MEST JOURNAL
DOI 10.12709/mest.01.01.02.13

SECURITY PLAN AS A PART OF CRITICAL INFRASTRUCTURE PROTECTION

Kamil Boc
Faculty of Special Engineering University of Žilina, Žilina, Slovak Republic

Dagmar Vidrikova
Faculty of Special Engineering University of Žilina, Žilina, Slovak Republic

Lucia Figuli
Faculty of Special Engineering University of Žilina, Žilina, Slovak Republic

JEL category: **K3, K32**

Abstract

Critical infrastructure protection and its elements is a strategic task not only of the European Union, but also of the Slovak Republic. For this reasons the Slovak government has adopted the Act No. 45/2011 on Critical Infrastructure in 2011. This legislation implemented Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The Act regulates the subject matter of the Act, definitions, organizations and competence of state administration in the area of critical infrastructure, sectorial and cross-cutting criteria, procedure for determining of the critical infrastructure elements, the obligations of the owner/operator, security plan, contact point between the owner/operator of the critical infrastructure element and the relevant Member State authority, the contain of the sensitive critical infrastructure protection related information, removal the element from the sector, administrative offence. The Act provides a stage of the process determining of European critical infrastructure elements and development of a security plan, sectors and sub-sectors of critical infrastructure and the List of transposed legally binding acts of the European Union in four annexes. The Act enacts to owner/operator of critical infrastructure elements the obligation to process security plan and to proceed according to the security plan in case of disruption or destruction of the element. According to the Act on critical infrastructure the content of security plan especially contains description of the possible ways of element threat, disruption or destruction. It describes vulnerability of element and security measures for its security. The methodology of processing of the security plan is the aim of this article.

The address of the corresponding author:
Kamil Boc
Kamil.Boc@fsi.uniza.sk

Keywords:
critical infrastructure, protection, elements, security plan, integrated security system, burglar resitance

1 INTRODUCTION

The Slovak Republic has the high developed economy. For this reason it is dependent on technology, power energy etc. Sources of the mentioned dependences are objects having a great importance for all our society. They required above-standard protection. The inclusion in elements of critical infrastructure provides this type of protection. The elements of critical infrastructure are subjected on convention security threat too, as other building used for business or services. There are mainly natural disasters, accidents, catastrophes and crime actions of singles or groups. For example the disruption of key objects of critical infrastructure from the reason of terrorist attack, natural or technological disasters would cause of a human life loss, moral damages (objects with national symbolical value) or a disorganisation of society.

2 DEVELOPMENT OF THE CRITICAL INFRASTRUCTURE PROTECTION IN DOCUMENTS OF THE SLOVAK REPUBLIC

The situation on the world has required of a protection and defence valuation of critical infrastructure on the national level. It has shown the building of isolation state formation or components is not a suitable solution. It is necessary to build an integration system. In this system individual components are capable cooperate and involve operationally in a solution of crisis situations, they are capable connect their effort according to the extent and the nature of the threat. The subject with the critical infrastructure protection and defence are considered in the Slovak Republic:

- international partners, international organisations,
- the government, public administration,
- regions,
- state economical subjects,
- private economic subjects.

After adopting of documentations of the European Union (for example The Council Directive 2008/114/ES) the Slovak Republic has realised fundamental measures for the its critical infrastructure protection. For the codification of the problem of critical infrastructure no existing in laws, its protection was only considered with the connection of the infrastructure defence according to the Act No. 319/2002 Coll. on the Defence of the Slovak Republic. (Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov, 2002) However the defence infrastructure does not involve all subjects creating critical infrastructure according this law. It only involves subjects serving for security of the state in war period.

For this reasons the Slovak government has adopted "*The Conception of Slovak Critical Infrastructure protection and defence*" (next called "Conception") in 2006. Goal has been:

a) to definite the terminology,
b) to sagest sectors of national infrastructure, which are used for the definition of critical infrastructure sectors,
c) to specify criteria for determining of critical infrastructure elements,
d) to specify principles and instruments for critical infrastructure protection and defence elements,
e) to sagest the solution for the protection of classified information (a list of classified information for private sector,
f) to outline of a security research direction,
g) to formulate conclusions and recommendations.

