

Ladislav Kittel – Tomas Lovecek *

PASSIVE PROTECTION ELEMENTS BREACH RESISTANCE MODELING

This article originated in response to requirement for creation of quantitative evaluation system of passive protection elements resistance, which could be implemented into complex process of technical effectiveness evaluation of property protection systems. It deals with design of model, which could be a basis for estimation of breach resistance time and which would use attributes of material of chosen homogeneous passive protection element – building construction. The article analyses possibilities of mathematical modeling of attack on homogeneous passive protection element on the basis of specifically chosen tool and attack method. The model used will simulate an attempt to overcome a wall made from single layer monolithic concrete panel using a hammer as chosen tool. For the purpose of attack modeling a model of contact force effect of direct central impact on passive protection element, while omitting the deformations on tool and the effect of deformation forces created by impact on the wall section will be studied. Subsequently the model will be applied to the breach resistance time assessment method based on the number of impacts required for overcoming of barrier.

1. Introduction

Property crime in the Slovak Republic has still the most numerous representation between individual crime types. The issue of protection of property from intentional human activities as: terrorist attacks, organized crime, sabotage, theft or vandalism, is covered by many legal acts, technical norms and professional publications. Neither of them approaches the property protection complexly and gives satisfying answer to question, how to design these systems optimally from the viewpoint of technical effectiveness and economic efficiency. Most of approaches to property protection are based on qualitative expert evaluations of designers or security managers, where the owner or property administrator has to fulfill minimal required amount of points set by corresponding law regulation while implementing the security measures or implement exact combination and specification of security measures. It is not possible to exactly prove technical effectiveness or economic efficiency of designed property protection system.

In the USA, software tools were developed to protect nuclear facilities, making use of qualitative-quantitative methods evaluating the existing or proposed system for property protection. These tools are based on certain measurable values. No similar tool for resolving effectiveness of protection systems using exact methods based on the probability theory and mathematical statistics has been developed in the EU so far. However, application of these tools has several disadvantages – they were developed for protection of specific materials and non-commercial facilities and were not intended to protect items of critical infrastructure with different

modes of operation. There has been no principal modifications done to these tools since their development, as can be seen from criticism of their authors and users (see [7], for an early discussion of this). It is impossible to evaluate level of protection in multi-level buildings and to evaluate level of protection in linear structures (such as a railway track, oil pipeline, electricity distribution system). And these tools do not consider European technical standards, standards and certifications applied in the field of property protection, making them unusable in EU conditions (e.g. safety classes or passive protection component resistance classes). [4]

It is possible to achieve safety of property as desired state by the means of technically effective and economically efficient security system. By security system we understand optimal combination of mechanical means of protection (passive protection elements), alarm systems (active protection elements), organizational and regime measures and physical protection for the purpose of this article. The objective of effective protection system of object is to prevent the violator to achieve his goal. Safety of object can be then characterized as a condition in which the access to protected interest is secured so the presence of violator during the attempt to overcome the protection system detected by alarm system and subsequently the violator will be detained by physical protection before reaching his goal. Object protection system effectivity can be assessed by multiple methods. Since we are interested in stopping the violator by physical protection before he reaches the protected interest, we will assess effectiveness of protection system by comparison of time necessary for overcoming the system by violator and time necessary for physical protection intervention. There-

* Ladislav Kittel, Tomas Lovecek

Department of Security Management, Faculty of Special Engineering, University of Zilina, Slovakia, E-mail: Ladislav.Kittel@fsi.uniza.sk

fore it is vital to specify time needed for overcoming individual passive protection elements, which can be very complicated in particular cases (e.g. the building construction).

2. Passive protection elements

Passive protection elements create a system of physical barriers, whose primary purpose is to influence the violator so he gives up on his intention. If he does not give up, then the purpose is to create sufficient time delay between the moment the attack begins and the moment violator reaches his goal, i.e. to impede or practically make the violator's penetration to the protected interest impossible [5].

Passive protection elements can be classified from different viewpoints - by their position in security system and protected area (e.g. passive elements of perimeter, shell, room and item protection), by breach resistance (e.g. sorting into security classes), by type (e.g. building construction, opening fillings, locks etc.). One of viewpoints that have not been yet elaborated is classification of passive protection elements into homogeneous - those composed of homogeneous components (e.g. building constructions) - and inhomogeneous - those composed of inhomogeneous components (e.g. opening fillings such as windows, door etc.). Homogeneous passive protection elements can not be bypassed by non-destructive methods, so we can focus on destructive means of their bypassing in specifying their breach resistance.

