Article citation info:
VALIS D, PIETRUCHA-URBANIK K. Utilization of diffusion processes and fuzzy logic for vulnerability assessment. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2014; 16 (1): 48–55.

David VALIS
Katarzyna PIETRUCHA-URBANIK

UTILIZATION OF DIFFUSION PROCESSES AND FUZZY LOGIC FOR VULNERABILITY ASSESSMENT

WYKORZYSTANIE PROCESÓW DYFUZYJNYCH I LOGIKI ROZMYTEJ DO OCENY PODATNOŚCI NA ZAGROŻENIE*

Assessing the vulnerability of critical infrastructure objects is of major concern when dealing with the process of dependability and risk management. Special attention is paid to the objects of higher interest, such as nuclear power plants. In spite of the protection of these objects, there is still a certain level of a potential threat. The aim of the paper is to describe a possible way of attacking on the object in order to get into a particular part of it. Several characteristics of an adversary´s attempt were obtained. For this reason as well as for modelling adversary´s behaviour diffusion processes have been used.

***Keywords**: vulnerability, critical infrastructure, diffusion processes.*

Ocena podatności na zagrożenie kluczowych obiektów infrastruktury jest głównym problemem rozpatrywanym w kontekście procesu niezawodności oraz zarządzania ryzykiem. Szczególną uwagę przywiązuje się do obiektów wysokiej rangi, takich jak elektrownie jądrowe. Pomimo ochrony tych obiektów, nadal istnieje pewien poziom potencjalnego ich zagrożenia. Celem artykułu jest opisanie możliwego sposobu zaatakowania obiektu z zamiarem dostania się do konkretnej jego części. Otrzymano kilka charakterystyk próby ataku ze strony przeciwnika. Do tego celu, jak również do zamodelowania zachowania przeciwnika, wykorzystano procesy dyfuzyjne.

***Słowa kluczowe**: podatność na zagrożenie, kluczowa infrastruktura, procesy dyfuzyjne.*

1. Introduction – motivation

Modern history is rich with examples of various terrorist attacks against structures, transportation systems, etc. worldwide. In the aftermath of the September 11th tragedies, the vulnerability of the whole infrastructure to terrorist attack has gained national attention. In light of this vulnerability, various governmental agencies are looking into ways to improve the design of structures to better withstand extreme loadings. Tens of per cent of the homeland security outlays are devoted by countries to making potential targets less vulnerable to potential terrorist attacks. This is to protect what we usually call "Critical Infrastructure", "Key Asset" and/or "Key Resources". The objective of this article is to assess the behaviour of a potential adversary whose intention is either to damage the object/system, or steal nuclear material. Since the behaviour of an adversary is highly unpredictable (at least at the beginning) and the result is rather uncertain (although we expect he needs to reach the goal), the way of describing his behaviour will be tackled in more detail. The process of breaking into the building is continuous in time. However, its development is dynamic and changeable, and, as we have mentioned before, the result is quite indeterminate [2, 23, 24, 32, 37, 38, 42]. But the adversary makes an effort to achieve the goal to a certain time. A proper tool used for assessing such process might be the diffusion Wiener process which was applied several times also in technical area see e.g. [1, 3, 4, 6, 7, 8, 9, 13, 25, 26 etc.]. In this case we presume that the attack time is a random variable.

System vulnerability is described in several ways and indicates many characteristics of system condition. The vulnerability term and its meaning are more developed in section 2. However, the main idea of the paper is to describe selected aspects of observed system vulnerability. We assume the vulnerability is compounded both from probability of successfully completed attack and from conditional consequences of this attack when completed successfully.

Therefore the paper describes expected adversarys behaviour in the secured area. The principles presented in the paper are subdivided into two parts.

Modelling the FPT (First Passage Time) using specific diffusion process – which is represented by the adversary's respective trajectory length and time to reach the goal. When an adversary is detected at the same time the security unit is alerted and gets into motion. We model here just the probability that the attacker will reach the goal – this is modelled by time elapsed or/and distance competed.

Modelling the consequences after successful attack is completed. Fuzzy approach seems to be suitable as the whole process includes humans. Therefore we assume the level of uncertainty is quite high plus consequences modelling are vague and conditional. Therefore the fuzzy logic seems to be appropriate.

The paper introduces the possibility of applying the Wiener process while modelling an expected movement trajectory (distance from a beginning – both time and physical distance). Provided an adversary really breaks into the building, the results of the work might serve to model not critical, but presumed path of adversary movement. In view of the stochastic way of the process, we have taken into consideration factors relating to time, morphology, area, shape and nature of an agglomeration, including adversary skills.

From the experience the terrorist attacks are unpredictable for two main reasons [22]:

Terrorists have many more categories of legitimate targets, as well as worldwide scope, compared to traditional security concerns (which

(*) Tekst artykułu w polskiej wersji językowej dostępny w elektronicznym wydaniu kwartalnika na stronie ***www.ein.org.pl***

used to have the comparable luxury of protecting obvious military assets, or home territory).

Terrorist attack can have different objectives like harming people, damaging infrastructure, causing panic, etc.

Although such objectives may often overlap, these varying objectives lead to varying types or location targets. However, we have to keep in mind that detection and prevention must always remain to be the first line of defence [39, 40].

In our case it is always about an attempt to damage the building, or steal interesting (e.g. nuclear) material. Several experiments have been performed very recently in this area and all models presented below are based on real data. Unfortunately the data are classified and quite sensitive. Before presenting the results here data were de-sensitised and the results correspond with the reality in modified way.

