided into different fields of sources of possible security risks. Security risks, which are not identified, can neither be managed nor influenced in another way.

Each identified security risk has to be assigned a weight, which corresponds with its significance (criticality). The process for determination of criticality is denoted as an evaluation of security risk. Value (magnitude) of security risk is an expression of its dimension. This is given by the probability of occurrence of a negative event. In addition to that, the magnitude of risk is also determined by consequences caused by the occurrence of negative events or phenomena. For the evaluation of risk, it is necessary to take into account also the character of consequences. Consequences may be direct or indirect. Direct consequences Cdir are related immediately to the protected interest. The amount of direct consequences Cdir > 1 (we may thus label them Cdir1, Cdir2... CdirN). Indirect consequences (secondary, tertiary) Cindir mean to expose the external security environment, environment, fulfillment of business obligations to immediate danger, etc. Thus, the number of indirect consequences Cindir > 1 (we may thus label them Cindir1, Cindir2, ..., CindirN). For example, effluence of suffocating gas from chemical company has no direct negative consequences on the protected object and its assets, but may cause damages on lives, health and property of persons located even several tens of kilometers away in the direction of the movement of the suffocating gas cloud (according to the current local meteorological situation).

This is determined by multiplication of non-zero probability of occurrence of potential risk (labeled P) and magnitude of its negative (harmful)

consequences – C (e.g. casualties, damages to health of persons, costs of damages on property, environment, loss of good business name, suppliers, clients, etc. The magnitude of security risk R may be expressed as the multiplication of probability P and consequences C:

$$R=P\cdot C \quad (1)$$

where $C=C_{dir}+C_{indir}$ (2)

then $R=P\cdot(C_{dir}+C_{indir})$ (3)

where:

R = potential security risk;
P = probability of occurrence of potential risk;
C = negative (harmful) consequences;
Cdir = direct consequences;
Cindir = indirect consequences.

The security risk magnitude can be expressed by a word description (so-called nominal scale), by an abstract number value (so-called ordinal scale), or percentual (so-called cardinal scale). For evaluation of security risks the following models may be used:

- probability models,
- expert estimations.

Probability models are based on the assumption, that a given phenomenon occurs with a certain probability, which may be statistically expressed (e.g. the number of cases of simple or complex thefts or violent crimes in last 5 years). Application of these models requires statistical data, based on which the parameters of probability relations could be determined. The sources of statistical data could be Office of Statistics of SR (Section Criminality and Fires), statistics of Ministry of Interior of SR published on their web pages, statistics administrated by municipal police in CI element place of residence, etc.

The expert estimates utilize direct statement of occurrence of a risk phenomenon or threat, usually not based on formalized calculation, for determination of its magnitude or significance.

The result of identification and subsequent evaluation of security risks should be their prioritization (order of significance), and thus the decision about the potentially most probable danger, to which the CI element is exposed to, if the conditions (triggers) of origin of a socially undesirable event or a phenomenon (fire, antisocial activities, electrical surge – lightning, natural disasters, emergencies, etc.).

By their priorities, measures shall be taken for individual risks, to lower their magnitude so their acceptability shall be achieved as far as possible.

Security risks that have unacceptable level, have to be lowered through the application of adequate measures to an acceptable level. The method of their correction and the tools and measures used are part of the security plan for the protection of CI element. (Sventekova & Cicmancova, 2013)

The quality of measures for lowering the evaluated security risks is positively correlated by the quality of a security plan (Hromada & Lukas, 2012b). That is influenced by the used methodology, range or complexity of proposed measures and their synergy, as well as efficiency and purposefulness. With regard to the importance of CI element (regional, national, European), it is necessary to decrease the element's riskiness as much as possible, given the potentially acting security risks, threats or dangers. Effective lowering of security risks is possible to achieve by a complex of measures that act both preventively and suppressively (Rehak, Hromada, & Novotny, 2016). The essence lies in simultaneous use of technical security devices, deployment of persons authorized to carry out guarding and organizational and regime measures. These elements constitute an integrated security system.

3 CONCLUSIONS

The perception of security may vary. Within a specific group of people, the perception of the level of security can be relatively similar. Studying the issue, personal experience and up-to-date information allow us to continually increase the level of security. The society is able to protect itself against the risks which it has already experienced relatively well. However, the protection against threats that have not yet occurred is essential. The advancement of science and research identifies new and new threats that were not considered in the past. The current results include e.g. the measurement of the content of plastics and pesticides in drinking water. Cyber-attacks on energy networks attempts to disrupt the operation of transport and computer networks are very serious. New challenges are emerging and new threats have to be considered.

The technical complexity of infrastructure networks in large agglomerations makes society very vulnerable. People living and working in agglomerations expect that all basic human needs will be secured. The shared task of academic and professional public is to find integrated and smart solutions. Their purpose is, with the use of the Internet of Things and the Internet of Everything, to continually monitor the state of all infrastructure networks and to take appropriate measures to reach predetermined security indicator boundaries.

Participation in solving international research projects brings us the knowledge of good practice from the advanced European countries. The participation of national projects links to academic and professional practice. The knowledge in the development of complex solutions, expert information systems, the use of the Internet of Things and the Internet of Everything as well as the application of the expanded reality of virtual reality is in the beginning. We are at the start of a long journey that will be characterized by many accidents, unexpected scenarios, and losses on life, property and environmental damage.