The conception was primarily focused on area of security and defence of critical infrastructure against terrorism as the most important factor. It accepted the need of a security comprehensive understanding of natural disaster, industrial accidents, physical wear of objects (networks), the lack of strategic reserves and raw materials, the using of weapons of mass destruction, a spread of contagious disease.

It defined the critical infrastructure as those part of nation infrastructure (chosen organisations and institutions, objects, facilities, services and systems) which destroying or putting to out of service caused by risk factor, will cause a threat or disruption of political or economical state running, or life threat and inhabitants health.

It considered as a sector of critical infrastructure the activity part which a failure (reversible or irreversible) caused by terrorist attack, will cause a threat or disruption from some of area of state security, for example:

- political or economical running of state or public administration,
- state defence,
- life, health or property of inhabitants,
- transports, informative and communicative system,

h) environment. (Koncepcia, 2006)

The critical infrastructure protection and defence in the conception was focused mainly on these the most probable attack:

- *direct action* – the direct armed physic attack carried out by armed terrorist group,
- *bomb attack* – the attack, which is generally carried out by an individual or a small group using non conventional explosives (not airplane bombarding),
- *CBRN attack* – the attack using chemical, biological, bacteriological or radioactive materials,
- *cybernetic attack* – the attack focused on the destroying of information and dates, hacking of computer system and programs generally by internet,
- *informative operations* – attacks, which wants to get or to abuse information, influence of processes founded on information (for example influence of informative system in such way that it seems to be all right, but it works with manipulateable dates) and its own information and system to protect. (Koncepcia, 2006)

Basic instruments of critical infrastructure protection and defence became:

- prevention of hazards (using mechanical barrier, public notification system, regime measures, controls, inspections, simulations, exercises and professional practices),
- risk reduction of threat of existence and stability of element (using technical facilities for discourage or detection, activities of security forces),
- avert and eliminate the consequences of the risks of attack (ensuring of alternative operations, replacement of damaged element of critical infrastructure etc.). (Jasenovec & Dvořák, 2012)

The Slovak Republic has adopted "*The National Programme for the critical infrastructure protection and defence of Slovak republic*" (next called "National Programme") in 2007 for the creating of condition to guarantee of the security of critical infrastructure.

The goal of the elaboration of National Programme was an evaluation of actual condition and an identification of the most important assets, and the determination of program steps for an improvement of it protection and defence. (Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, 2007)

It has been identified and fully-fledged 9 major sectors and 14 subsectors of critical infrastructure:

- Water,
- Food,
- Health,
- Energy (subsectors: electro energy, gas production, oil production, mining and metallurgy industry),
- Information and Telecommunication,
- Transport (subsectors: road transport, rail transport, air transport and waterways transport),
- Public Policy and Homeland Security (subsectors: Security emergency services – civil emergency services, Fire department and Emergency medical services, Police, Military),
- Industry (chemical, pharmaceutical industry),
- Finance (subsectors: payments systems, accounting system and settlements of transaction by financial instruments). (Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, 2007)

The ensuring of selected assets critical infrastructure protection had been necessary to lay out in a law.

The Act No. 45/2011 Coll. on Critical Infrastructure has been adopted by National Council of the Slovak republic on February 8th 2011. It had laid out the organisation and the scope of the public administration departments for critical infrastructure, the procedure of critical infrastructure asset selections and the

responsibility for disruption. (Zákon č. 45/2011 Z. z. o kritickej infraštruktúre, 2011)

The essential goal of the critical infrastructure law is the improvement of the present critical infrastructure protection against the increasing threat of terrorist attack.