Outcomes of this paper might be used for adjustment of physical protection systems in secured area. We have proved in this particular case that the reaction time of security unit is acceptable in terms of adversary's behaviour when attempting to reach the goal. For other instances the outcomes of this paper might be of use and inspirational when setting up the physical protection system.

2. Vulnerability and different ways of its assessment

We would like to turn our attention to some selected information sources since there are many of them and many options how to describe vulnerability. Department of Homeland Security (DHS) in the USA defines vulnerability as "physical feature or operational attribute that renders an entity, asset, system, network, or geographical area to exploitation or susceptible to a given hazard" (2010) [12]. The key of assessing vulnerability properly is in the last phrase of that definition. Although vulnerability assessments can be standalone documents, vulnerability is best understood within a risk context, specifically the interaction between the threat and the consequence. This interaction is the reason that vulnerability V is sometimes defined as the probability of success (of an attack) P_S given an attack A or probability of the consequence occurring given an event. Mathematical expression is then:

$$V = P_S(\mathrm{A}) \tag{1}$$

In either case vulnerability is the collective influence of physical features or operations that reduce the effectiveness (alternatively success) of the adversary's attack or that make the target better able to sustain the attack. Analysis is highly dependent, therefore, on the method of attack and strength of the attack expected. A building's vulnerability to an improvised explosive device (IED) will differ from the vulnerability to a vehicle-born IED (VBIED), for example, depending on the assumption in the definition of those attacks, such as amount or type of explosives, entry points, and stand-off distance. Even within the category of VBIED, vulnerability will differ based on terrorist tactics, such as leaving the vehicle on the street adjacent to the building or ramming the vehicle into a building or its defensive perimeter. The more specific the context, the more accurate the vulnerability assessment for particular target can be [41, 43].

For security risk, vulnerability is also influenced by the terrorist adversary. Terrorist groups have different levels of competence and expertise. This can affect not only target selection, but also their knowledge of countermeasures and their determination to overcome those countermeasures through technology or effort. For this reason we have to accept kind of conceptual approach to vulnerability assessment of structures as mentioned for instance in [12]:

1. Characteristics of the asset itself.
2. The protective measures that prevent the attack.
3. Access allowed to outsiders and insiders.
4. The functional dependencies on internal and external entries.
5. Generating scenarios.
6. Attack methods filtering.
7. Event/fault tree analysis (recognisability, countermeasures effectiveness, robustness/resistance).
8. Combining the components.

If we speak about vulnerability, we cannot forget to emphasise also the structural robustness. It might be expressed by "Protection categories" as said in [43], "Robustness Index" as mentioned in [14] and has several degrees on scale – usually 1-10. Some retrofit recommendations for increasing the structure robustness are for instance listed in [11]. Considering the further statements in [14], there are three most important structural properties which increase a structure's/building's ability to survive catastrophic overload or damage:

- Structural redundancy (A structure that will perform well in catastrophic situation will permit gravity loads that must be supported during the event to be carried to the foundations using multiple load paths).
- Fireproofing toughness (A structure's ability to resist fire is an important contribution to its robustness, since fire is often a part of a catastrophic event).
- Connection robustness (Structural connections are very important and are critical in holding a building together during the large movements that occur in a fire or another catastrophic event).

There are several ways of assessing the severity of a possible terrorist attack. Many of them are based on conventional standards like [e.g. 15, 17, 19, 21, 31]. In [29] there are also mentioned some possible tools for risk assessment either software-based (e.g. RAMPART – Risk Assessment Method-Property Analysis and Ranking Tool; CONTAMW – software for vulnerability assessment; HVAC – software for heating, ventilation, and air condition in buildings assessment) or classical (standards and books).

Referring to the application of mathematical tools applied and to the materials presented above, the vulnerability is associated with the probability the adversary achieves the goal plus consequences from such act – meaning successful goal approach. Both of these components might be modelled differently.

3. Diffusion processes and attacks on the objects of critical infrastructure

Diffusion processes are part of mathematics in the area of stochastic processes [such as 6, 7, 8, 9, 13, 25, 26, 27, 34, 35, 36]. Generally, the Brownian motion ranks among the simplest stochastic processes with continuous time. In fact it is understood as a limit process for both simpler and more complex types of stochastic processes. Due to normal distribution of random variable and its application capabilities, the Brown motion might be used universally. The application of the Brown motion can be found in many areas. Among others we suppose it can be also used when assessing the vulnerability of critical infrastructure objects. Standard use is related to modelling with the use of differential equations. We pick up one specific example of diffusion processes which is Wiener process.

Rules of the general Wiener process might be specified as follows:

A real stochastic process $\{W(t)\ t\in\langle 0; +\infty)\}$ in a probability space (Ω, A, P) is called *the Brown motion* or the *Wiener process*, if the following applies:

1. $W(0) = 0$ almost everywhere,
2. $W(t) - W(s)$ has $N(0, t - s)$ distribution for $t > s \geq 0$,
3. For arbitrary $0 < t_1 < t_2 < \cdots < t_n$ growths $W(t_1), W(t_2) - W(t_1), W(t_3) - W(t_2), \ldots, W(t_n) - W(t_n - 1)$ are mutually independent random variables. $W(t)$ is in fact a physical movement trajectory of an adversary in a building – it can represent the travelled distance or time – in a very specific manner.