The authors encourage readers to study other available publications as much as possible so that individual risks are continuously monitored and evaluated. When creating scenarios, always ask what else can happen.

The current trend should be a culture of security in all levels ranging from personal, corporate, regional, and national to global. The security community within the globalized society will adopt new roles. Security practice requires, on one hand, safety specialists and, on the other hand, security experts.

The authors are convinced that this book has contributed to enhancing knowledge in the field of critical infrastructure and its integrated security. Let the scenarios that are created in the theoretical works and scenarios that are practiced in exercises and testing help increase the level of security and protection of critical infrastructures.

WORKS CITED

Act no. 122/2013 Coll. on the protection of personal data as amended.

Act no. 215/2004 Coll. on the protection of classified information as amended, implementation decrees of National Security Authority of the Slovak Republic for the abovementioned act.

Act no.45/2011 Coll. about critical infrastructure.

Documentation. (2015). Study program - Security and Protection of Critical Infrastructure, 2015, Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline. Retrieved from http://vzdelavanie.utc.sk/vzdelavanie/plany.php

European Council Directive 2008/114/ES. (2008). z 8.12.2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu, In Úradný vestník Európskej únie, L 345/75-82, zo dňa 23.12.2008.

Hromada, M., & Lukas, L. (2012a). Multicriterial Evaluation of Critical Infrastructure Element Protection in the Czech Republic. Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity, Vol. 2012, Iss. 340, pp. 361-368. ISSN 1865-0929.

Hromada, M., & Lukas, L. (2012b). Conceptual Design of the Resilience Evaluation System of the Critical Infrastructure Elements and Networks in Selected Areas in the Czech Republic, The twelfth annual IEEE Conference on Technologies for Homeland Security (HST '12), held 13-15 November 2012 in Greater Boston, Massachusetts, pp. 353-358. ISBN 978-1-4673-2707-7.

Lovecek, T., & Nagy, P. (2008). Security systems: CCTV security systems. Zilina: EDIS. ISBN 978-80-8070-893-1.

Project documentation OKI. (2010). APVV-0471-10 - Ochrana kritickej infraštruktúry v sektore doprava

Rehak, D., Hromada, M., & Novotny, P. (2016). European Critical Infrastructure Risk and Safety Management: Directive implementation in practice. *Chemical Engineering Transactions, 48*, 943-948. ISBN 978-88-95608-39-6. ISSN 2283-9216. DOI: 10.3303/CET1648158

Sventekova, E., & Cicmancova, S. (2013). *Risk assessment of rail transport*. In: Transport means 2013: proceedings of the 17th international conference: October 24-25, 2013, Kaunas University of Technology, Lithuania. ISSN 1822-296X. Kaunas: Kaunas University of Technology, 2013. S. 228-231.

Simak, L., & Ristvej, J. (2009). The Present Status of Creating the Security System of the Slovak Republic after Entering the European Union. *Journal of Homeland Security and Emergency Management, 6*(1), Article 20, ISSN: 1547-7355. DOI: 10.2202/1547-7355.1443 Retrieved from http://www.bepress.com/jhsem/vol6/iss1/20.

STN 74 6481. (2000).

Velas, A. (2010). *Electronic security systems*. Zilina: University of Zilina. ISBN 978-80-554-0224-6.

Vidrikova, D., Boc, K., Dvorak, Z., & Rehak, D. (2017). *Critical Infrastructure and Integrated Protection*. 1st edit. Ostrava, Czech Republic: The Association of Fire & Safety Engineering, 2017. 172 p. ISBN 978-80-7385-190-3.

Acknowledgement

This paper was supported by project
VEGA 1/0159/19
Assessment of the resilience level of the key elements of the ground transport infrastructure

Received for publication:	10.04.2018
Revision received:	20.05.2019
Accepted for publication:	10.07.2019

How to cite this article?

Style – **APA** *Sixth Edition:*

Dvorak, Z., Leitner, B., & Rehak, D. (2019, July 15). Critical Infrastructure Protection Specifications in the Transport Sector. (Z. Cekerevac, Ed.) *MEST Journal, 7*(2), 31-40. doi:10.12709/mest.07.07.02.04

Style – **Chicago** *Sixteenth Edition:*

Dvorak, Zdenek, Bohus Leitner, and David Rehak. 2019. "Critical Infrastructure Protection Specifications in the Transport Sector." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 7 (2): 31-40. doi:10.12709/mest.07.07.02.04.

Style – **GOST** *Name Sort:*

Dvorak Zdenek, Leitner Bohus and Rehak David Critical Infrastructure Protection Specifications in the Transport Sector [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, July 15, 2019. - 2 : Vol. 7. - pp. 31-40.

Style – **Harvard** *Anglia:*

Dvorak, Z., Leitner, B. & Rehak, D., 2019. Critical Infrastructure Protection Specifications in the Transport Sector. *MEST Journal,* 15 July, 7(2), pp. 31-40.

Style – **ISO 690** *Numerical Reference:*

Critical Infrastructure Protection Specifications in the Transport Sector. **Dvorak, Zdenek, Leitner, Bohus and Rehak, David.** [ed.] Zoran Cekerevac. 2, Belgrade – Toronto : MESTE, July 15, 2019, MEST Journal, Vol. 7, pp. 31-40.