Considering these facts the law had:

a) To determine the structure and scope of the public administration departments for critical infrastructure.
b) To adjust the process of critical infrastructure asset selections. They will be important buildings for the functioning of a society and economy. Some of them, they have cross-border importance (for example the disruption or destruction of them would have significant cross-border impact, outside
of the territory of the Slovak Republic.
c) To define tasks of natural and legal persons, which as the operators of critical infrastructure assets, they will be responsible for that.
d) To determine the sectors of critical infrastructure in which individual elements will be selected.
e) To solve the administrative-legal relationship in violation of this law. (Šimák, 2012)

In this law there is declared the one part of the critical infrastructure system is the defence infrastructure too. It serves for the ensuring of state defence adjusted in the accordance with the special law.

State administrative bodies for Critical infrastructure are the Government of Slovak Republic, The Ministry of the Interior or other state administrative bodies which will have responsible for some critical infrastructure sector. They will classify critical infrastructure elements in the critical infrastructure sectors.

The Government of Slovak Republic is required to approve:

- Conception documents of a critical infrastructure development.
- Criteria to including and excluding of critical infrastructure elements.
- Central register of critical infrastructure elements.
- Fulfilling of contact point tasks for the protection of the European critical elements in relation with Member States of European Union and European committee. (Zákon č. 45/2011 Z. z. o kritickej infraštruktúre, 2011)

Competent Ministries are empowered to carry out the public administration, controls including.

The cross-cutting criteria are provided by the law based on supposed:

1) Number of threatened person (the number of death and injured person).
2) Economic influence consisting of:
   a) Economic loss.
   b) Deterioration in the quality of goods.
   c) Deterioration in the quality of provided services in the public interest.
   d) Negative influence on environment.
3) Influence on inhabitants, it is the disruption of the deterioration in the quality of inhabitants according to:
   a) Seriousness of failure of goods supply and its recovery time.
   b) Seriousness of failure of provided services in the public interest supply and its recovery time.
   c) Availability of goods supply substitutes.
   d) Availability of provided services in the public interest supply substitutes.

The law provides for 8 sectors of critical infrastructure (Table 1.).

A condition for an including of critical infrastructure element is a fact of satisfying almost one sectorial criterion and one cross-cutting criterion.

The operator is obligatory to protect against disruption and destruction his or her critical infrastructure element. For fulfilling this task he or she is obligatory:

a) to implement the security plan, this must be reviewed and updated regularly,
b) to inform his or her employees with the content,
c) to practise at least one or more time a model situation of disruption and destruction element threat according to security plan,
d) to follow the security plan in the moment of disruption and destruction element threat.

Table 1. Sectors and sub-sectors of the Critical infrastructure

Sector	***Sub-sector***
Transport	- Road transport - Air transport - Waterways trasport - Rail transport
Electro-communicatios	- Sattelite communication - Networks and services of fixed-line and mobile electronic communications
Energy	- Mining - Electroenergy - Gas production - Oil and oil products production
Information and communication technologies	- Informational systems and networks - Internet
Post	Providing of post services, post payments and procurement activities
Industry	- Pharmaceutical industry - Metallurgical industry - Chemical industry
Water and atmosphere	- Meteorological service - Water buildings - Drinking water supply
Public health	

(Zákon č. 45/2011 Z. z. o kritickej infraštruktúre, 2011)

According to law the operator may request financial contribution for fulfilling tasks executing security measures for elements protection. (Šimák, 2012)

3 SECURITY PLAN

A Security Plan is a legal instrument for the protection of critic infrastructure element. The operator has to possess and update regularly a security plan for each critical infrastructure element. The low establishes the content of the security plan to the ensuring of critical infrastructure protection, in particularly:

- Description of various way of threats of disruption and destruction, vulnerable spots of element and security measures for it protection.
- Security measures for it protection, mainly mechanical barrier, technical security measures, security elements of informational system, physical security, organizational measures, control measures and their mutual combination. (Vidriková & Boc, 2013)

The range of security measures for protection of critical infrastructure element is determined according to assessment of disruption and destruction of element.