Next, it applies that

1. $E[W(t)] = 0$ for $t > 0$
2. $E[W_2(t)] = t$ *for* $t > 0$

The Wiener process represents one possible form of diffusion processes. It is actually the integral of what is in practical applications called a white noise. The Wiener process with drift will be used in our application.

In view of simplified and generally hypothetical theoretical adversary's behaviour and the nature of diffusion processes the Wiener process – meaning Brownian motion without drift – model might be shown e.g. in the graph below – figure 1, where "mu" is mean value and "sigma" is standard deviation. This process in practice however is not much likely.

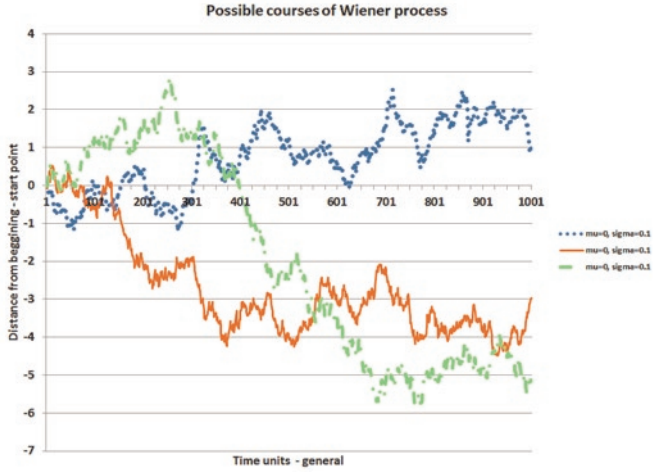

Fig. 1. Graphical model of general Wiener process

The attacker may use basically two principles/ways for reaching the goal – either brutal force or smart strategy as presented in figure 2. We assume a weighted stochastic proportional combination of both will apply while the equipment of the attacker is always the same. The weight of proportion for both brutal force and strategy is based on empirical experience. These input boundary conditions are to be justified at the beginning of the process. It is assumed that the time of passing obstacles (Level of Protection – LOP) will be the same when having the same equipment. The next assumption is that the likelihood of adversary detection at single LOPs will be also the same, or may equal to 0.

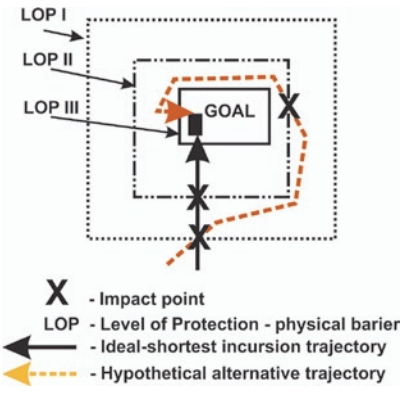

Fig. 2. Possible way of incursion of an adversary into a building

First Passage Time (FPT) – meaning the moment when attacker reaches the goal or some front layers of protection (LOP) – is presented in figure 3. This is just generalised way of the attacker's approach to the understanding the mean values of passage as they are linear for us. Real data were recorded while performing live experiments.

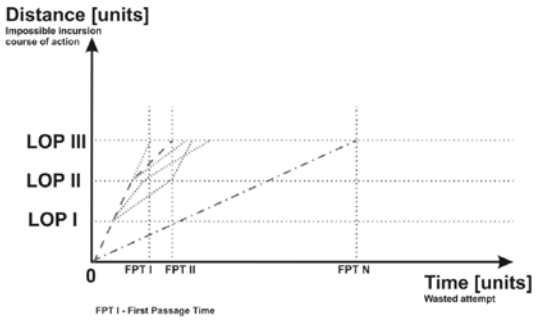

Fig. 3. Possible way of incursion into a building by an adversary

4. Example of a possible adversary's attack on an object of interest

The adversary's incursion into a building might be crippled by time and distance limits. The adversary wants to achieve his goal as soon as possible (it does not always mean the shortest way and fastest motion and neither that the goal could not be achieved more quickly). His main effort is to complete his mission (as fast/smoothly as possible) and if possible not to be detected due to security systems during his incursion. If he were detected, he could try to abandon his plan, or could keep achieving the objective. However, according to Wiener process assumptions, adversary's movement in the area of concern is expected in any way but always consist of combination of brutal force and smart strategy. FPT (First Passage Time) is the moment when the adversary achieves his final goal. While the way forward might have two typical boundary conditions 1. „the sooner the better" or 2. „Rome was not built in a day…". Let's assume that both previously mentioned strategies have their actual and effective limits.

The experimental data were used as inputs to above mentioned Wiener process. These data were collected for individual attackers therefore the linear course of a mean time of the goal approach was calculated using linear regression and including confidence interval for an individual attempt. The experiments were performed on various surfaces. Generalised and publically accessible outcomes are shown in figure 4. This figure has been constructed based on many consulta-

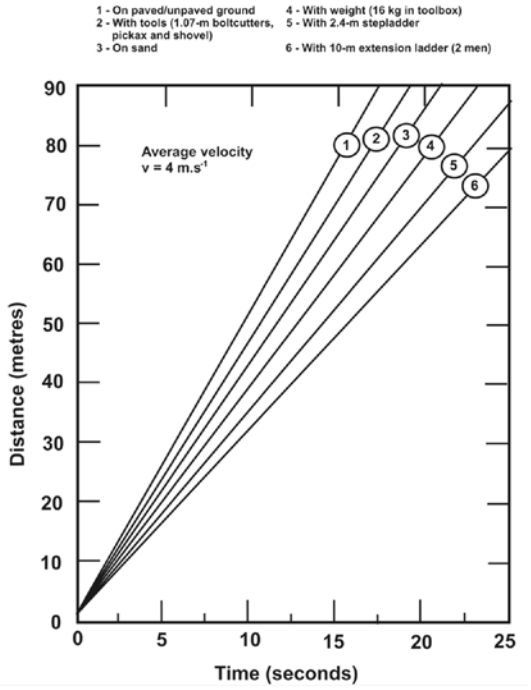

Fig. 4. Basic regression parameters as inputs to Wiener process

tions with experts in this area, based on searching several literature sources and based on personal experience of the authors. It may have similar origin in other publications. Detailed analytical results from tests can unfortunately not be presented in open form but were available and used for further modelling and simulation process.