3. Tools used for bypassing passive protection elements

For the purpose of this article the term tools for bypassing passive protection elements will be understood as items used by violator to enable the bypassing of passive protection element or facilitate it. The term tool in this article encompasses either normal tools, improvised ones, weapons and ammunition, vehicles and explosives. The disadvantage of such approach is wide range which makes the creation of complete database of tools impossible. It is possible to narrow this range in two ways:

- creation of integrated standard set of tools, which would reflect the preferences and abilities of chosen group of potential violators (e.g. use of only improvised tools by random violator),
- classification of tools by the method of their use in process of bypassing the passive protection element and selection of one tool for each such group as standard or average representative of the group of tools.

The violator can use both destructive and non-destructive methods to bypass the passive protection elements. It usually depends on the violator which tool he chooses. For destructive methods, the passive protection elements breach time depends not only on structural design of passive protection element, but also from the set of tools used for its bypassing and ability of passive protection element to resist the attack. His choice can be influenced by multiple factors:

- characteristics of passive protection element material,

- power and consumption of tool,
- skill necessary for tool operation,
- possible sources of electricity,
- construction material,
- concealability, noisiness and mobility,
- availability, anonymity/registration of owner,
- unambiguous identification of tool in case of use (partial, full),
- standby time.

4. Breach resistance of passive protection elements

Currently no breach resistance times of passive protection elements are defined complexly for all categories of tools. For instance, the norm for opening fillings [7] does not define breach times corresponding to appropriate resistance classes for all tools, but only for some of them. For example, the breach resistance time defined by the norm for resistance class 3 is 20 minutes, but only for defined set of tools (screwdriver, wedge, crowbar), which makes it difficult to assess how the opening filling would resist more aggressive type of tool. Breach times for specific tools are then identical with values of breach times corresponding to specific resistance class according to the norm [7]. Breach time is working time during manual break-in test, including times shorter than 5 seconds for exchange of tools (e.g. exchange of screwdriver for crowbar).

The norm intended for security depositories [9] is more elaborate. In it the breach resistance time of appropriate security class depends on tool expected to be used and so it is possible to calculate it for all tool categories. Breach times are equal to sum of operational time periods expressed in time units (minutes), defined for security depositories in [9]. The sum of operational times $\sum t$ depends on value of breach resistance Vr in resistance units RU (unit of resistance against break-in, which results from one minute use of tool with tool coefficient value equal to 1 and with base value equal to 0) and sum of all base values of every used tool ($\sum BV$) in resistance units too. [9]. In case of security films and security glass the norms do not mention time units, but only quantity of impacts by different tools which the specific passive element should resist [10], [11], [12]. No technical norm defines breach resistance of building constructions, which belong to passive elements of shell protection, and all passive elements of perimeter protection. National security authority of the Slovak Republic processed a classification of most used building constructions, where individual building constructions were divided into four basic groups by degree of confidentiality [13]. There is innumerable amount of passive elements of perimeter, shell and item protection and also there are several approaches to their assessment. Due to this normative disharmony it is not possible to determine breach resistances of all passive protection elements available on the market in relation to specific type of tool used. This disharmony is caused mostly by the fact that there are several technical committees which deal with development of technical norms for passive protection elements (e.g. CEN/TC 33, CEN/TC 370, CEN/TC 129, CEN/TC 263) in international (e.g. ISO) or European (CEN) organization/committee for normalization and simultaneously there are representatives of producers in these committees so they may lobby for their own benefits.

From given facts results that it impossible to determine breach resistance expressed in time units for most of passive protection elements, but it is only possible to verify/certify conformity of attributes for these elements. It is possible to state that security class 3 door made in the Slovak Republic have the same or similar attributes as the door of same class made in Germany, but it is not possible to say, what time the door will be able to resist an attack by an aggressive cutting thermal tool, for example. By certification of passive protection elements we mean the activity that verifies conformity of attributes with appropriate security standard/norm. In order to allow the customer to orientate between wide spectrum of passive and active protection elements available on the market and compare them qualitatively, there exist specific certification symbols of authorized subjects [2]. An example of such certification symbols is the mark "SECURITY TESTED" from Revimont-DG, s.r.o. or „SECURITY PYRAMID“, which was introduced by the Czech association of insurance companies for purpose of insurance contracts. Similar certification symbols of authorized subjects are issued across Europe (e.g. VdS Schadenverhütung GmbH - Germany, SKG - Stichting Kwaliteit Gevelbouw - Netherlands). But that does not change the fact that for most of passive protection elements it is only possible to determine qualitative difference from other passive elements and not directly breach resistance expressed in time units.