Elaboration process of the security plan

The security plan is elaborated in this way:

1. Definition of essential element installation.
2. Evaluation of risks, threat of disruption or destruction individual element installation, its vulnerable spot, expected consequences of element function by the disruption
   or destruction and continuity of element activity.
3. Selection of main security measures for element protection. These are divided in:
   e) Permanent security measures as investments and the processes for element protection.
   f) Extraordinary security measures, which are used according to the intensity of the threat of element disruption or destruction.
4. Definition of principal security measures for element protection.
5. The security plan is consulted by members which cooperation is expected by the element protection. (Zákon č. 45/2011 Z. z. o kritickej infraštruktúre, 2011)

The minimal method for the creating of the security plan of the critical elements protection is written in the appendix n.2 of the Act No. 45/2011Coll. under the letter C, the Act states the accepting of permanent security steps for the securing of element security. Using:

1. mechanical barriers,
2. technical security measures,
3. security elements of information systems,
4. organizational measures laying stress upon the knowing and warning, and the crisis management,
5. professional preparation for person securing the element protection,
6. control arrangements for the keeping of permanent security steps. (Zákon č. 45/2011 Z. z. o kritickej infraštruktúre, 2011)

The necessary condition for the elaboration of the security plan is executing of:

a) Analyse of security environment (external environment, internal environment).
b) Identification and evaluation of security risks, resulting from the security environment analyse.

3.1 Analyse of external security environment of critical infrastructure element

Analyse has to identify source of hazards and threats, which in macro or micro environment are located.
External security environment:

1. *Geographic characteristic* - unequivocal location:
   – Earth coordinates of critical infrastructure elements.
   – Connection and location among other critical infrastructure elements (mountain region, by floods threat region etc.).
2. *Hydro meteorological characteristic* - a factor influencing work environment if the work is performed outdoor. The important factors are: climatic condition, precipitations, floods, snow disasters, possibilities of fire.
3. *Demographic statistics* - consists from the population data (a sex, an average age, a nationality, marital status, migration). It can be supplemented by economic development indicators (employment, unemployment, a salary, an industry, a transport etc.).
4. *Characteristics of antisocial actions* are consisting of social statistic data of criminality and offences. This data are obtained from Registered-statistic system leaded by Police, or from the Statistical Office of the Slovak Republic. For the security analysis it is necessary to evaluate the data about the individual types of crime acts and about the number of attacks. These are:
   a) General criminality.
   b) Economical criminality.
   c) Other criminality. (Vidriková, 2012)

3.2 Analyse of external security environment of critical infrastructure element

The goal of analyse of internal security environment of critical infrastructure element is the achievement of the basic summary of the condition and the security structure. The structure of the security is determined by the ensuring of the protected interest:

– physical security,
– technical security measures, in particular:
  • Mechanical barriers.
  • Alarm system:
    a) Electrical security system.
    b) Camera system.
    c) Access control system.
– organisational measures.

Some of the listed elements can absent. In the order to achieve the objective it is not important if the security of protected interest is secured by all listed elements. It is fundamental to acquaint, which elements for the security of protected interest are used, for which purpose and which quality. (Vidriková & Boc, 2013)

3.3 Identification and assessment of security risks

The goal of the security risks identification is to determine:

– all important types and sources of security risks and treats in the relation with the protected critical infrastructure element or with the interest and the security environment,
– assumption of the origination of an every security risk.

The main task of the security risks identification is the elaboration of a *risks register*. There are listened all supposed risks in the register, which has or can have a connection with the protection of the evaluated protected interest (or critical infrastructure element).

To every considered security risk it is necessary to assign the importance, corresponding to its significance. The process of the importance determining we mark as the evaluation of security risks. The evaluation of security risk is an expression of its size. It depends on the probability of the occurrence of unwanted phenomenon.

The result of the identification and consecutive risks evaluation is *a prioritizing*. So it is a determination of the most probable danger, which the protected element is exposed, if the conditions for the source of society non desirable event (fire, directed against society activity, lightning, natural disasters, exceptional events

etc.) To every risk will be received steps for its acceptance. (Šimák, 2012)

4 RESISTANCES OF THE CRITICAL INFRASTRUCTURE ELEMENTS

The effective bringing down of security risks is possible to achieve with the complex of steps having the preventive and effects on the risks. The substance of it is the using of technical security measures, persons for the physical security and organized – executive steps in the same time. These elements represent *integrated security system*.