Graphical representation of de-sensitised characteristics is mentioned in figure 5 bellow. Confidence level is 95%. The positive shift on y-axis means that in time "0" – when detected on some LOP – the attacker has already managed to reach some trajectory.

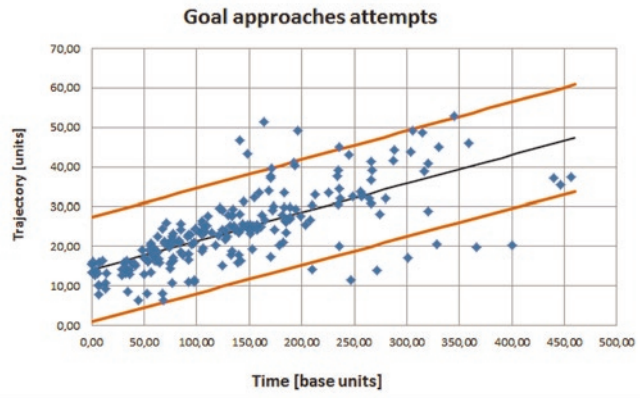

Fig. 5. Basic regression parameters as inputs to Wiener process

For our particular practical application we use a Wiener process with positive drift where mu is higher than 0. Which means the adversary is approaching the intended final goal. The principle of such approach is presented by function in equation (2):

$$f(x) = \frac{W(t) \cdot \sigma}{\sqrt{t}} + \mu \qquad (2)$$

where W(t) – is standard randomly generated Wiener process depending on time of attempt, σ is standard deviation for individual value calculated for each time increment, μ is calculated mean value of an attacker's trajectory increment in time (t).

There are two possibilities when an adversary behaves inside the area. As previously said we always assume positive drift which means the attacker will approach the final goal. Negative drift means that the attacker will never reach the goal and will be caught and pacified by action of security service. First of this options is modelled, simulated and presented in figure 6 while the second one in figure 7. The Wiener process simulation courses were performed 10e6 times which are assumed to be almost near the reality.

On "y – axis" there is line in value number 50 (always the modified value). Where the value actually means the critical length of the estimated physical/ideal/air-line or ground plot trajectory needed to reach the goal successfully. The other threshold both in figure 6 and 7 (on x-axis 260) means in our case experimentally recorded first time point where security unit comes to the scene and act. The adversary's behaviour behind this point will be modelled using probability distribution with expected goodness-of-fit.

Let us presume the way of breaking an adversary into a building could be demonstrated by the Wiener process with positive drift as presented above. We assume that the random variable – the time trajectory parameter – has either Gamma Distribution, Inverse Gaussian Distribution or LogNormal Distribution.

The FPT distribution was modelled based on the real test data and above mentioned principles. The outcome in form of boundary conditions and FPT probability distribution is presented in figure 8. Where full line presents Gamma Distribution, dash line presents LogNorm

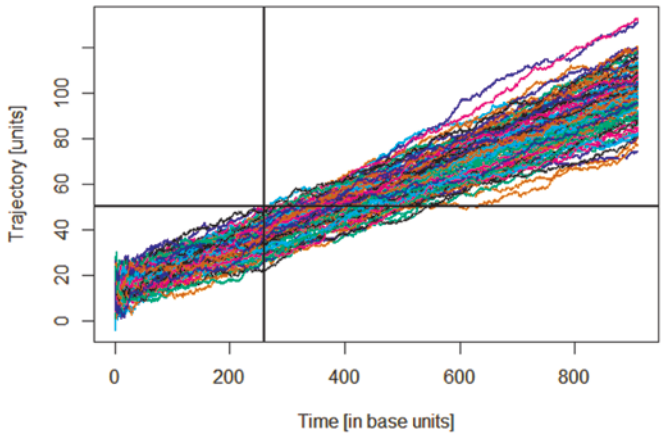

Fig. 6. Model of attacker behaviour when reaching the goal in positive attempt

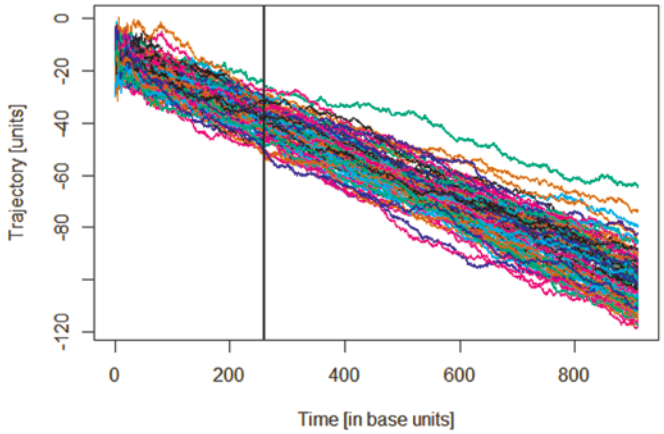

Fig. 7. Model of attacker behaviour when reaching the goal but with negative attempt

Distribution and dash and dot line presents the Inverse Gaussian Distribution (IGD).