The same applies for known practices across the world. Usual method for breach resistance time determination are expert estimations and even use of minimal breach time from the norms that deal with certification of passive protection elements. Currently there are no methods for exact calculation of breach resistance time used in practice.

5. Methods of passive protection elements bypassing

Passive protection elements breach resistance should represent the time it takes to bypass a chosen passive protection element. But breach resistance does not depend only on attributes of material the passive protection element is made of, but also on tools used for bypassing. Passive protection element can be for example made of hard material that resists the mechanical stress well, but it may be in the same instance particularly vulnerable to thermal cutting. So it would be useful to determine breach resistance for each tool, but that is practically impossible given the amount of existing tools. But it is possible to determine attributes that affect process of protection element bypassing and subsequently sort tools into groups by attributes that affect breach resistance time most significantly.

As stated before, the methods for bypassing security system elements can be divided into destructive and non-destructive. The bypassing of protection element with use of destructive methods is based on damaging or destruction of part or whole protection element, or creation of opening which will allow the bypassing. After successful bypassing with use of destructive methods the protection element is no longer able to fulfill its original function until repair or replacement. Non-destructive methods include bypassing with use of deceit, stealth, evasion by utilization of insufficiently secured

elements of system (e.g. climbing over/digging under the fence) and other methods. The basic characteristic is that these methods need not damage the protection element and it can be still be rendered usable without other costs.

For purpose of this article we will deal only with destructive methods of bypassing. Destructive methods can be further classified by attributes of passive protection element and tool that most significantly affect breach time. Proposed classification of destructive methods of bypassing is as follows:

- contact force effect of impact,
- dynamic application of force,
- utilization of machine tools,
- utilization of explosives,
- thermal cutting,
- combined use of multiple methods.

For each of these methods there can be defined specific attribute of passive protection element material that limits effectivity of chosen method. These attributes can be mechanical (e.g. tensile strength, spatial rigidity, elasticity) or physical (e.g. melt temperature). It is also possible to define specific attribute of tool that limits its effectiveness (e.g. force of impact, power, rpm, torque).

The example given in this article deals with modeling of contact force effect of impact of hammer on a monolithic wall made of concrete.

6. Contact force effect of impact model

Contact force effect of impact covers wide range of tools, both improvised and intended for this method of use. So it is necessary to propose the model in such way, it will allow for calculation of breach resistance time with few basic attributes. These attributes should be common for all tools.

It is possible to utilize tools driven both by power of human muscle (e.g. impact by hammer, axe, ram etc.) and driven by other sources of energy (e.g. pneumatic hammer, impact by vehicle, impact by bullet etc.) to breach the passive element by contact force of impact. It is necessary to design the model with possible application for both types of tools.

Effects of contact force impact can be studied through Newton's elementary impact theory, which takes course of force during time into account. During contact of two moving bodies, it is possible to observe significant change of their speeds. This phenomenon is called impact of bodies. Accompanying event during the impact are deformations of bodies induced by effect of impact force. The impact force of two colliding bodies has two components - normal and tangential component. Shear and pressure stress forms during impact. [3]

The model used for calculation of penetration depth of tool into passive protection element described in this article is based on constant spatial rigidity and it can be used for estimation of

protection element resistance. General attributes of tool and passive protection element are defined by geometric shape and coefficient of rigidity.

For calculation of penetration depth we shall assume in this model that the tool is made of infinitely rigid material in comparison to material of protection element and so the deformations of tool can be omitted. Tangential force will be omitted too so we will deal with the deformation as during direct central impact without change of motion state and neglect the restitution of material after impact.

Rigidity is measured by rigidity coefficient S , which is defined as ratio of force applied on construction and its deformations. Rigidity is affected by bulk modulus E , geometric characteristics of cross-section A and also length dimensions of stressed cross-section l . [1]

Coefficient of rigidity can be calculated as in equation 6.1

$$S = \frac{E \cdot A}{l} \quad [\text{Nm}^{-1}] \quad (6.1)$$

Bulk modulus E for class B20 concrete is equal to value of 277 000 MPa. [14]

Geometric characteristics of cross-section A are equal to dimensions of affected area squared, which in our case means the width of section hit by hammer squared. Length dimensions are characterized by wall thickness.