The structure of integrated security system is consists from the mutual relationships between the subsystem created by technical security measures, subsystem of organizational measures and subsystem of physical security. Individual subsystems of the protection interlock, they depend on each other and they are synergic (figure 1).

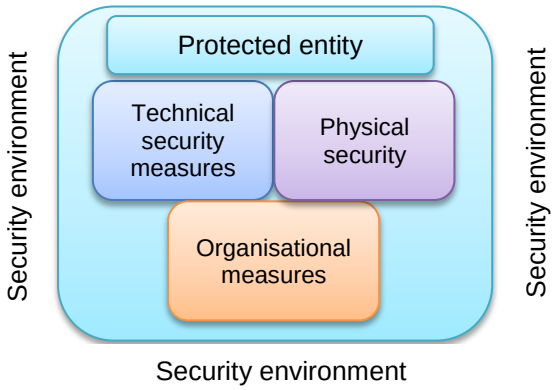

Fig. 1 Integrated security system (authors)

The quality of security by technical security measures can be determined by *burglar resistance.*

The burglar resistance is the time *Δt* to need for break through burglar resistant construction products. It is the time which the disturber needs for the breaking through the mechanical barriers. It is determined as

$$\Delta t = t_2 - t_1 \quad [\text{min}] \qquad (1)$$

where

Δt – Time needed for breaking the mechanical barriers,

t_1 – Time of the starting of breaking the mechanical barriers,

t_2 – Time of breaking the mechanical barriers.

Using mechanical barrier equipments it is determined the minimal value of burglar resistance of infillings and the secure storages units.

The calculation of infilling burglar resistance

It applies for the infillings (windows, doors, grilles etc.) that minimal time needed for breaking through is set by their resistance classes. If we multiply this time two or three time, obtain the real time for breaking through of specific infilling. Minimal time of breaking through of infillings is set in technical standard (e.g. the STN EN 1627 which set the requirements and classification of characteristics “Burglar resistance” Pedestrian doorsets, windows, curtain walling, grilles and shutters. (STN EN 1627, 2011)

Table 2. Technical standards setting the mechanical barriers

Mechanical barriers	***Number of standards***
Secure storage units, safes, strongroom doors and strongrooms	STN EN 1143-1
Windows, doors, shutters	STN P EN 1627
Cylinders for locks	STN EN 1303
Security glazing	ČSN EN 356

(authors according to technical standards)

In these standards there are defined e. g. coefficients of used tools, burglar resistance for specific burglar resistant construction products. For the calculation there are used resistance classes, the real time of burglar resistance (T_{vl}). As the example we can introduce the requirements for resistance classes of manual burglar attempts – infillings according to STN EN 1627. There are six resistance classes defined, their values are in table number 3.

Table 3. Resistance classes of infillings (STN EN 1627, 2011)

Resistance classes	Tools	Resistance time (min.)	Total time of the test (min.)
1	*Without manual burglar attempts*		
2	A	3	15
3	B	5	20
4	C	10	30
5	D	15	40
6	E	20	50

The calculation of infilling burglar resistance of secure storage units

By the secure storage units, the real time T_{vl} is determined by the calculation, it is necessary to characterise specific type of secure storage units, its classification in safety class (number of the resistance classes is determined by 0 ÷ XIII (STN EN 1143-1, 2012), the classification of used tools, using of coefficient burglar resistance and coefficient of testing time.

$$T_{vl} = [(V_R - BV) : C_1] \times (2\psi 3) \quad [\text{v min; RU; RU/min}] \qquad (2)$$

where

T_{vl} – real time of burglar resistance,
V_R – value of burglar resistance of secure storage units defined in resistance units (RU),
BV – basic valuation of tools, numerical values is defined in resistance units for each tool,
C_1 – coefficient of burglary resistant for secure storage unit,
$(2\ \psi 3)$ – coefficient of raising of test time,
RU – resistance units, burglary resistance, it sets as 1 minute long using of tool with the tool coefficient equal to one, with the basic valuation equal to 0.