Basic characteristics of the FHT histogram are: Min Value: 134.00 [Time units]; 1st Qu: 336,40 [Time units]; Median: 377.70 [Time units]; Mean Value: 382.00 [Time units]; 3rd Qu: 422.80 [Time units]; Maximum Value: 886.60 [Time units]; 2.5%: 265.05 [Time units]; 97.5%: 523.65 [Time units]; Variance: 4333.44 [Time units]; Standard Deviation: 65.62887 [Time units].

The Kolmogorov-Smirnoff tests for goodness-of-fit were performed at the same time in R-Studio for foreseen types of distri-

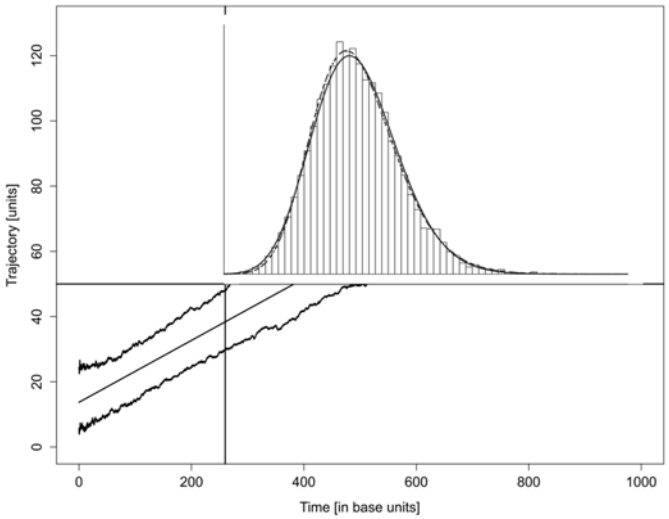

Fig. 8. FHT model of an adversary when reaching the goal

butions. The outcomes showed and confirmed our expectations. The "p-value" for LogNorm Distribution was 0.7453, for IGD was 0.3957 and for Gamma 0.2733. So in terms of FPT distribution we can more likely rely on the Log Norm distribution in this case. The Comparisons of probability density functions with empirical cumulative distribution function (Ecdf) for IGD and LogNorm Distribution is presented in figure 9 where LogNorm (left) is green and IGD (right) is red.

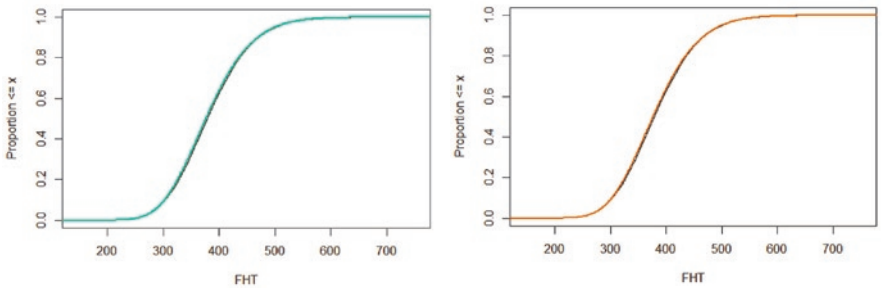

Fig. 9. Comparison of cdf of LogNorm (left) and of IGD (right) with Ecdf

Based on these outcomes we can see that an adversary's attempt will be most likely not successful if the security unit reacts by 260 [Time units]. Everything behind this time point onwards may create potential for an adversary's success when reaching the goal.

It would be very useful – based on an attacker position, target location and distance of both an attacker to the target and the security unit to the attacker – utilization of multidimensional Brownian motion for this whole procedure assessment.

Therefore we have also to assess next situation when the attacker's success can generate variable consequences. The level of uncertainty and vagueness in terms of effects assessment is quite high since human element is present. Therefore classical risk approach combined with fuzzy approach is presented further to assess the level of consequent risk.

5. Proposal of risk assessment of an adversary's attack

Risk assessment is a key phase of the system safety management process and shall introduce some risk reduction activities [see e.g. 18, 19, 20, 33]. Safety and protection of the system performance plus critical infrastructure objects is associated with the relation to hazard analysis – especially an event frequency, case of and event occurrence, identification of an event causes and reducing negative effects of an event occurrence.

The following method of risk assessment is proposed while estimating the risk of nuclear power plant fault. The discussed risk assessment is associated with an adversary's attack. We consider the probability of reaching and destruction a goal/target (e.g. generator, first circle, and reactor) (P), consequences of reaching and destruction the target (C), and the possible threat detection (D). The idea for this approach was inspired by principles of addressing the risk priority number (RPN) – as we consider as total risk level [see e.g. 15]:

$$RPN = R = P \times C \times D \tag{3}$$

For every situation we have assessed a score which is assigned to the parameters P, C and D. Total risk number may vary in the range of [1÷75].

Probability (P) estimates that a particular system target (e.g. generator, first circle, and reactor) will be chosen by an adversary's for attack, and then it might be reached in respective time based on his intent and capability as described in previous section.

Point weights associated with P – probability of choice a target – are based on common expert estimates and are as follows:

- remote; it would be very unlikely to be observed, $P < 10^{-6}$ 1/year; point scale 1,
- moderate; likely to occur more than once, $10^{-6} < P < 10^{-3}$ 1/year; point scale 2,
- very high; near certain to occur several times, $P < 10^{-3}$ 1/year; point scale 3.