Penetration depth can be calculated as in equation 6.2.

$$\lambda = \frac{F}{S} \quad [\text{m}] \quad (6.2)$$

where λ stands for penetration depth [m], F stands for contact normal force [N] and S stands for protection element rigidity coefficient [Nm^{-1}]. [3]

By substituting we can obtain equation 6.3 for penetration depth of tool into passive protection element for one impact.

$$\lambda = \frac{F \cdot l}{E \cdot A} \quad [\text{m}] \quad (6.3)$$

For total number of impacts necessary for creation of breach opening with needed dimensions we have to calculate circumference of such opening and determine total number of impacts needed. For this example we will assume the violator needs to create opening with dimensions of 400×250 mm as stated in norm [8].

The model described does not provide us directly with breach resistance time. It provides us with an answer to the question: "How many single operations (impacts) will the violator need to create breach opening of specified dimensions?" So we need to determine the time needed for one operation. One possible way to do this is to use standardization of operations, which lies in determining time needed for one operation by means of expert estimations or experiments.

For purpose of this article we assume that it takes precisely one second for single impact.

7. Example of contact forces effect of impact model application

For the breach resistance time calculation example we decided to simulate bypassing of 100 mm thick monolithic wall of class B20 concrete, whose bulk modulus E equals to 277 GPa. The tool chosen by the violator for bypassing is in this case a hammer used for security glass breach resistance testing.

The hammer head is made of steel block with a square cross-cut 40 mm wide and 232 mm long weighing 2 kg. The impact edge has a diameter smaller than 1 mm. The impact speed must be 12.5 m/s, so the hammer causes the impulse force of $F = 2500$ N for duration of impact equal to 0.01 seconds. [11]

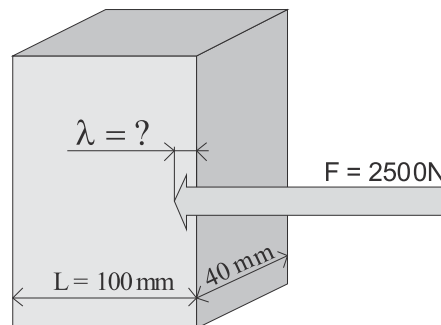


Fig. 1: Example of contact forces effect of impact model application scheme

Equation 6.3 shows us the formula for calculation of penetration depth of tool into protection element. After substitution of values we get the result $\lambda = 0.564$ mm (7.1).

$$\lambda = \frac{2500 \text{ N} \cdot 0.1 \text{ m}}{2.77 \cdot 10^8 \text{ Pa} \cdot 0.04^2} = 5,64 \cdot 10^{-4} \text{ m} = 0.564 \text{ mm} \quad (7.1)$$

This means that the penetration depth of one impact will be 0.564 mm. From this we can easily calculate that for breach of one opening in the chosen wall 178 impacts with hammer will be necessary.

Breach opening circumference is 1300 mm and width of impact area is 40 mm. With this in mind we can state that to create opening of set dimensions 5785 impacts will be necessary, which means that with specified time for one operation the total time of breach resistance will be $T_{pr} = 5785$ s.

Based on this calculation the estimated breach resistance time of a 100 mm thick wall of class B20 concrete will be 96 minutes and 25 seconds.

8. Disadvantages of model, possible improvements and alternatives

This model is considerably simplified, which can have negative impact on its precision. This can be improved by more exact standardization of operations (e.g. implementing the violator's fatigue, needed pauses in work etc.), more precise determination of individual variables (e.g. experimental determination of impact force of chosen tools and application of findings into calculation) and finally application of eccentric impact, tool skid and material restitution after impact.

The disadvantage of this model is necessity of an impact force estimation, which is lowering the precision of model mainly for muscle powered tools. If we take into account all factors affecting assumed strength of the violator and practically infinite amount of their combination, we will find out that it is not possible to exactly determine impact force and so it is necessary to simplify the method of impact force determination. This is possible by determination of average impact force based on examination of statistic data obtained through experiments or by classifying the potential violators into groups by their assumed physical attributes and determining a typical representative for each given group and his attributes.

There are several alternatives to breach resistance of passive protection elements determination. One of these is already mentioned standardization of operations, which can be based on empiric assessment, experimental research or their combination. Experimental research would be very demanding both on time and sources. However, empiric assessment does not allow determining exact time of breach resistance. Their combination – experimental research of breach resistance time for one passive protection element in group and utilization of this element as gauge with subsequent deduction of breach resistances for other elements based on coefficients determined by expert estimations – allows us to obtain approximate breach resistance times for specific group of elements (e.g. for walls) from one series of experiment with rela-

tively low costs and based on real breach resistance time. Such approach is possible even without experimental research – utilizing expert estimations of several experts could increase precision of breach resistance time approximation. Another possible way is utilization of norms for demolitions.