According the real burglary time we can determine the *risk of object treatment. (so-called coefficient of risk)* **– R.**

$$R = \frac{T_{vl}}{t_z} > 1 \qquad (3)$$

where

R – risk of object treatment,
T_{vl} – real time of burglary resistance,
t_Z – time of intervention unit.

From the equation (3) is evident that the higher the coefficient R is, the real treatment of protected element will be smaller. Time of the intervention is individual and depends on various factors (e.g. the distance to the protected object, physical fitness, weather condition i.e.). From the statistics of the private security services and police forces is evident that the intervention time ranges from 2 to 20 minutes.

We will determine the calculation of infilling burglar of secure storage units for a strong-box with security class V, which according the tables has a burglar resistance V_R =220 RU. Breaking throw the secure storage units will be realised using two different tools in the same time. There are used electrical angle grinder of the power 750 W with diamond disk which has according the table BV_1 = 35 RU and oxygen cutting torch BV_2 = 28 RU. With the coefficient of burglary resistance of secure storage unit C_1 = 10 RU/min (resistance units/min) is the resistance time:

$$T_{vl} = [(V_R - BV) : C_1] \times (2\psi 3)$$

T_{vl} = [(220 – (35 + 28) : 10] x 2,75 = 5,7 min

Calculated time is obtained with the test of burglary resistance (in lab). The real time for breaking through of specific infilling is three time higher, that is 17,1 min. The time of intervention unit is t_Z = 5 min, according to (3) we can mathematically determine *a coefficient of the object risk*:

$$R = \frac{T_{vl}}{t_z} = 17{,}1 / 5 = 3{,}42$$

We can determine the real time of burglar resistance and the coefficient of risk for the other mechanical burglar resistant construction products. In real conditions of the mechanical burglar resistant construction products design

there is necessary to do it comply with the follow methods:

- to set all incoming routes into consideration that the offender can used to achieve that protected interest (from the perimeter, starting and ending internal environment),
- to calculate maximal time (T_{vlmax}) and minimal time (T_{vlmin}) of burglar resistance of used mechanical barriers for the security of protected interest,
- to set t_{zmax} (maximal time of intervention unit),
- to set total coefficient of object risks R according to supposed moving of offender, the road which had the minimal real time of burglar resistance and the maximal time of intervention unit

$$R = \frac{\mathbf{T}_{\mathbf{vl}\,\min}}{\mathbf{t}_{\mathbf{z}\,\max}}$$

- if $R \leq 1$ it is necessary to change the design of mechanical barrier (with the higher coefficient of resistance C_1).

For the determination of rout setting (the shorter according to T_{vlmin}) is good to use Dijkstra´s algorithm for the shortest path. (Mach, 2012)

For the design of technical security measures we must consider the fact that every mechanical barier is possible to breaking through. Every mechanical barrier varied according to breaking time T_{vl}, energy input a technical equipments B_v, according to these is set security resistance grade of objects R. By these parameters is defined the passive security, which is influenced by mechanical resistance and the quality of used materials. A similar procedure can also be applied to other types of protection, using mechanical barriers.

5 CONCLUSIONS AND DISCUSSION OF RESULTS

Authors of the paper refer to possibilities of the methods for the determination of obtainable or designed condition of burglary resistance of used components for interest entity protection. We assume that the determination of existing and designed condition of burglary resistance it would be a starting-point for judgement and design of mechanical barriers of perimeter, shell, spatial, or subject protection of critical infrastructure element (or its part). Object of the paper is the increment of quality for critical infrastructure element protection. Authors recommend examining the burglary resistance in design of technical measures. We suppose the increment of investment in these elements protection with previously mentioned step. The aim of this article was initiate a discussion about the importance of burglar resistance as a one of the key measurable values of resistance of protected assets.