The values for C, D parameters can be obtained as follows:

The criteria for evaluating the threat consequences:

- minor: point scale 1; performance of system is affected with minor effect,
- low: point scale 2; system performance is affected with small effect; the maintenance may not be needed; renewal costs will be up to 10e3 EUR,
- moderate: point scale 3; performance of system is affected seriously and the maintenance is needed, renewal costs will be up to 10e5 EUR,
- high: point scale 4; operation of system is broken down without compromising safe, renewal costs will be up to 10e7 EUR,
- very high: point scale 5; highest consequences ranking of a failure mode, hazardous consequences, renewal costs will exceed 10e9 EUR.

Consequences (C) can be divided into the following groups in the case of a nuclear power plant might be chosen for terrorist attack:

- economic and financial (energy network disorganization of the country or region, the need to repair the damage and launch control systems, the removal of radioactive contamination, the need of the population evacuation from the contaminated sites, the impact on the local economy and the national capital losses),
- environmental (associated with environmental pollution),
- health (birth defects caused by radiation, increased mortality, illness absences and medical expenses),
- social, governance and the psychological (impact on the ability to maintain order and to deliver minimum services by the state),
- other (legal, cost of land interdiction and litigation, payment of compensation adjudicated).

Basically all consequences might be also expressed in monetary values. However the criteria of the consequences assessing suggested in this work should be based on the information from entrepreneurs of the nuclear power plant and can be derived from incident data.

Point weights associated with D are as follows:

- point scale 1: almost certain likelihood that the potential of occurring such failure mode will be detected,
- point scale 2: high likelihood of detecting the potential of occurring such failure mode,
- point scale 3: moderate likelihood of detecting the potential of occurring such failure mode,
- point scale 4: remote likelihood of detecting the potential of occurring such failure mode,
- point scale 5: absolute uncertain likelihood that the process controls will not detect a potential adversary's attack and subsequent failure mode.

It is needed to apply specific approach as all these components – P; D; C – are of various natures in terms of their assessment and description. Therefore subsequent fuzzy sets scaling is applied. Such approach with fuzzy logic implementation would be useful when we deal with incomplete, imprecise, unclear data.

The final step is to define the risk level and to determine limits of its fragmental levels: tolerable (further reduce if practicable), [1÷9]; undesirable (risk reduction as much and promptly as possible),

Table 1. Three-parametric risk matrix

Detection (D)	Consequences (C)														
	Minor			Low			Moderate			High			Very high		
	Probability (P)														
	Unlikely	Moderate	High	Unlikely	Moderate	High	Unlikely	Moderate	High	Unlikely	Moderate	High	Unlikely	Moderate	High
Almost certain possibility	(1) T	(2) T	(3) T	(2) T	(4) T	(6) T	(3) T	(6) T	(9) T	(4) T	(8) T	(12) UN	(5) T	(10) UD	(15) UD
High possibility	(2) T	(4) T	(6) T	(4) T	(8) T	(12) UD	(6) T	(12) UD	(18) UD	(8) T	(16) UD	(24) UD	(10) UD	(20) UD	(30) UA
Moderate possibility	(3) T	(6) T	(9) T	(6) T	(12) UD	(18) UD	(9) T	(18) UD	(27) UD	(12) UD	(24) UD	(36) UA	(15) UD	(30) UA	(45) UA
Low possibility	(4) T	(9) T	(12) UD	(9) T	(16) UD	(24) UD	(12) UD	(24) UD	(36) UA	(16) UD	(32) UA	(48) UA	(20) UD	(40) UA	(60) UA
Absolute uncertain possibility	(5) T	(12) UD	(15) UD	(12) UD	(20) UD	(30) UD	(15) UD	(30) UA	(45) UA	(20) UD	(40) UA	(60) UA	(25) UA	(50) UA	(75) UA

where: T– tolerable risk, UD – undesirable risk; UA – unacceptable risk

[10÷27]; unacceptable (immediate action required), [30÷75]. In table 1 there are presented the three-parameter risk matrix.

The calculated risk can be presented in form of fuzzy risk priority numbers which are shown on figure 10 and for membership function F_T, F_{UD}, F_{UA} can be determined by the formulas 4–6. On the *x*-axis there is the Total Risk Number following the principles above.

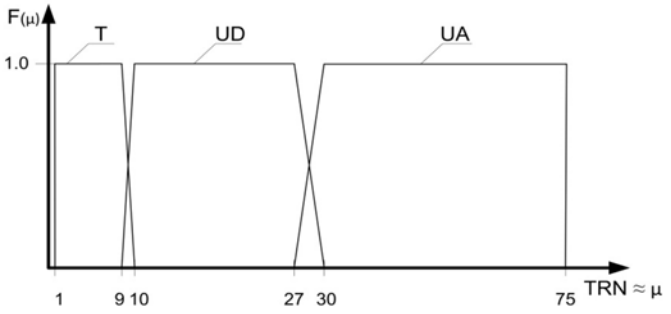

Fig. 10. Membership function of risk

$$F_T(\mu)=\left\{0\ for\ TRN\in\left(-\infty;1>@1\ for\ TRN\in<1;9>@\frac{TRN-10}{9-10}\ for\ TRN\in<9;10>@0\ for\ TRN\in<10;\infty\right)\right.$$

$$F_{UD}(\mu)=\left\{0\ for\ TRN\in\left(-\infty;9>@\frac{TRN-9}{10-9}\ for\ TRN\in<9;10>@1\ for\ TRN\in<10;27>@\frac{TRN-30}{30-27}\ for\ TRN\in<27;30>@0\ for\ TRN\in<30;\infty\right)\right.$$

$$F_{UA}(\mu)=\left\{0\ for\ TRN\in\left(-\infty;27>@\frac{TRN-27}{30-27}\ for\ TRN\in<27;30>@1\ for\ TRN\in<30;75>@0\ for\ TRN\in<75;\infty\right)\right.$$

The fuzzy approach has been used as initial idea description, proposal and determination of possible risk resulting from adversary's attack. This field is just open and not completed yet. Deeper studies on this issue will continue.