9. Conclusion

It is possible to somewhat apply methods proposed in this article into quantitative system of security system effectivity evaluation, but it is necessary to develop these methods with newly acquired knowledge and to review possible applications in practice. It is also necessary to consider possible application of alternative methods of breach resistance time approximation. Subsequently a method should be created for estimation of time of passive protection system bypassing by non-destructive methods and implemented into complex system of security system effectiveness evaluation.

Calculations used in contact forces effect of impact model are estimations of protection elements resistance and are, at this time, too inaccurate to be fully applied into practice. Future research should concentrate on precise determination of individual variables, maybe even experimental determination of impact force of chosen tools, more exact standardization of operations and eccentric impact, tool skid and material restitution after impact should be implemented for increased accuracy. The results should be then proved by experimental methods.

If improved to be more accurate, the model could be used for calculation of breach resistance time, which could be implemented into process of security system evaluation and design.

This work has been supported by the scientific grant agency VEGA, grant No. VEGA 1/0640/10 “Modeling of Property Protection Systems and Evaluation of Efficiency and Effectiveness”.

References

- [1] CILLIK, L., ZARNAY, M.: *Methodology of Constructing*, University of Zilina : EDIS ZU, 2002, ISBN 80-7100-934-2.
- [2] KALUZA, F.: *Certification of Mechanical Protection Systems and Technical Protection Systems in Legislative National Environment*, Proc. of Intern. conference Perspective security technologies for property protection, Brno, 2008, ISBN 978-80-7318-699-9.
- [3] KASANICKY, G. et al.: *Theory of Motion and Impact in Analysis and Simulation of Accident Events*, University of Zilina, 2001. ISBN 80-7100-597-5.
- [4] LOVECEK, T. – RISTVEJ, J. – SIMAK, L: Critical Infrastructure Protection Systems Effectiveness Evaluation. In: *J. of Homeland Security and Emergency Management*. ISSN 1547-7355. – Vol. 7, no. 1 (2010), art. no. 34, [24] s.
- [5] MACH, V.: *Contribution to Possible Unification of Security Classes of Mechanical Protection Means*, In: Topical questions of current and perspective development of private security: Scientific conference, University of Zilina, 2010
- [6] MELCER, J., KUCHAROVA, D.: *Dynamics of Building Constructions: Examples*, University of Zilina, Faculty of Civil Engineering, 2004. ISBN 80-8070-326-4
- [7] Phillips, G. et al., *New Vulnerability Assessment Technologies vs the Old VA Tools*, 2005, National Security Program Office Y-12, TN USA, Accessed on 10 November 2008, Available at: <http://www.projectenhancement.com/new.pdf>.
- [8] REITSPIS, J., KORMANCOVA, G.: Implementation Principles of the Project Management by a Security Systems Design. In: *Communications, Scientific Letters of the University of Zilina*, 2008. ISSN 1335-4205

- [9] STN P ENV 1627 (74 6173) Windows, door, shutters. Burglary resistance. Requirements and classification.
- [10] STN P ENV 1630 (74 6176) Windows, door, shutters. Burglary resistance. Test method for determining resistance of manual attempts for breaking-in.
- [11] STN EN 1143-1 (93 7704) Security depositories. Requirements, classification, test methods of resistance against burglary. Part 1: Safes, safes for cash machines, safe door and strong-rooms.
- [12] STN EN 356 (70 0595) Glass in buildings. Security glazing. Testing and classification of resistance against manual attack.
- [13] STN EN 13541 (70 1616) Glass in building. Security glazing. Testing and classification of resistance against explosion pressure.
- [14] STN EN 1063 (70 0594) Sklo v stavebníctve. Bezpečnostné zasklenie. Skúšanie a klasifikácia odolnosti proti strelám.
- [15] Construction Materials of walls, partition walls and ceiling [on-line]. National security authority of Slovak Republic. [cited 5.1.2008]. available at: <http://www.nbusr.sk/sk/oblasti-bezpecnosti/objektova-a-fyzicka-bezpecnost/dokumentacia/index.html>
- [16] Constructions Made of Concrete - Design of Concrete Constructions [on-line]. Civil engineering. [cited 7.1.2010]. available at: <http://pozemni-stavitelstvi.wz.cz/bek32.php>.
- [17] VELAS, A.: *Insurance for security managers*, EDIS - University of Zilina, 2009, ISBN 978-80-554-0149-2.