Works Cited

Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení neskorších predpisov. (23. máj 2002).

Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike. (2007).

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre. (08. február 2011).

ČSN EN 356. (01. október 2000). ČSN EN 356 Sklo ve stavebnictví - Bezpečnostní zasklení - Zkoušení a klasifikace odolnosti proti ručně vedenému útoku.

Jasenovec, J., & Dvořák, Z. (2012). Metodika definovania kritickosti infraštruktúry. Civilná ochrana: revue pre civilnú ochranu obyvateľstva, 46-49.

Koncepcia. (2006). Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany.

Mach, V. (2012). Zisťovanie prielomovej odolnosti mechanických zábranných prostriedkov obvodovej a predmetovej ochrany. Security Revue, 12.

Smernica, R. (dátum neznámy). Smernica Rady 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

STN EN 1143-1. (01. september 2012). STN EN 1143-1 (93 7704) Bezpečnostné úschovné objekty. Požiadavky, klasifikácia a metódy skúšania odolnosti proti vlámaniu. Časť 1: Skriňové trezory pre peňažné automaty, trezorové dvere a komorové trezory.

STN EN 1303. (01. október 2005). STN EN 1303 (16 5191) Stavebné kovanie. Cylindrické vložky do zámok. Požiadavky a skúšobné metódy.

STN EN 1627. (01. december 2011). STN EN 1627 (74 6173) Dvere, okná, závesné steny, mreže a utávery. Odolnosť proti vlámaniu. Požiadavky triedenie.

Šimák, L. (2012). Ochrana kritickej infraštruktúry v sektore dopravy 1. vyd. Žilina: Žilinská univerzita.

Vidriková, D. (2012). Model bezpečnostného plánu na ochranu prvkov kritickej infraštruktúry. LOGVD 2012 Dopravná logistika a krízové situácie: Zborník 15. vedecko-odbornej konferencie s medzinárodnou účasťou (s. 211-215). Žilina 20.-21.september 2012: Žilina: Žilinská univerzita.

Vidriková, D., & Boc, K. (2013). Ochrana kritickej infraštruktúry I. časť. Žilina: Žilinská univerzita.

Received for publication: 11.04.2013
Revision received: 20.06.2013
Accepted for publication: 29.06.2013

How to cite this article?

Style – **APA** *Sixth Edition:*
Boc, K., Vidrikova, D., & Figuli, L. (2013, 07 15). Security plan as a part of critical infrastructure protection. (Z. Čekerevac, Ed.) *MEST Journal, 1*(2), 136-145. doi:10.12709/mest.01.01.02.13

Style – **Chicago** *Fifteenth Edition:*
Boc, Kamil, Dagmar Vidrikova, and Lucia Figuli. " Security plan as a part of critical infrastructure protection." Edited by Zoran Čekerevac. *MEST Journal* (MESTE) 1, no. 2 (07 2013): 136-145.

Style – **GOST** *Name Sort:*
Boc Kamil, Vidrikova Dagmar and Figuli Lucia Security plan as a part of critical infrastructure protection [Journal] = Security plan and critical infrastructure // MEST Journal / ed. Čekerevac Zoran. - Belgrade : MESTE, 07 15, 2013. - 2 : Vol. 1. - pp. 136-145. - ISSN 2334-7058 (Online); ISSN 2334-7171.

Style – **Harvard** *Anglia:*
Boc, K., Vidrikova, D. & Figuli, L., 2013. Security plan as a part of critical infrastructure protection. *MEST Journal,* 15 07, 1(2), pp. 136-145.

Style – **ISO 690** *Numerical Reference:*
Security plan as a part of critical infrastructure protection. **Boc, Kamil, Vidrikova, Dagmar and Figuli, Lucia.** [ed.] Zoran Čekerevac. 2, Belgrade : MESTE, 07 15, 2013, MEST Journal, Vol. 1, pp. 136-145. ISSN 2334-7058 (Online); ISSN 2334-7171.