6. Discussion

Following the suggested way of using the Wiener process, some adversary's behavioural patterns can be modelled. As stated above and assumed before the Wiener process parameters shall be in special form – namely the drift. Mainly, we are not going to focus on a critical trajectory – ideal for achieving the goal. We are going to concentrate on adversary's possible movement between single layers of protection. These layers are the same in terms of detection probability and the time necessary for overcoming them. The result of the solution is the time of the first achievement of the goal. This result is compared with an ideal time of detection – the sum of times from the detection to the reaction of protections systems. If the result is for a potential intruder more beneficial, then it will be necessary to take measures.

Next, we follow the assumption that we know all weak points of a protected building. However, we suppose a potential adversary does not know them and we do not know his attack plan. Therefore the adversary's movement between protection layers could be stochastic, although he is motivated by not being detected at all and by achieving his goal as soon as possible. The reasons for his stochastic behaviour have been stated above. This model does not take into consideration different levels of difficulty when overcoming obstacles on an adversary's trajectory. It is rather obvious

and not unambiguous that different wall fillings in a building (or potential paths to the building) have effect on the speed of the advance. This situation could affect the Wiener process development for this application. Therefore we have not included the difficulties of overcoming obstacles this time.

This approach can very well fit while modelling an attacker's movement for low risk targets as well as higher level risks. On these assumptions – based on our practical experiences and real examples – the fuzzy model was created.

7. Conclusion

This paper is to bring one of possible alternatives for using diffusion processes in technical applications. Because the attack on the objects of interest is a fact, we are made to look for adequate ways of expressing such processes. The presumed movement of an adversary and his behaviour in time is believed to be diffusion stochastic processes. Admittedly we do not know where exactly the attack will take place, but we could be able to predict how it might develop, how long it might take and how successful it could be. Using all these characteristics, the vulnerability of critical infrastructure objects can be described directly and indirectly. It is widely supposed that the Wiener processes are going to be used in this area in much greater extent.

For further development we expect combining of two-dimensional diffusion stochastic processes. One motion of the trajectory will represent attacker's behaviour while the other one – at the same time – will represent the RFT (Response Force Time). It is expected that while combining these two processes together it will be possible to obtain precise picture of the physical protection system efficiency and facility vulnerability.

***Acknowledgement**: This paper has been prepared with the great support of the project for the institutional development of K-202 University of Defence, Brno and by the Ministry of Interior of the Czech Republic (project "The Evaluation of Physical Protection System Effectiveness Based on its Modelling ", No. VG20112015040).*

Bibliography

1. Bibbona E, Panfilo G, Tavella P. The Ornstein-Uhlenbeck process as a model of a low pass filtered white noise. Metrologia 2008; 45: 117–126. doi:10.1088/0026-1394/45/6/S17.
2. Blais RA, Henry MD, Lilley SR, Pan JA, Grimes M, Haimes YY. Risk-based methodology for assessing and managing the severity of a terrorist attack. 2009 IEEE Systems and Information Engineering Design Symposium, SIEDS '09, art. no. 5166175: 171–176.
3. Bohner M, Peterson A. Dynamic Equations on Time Scales: An Introduction with Applications. Boston: Birkhäuser, 2001.
4. Bohner M, Sanyal S. The Stochastic Dynamic Exponential and Geometric Brownian Motion on Isolated Time Scale. Community Mathematical Anals 2010; 8: 120–135.
5. Coffey WT, Kalmykov YP, Waldron JT. The Langevin Equation. With Application in Physics, Chemistry and Electrical Engineering, World Scientific Series in Contemporary Chemical Physics, World Scientific, Singapore 1996; 10: 428.
6. Csörgö M. Random Walk and Brownian Local Times in Wiener Sheets. Periodica Mathematica Hungarica 2010; 61: 1–21.
7. Desmond AF, Chapman GR. Modelling Task Completion Data with Inverse Gaussian Mixtures. Applied Statistics 1993; 4(42): 603–613.
8. Doksum KA, Hóyland A. Models for Variable-Stress Accelerated Life Testing Experiments Based on Wiener Processes and the Inverse Gaussian Distribution. Technometrics 1992; 1(34): 74–82.
9. Doob JL. The Brownian movement and stochastic equations. Annals of Mathematics, 1942; 43: 351–369.
10. ECSS (European Cooperation for Space Standardization)-Q-ST-40-02C Space product assurance – Hazard analysis.
11. Eytan R. Cost effective retrofit of structures against the effects of terrorist attacks – the Israeli experience. Proceedings of the Structures Congress and Exposition 2005; 2161–2172.
12. French GS, Gootzit D. Defining and assessing vulnerability of infrastructure to terrorist attack, Vulnerability, Uncertainty, and Risk: Analysis, Modelling, and Management. Proceedings of the ICVRAM 2011 and ISUMA 2011 Conferences 2011; 782–789.
13. Grow D, Sanyal S. Brownian Motion Indexed by a Time Scale. Stochastic Analysis and Applications 2011; 29: 457–472.
14. Iding RH. A methodology to evaluate robustness in steel buildings – Surviving extreme fires or terrorist attack using a robustness index, Proceedings of the Structures Congress and Exposition 2005; 511–515.
15. IEC 60812:2006 Ed. 2.0 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).
16. IEC 61508-(1-7)/:2008 Ed. 2.0 Functional Safety of Electrical/ Electronic/ Programmable Electronic safety-Related Systems.
17. ISO 13824:2009 Ed. 1.0 – General principles on risk assessment of systems involving structures.
18. ISO 31 000:2009 Ed.1.0 – Risk management – Principles and guidelines on implementation.
19. ISO/IEC 31010:2009 Ed. 1.0 – Risk Management – Risk Assessment Techniques.
20. ISO/IEC Guide 73:2009 Ed. 2.0 – Risk management – Vocabulary – Guidelines for use in standards.
21. JCSS (Joint Committee on Structural Safety) – Principles, System Representation & Risk Criteria 2008.
22. Jordán F. Predicting target selection by terrorists: A network analysis of the 2005 London underground attacks. International Journal of Critical Infrastructures 2008; 4(1–2), 206–214.
23. Kelly TJ, Hofacre K C, Derringer T L, Riggs K B, Koglin E N. Testing of safe buildings detection technologies and other homeland security technologies in EPA's Environmental Technology Verification (ETV) program, Proceedings of the Air and Waste Management Association's Annual Meeting and Exhibition 2004; 3449–3457.
24. Kemp RL. Assessing the vulnerability of buildings, Journal of Applied Fire Science 2007; 14 (1): 53–61.
25. Kolárová E. Stochastic differential equations in electro-technic. Dissertation thesis. Brno: VUT, 2005.
26. Kolárová E. The Brownian Bridge Process. In XXVII International Colloquium, Brno, 2009.
27. Lefebre M, Perotto S. A semi-Markov Process with Inverse Gaussian Distribution as Sojourn Time. Applied Mathematical Modelling 2011; 35: 4603–4610.
28. Linden M. Modelling Strike Duration Distribution: a Controlled Wiener Process Approach. Applied Stochastic Models in Bussiness and Industry 2000; 16: 35–45.
29. Marshall HE, Chapman RE, Leng CJ. Risk mitigation plan for optimizing protection of constructed facilities. Cost Engineering 2004; 46(8): 26–33.

30. Merritt D, Berczik P, Laun F. Brownian motion of black holes in dense nuclei. The Astronomical Journal 2007; 2(133): 553–563, doi:10.1086/510294.
31. MIL-STD-882D Standard Practice for System Safety.
32. Mueller J. Assessing Measures Designed to Protect the Homeland, Policy Studies Journal 2010; 1(38): 1–21.
33. Pietrucha-Urbanik K, Studziński A. Analysis of water pipe breakage in Krosno, Poland. Environmental Engineering IV, Pawłowski A., Dudzińska MR, Pawłowski L. (eds), London: Taylor & Francis Group, 2013, 59–62.
34. Promislow D, Young V. Minimizing the Probability of Ruin when Claims Follow Brownian Motion with Drift. North America Actuarial Journal 2005; 9: 109–128.
35. Sherif YS. and Smith ML. First-Passage Time Distribution of Brownian Motion as a Reliability Model. IEEE Transaction on Reliability 1980; 5(R-29): 425–426.
36. Smith ChE, Lánský P. A reliability application of a mixture of inverse Gaussian distributions. Applied Stochastic Models and Data Analysis 1994; (10) 61–69.
37. Stewart MG. Cost effectiveness of risk mitigation strategies for protection of buildings against terrorist attack. Journal of Performance of Constructed Facilities 2008; 2(22): 115–120.
38. Stewart MG. Life-safety risks and optimisation of protective measures against terrorist threats to infrastructure. Structure and Infrastructure Engineering 2011; 6(7): 431–440.
39. Valis D, Koucky M, Zak L. On approaches for non-direct determination of system deterioration. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2012; 14(1): 33–41.
40. Valis D, Vintr Z, Koucky M. Contribution to highly reliable items' reliability assessment. Reliability, Risk and Safety: Theory and Applications, Proceedings of the European Safety and Reliability Conference, ESREL 2009, Prague, Czech Republic, 2010; 1–3: 1321–1326.
41. Valis D, Vintr Z, Malach J. Selected aspects of physical structures vulnerability – state-of-the-art. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2012; 14(3): 189–194.
42. Williamson EB, Winget DG, Risk management and design of critical bridges for terrorist attacks. Journal of Bridge Engineering 2005; 10 (1): 96–106.
43. Zehrt Jr WH, Acosta PF. Analysis and design of structures to withstand terrorist attack, Proceedings of the Structures Congress and Exposition 2003; 585–592.

David VALIS
Faculty of Military Technologies
University of Defence
Kounicova 65, 662 10 Brno, Czech Republic
E-mail: david.valis@unob.cz

Katarzyna PIETRUCHA-URBANIK
Faculty of Civil and Environmental Engineering
Rzeszów University of Technology
Al. Powstańców Warszawy 6, 35-959 Rzeszów, Poland
E-mail: kpiet@prz.edu.pl