CHEMICAL ENGINEERING TRANSACTIONS
VOL. 32, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Chief Editors: Sauro Pierucci, Jiří J. Klemeš

ISBN 978-88-95608-23-5; **ISSN** 1974-9791
DOI: 10.3303/CET1332046

Contribution to Diffusion Processes Utilization for Vulnerability Assessment

David Valis

University of Defence, Kounicova 65, 662 10 Brno, Czech Republic,
david.valis@unob.cz

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 e.g. 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 potential model of a possible way of attacking on the object in order to get into a particular part of it. For this reason as well as for modelling adversary´s behaviour the diffusion processes have been used. The intention is to explain how and when the goal can be achieved by an adversary. The results are assumed to be possibly used for setting the efficiency of an object physical protection system, or the algorithm development of the way a possible adversary selects the goal.

1. Introduction

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 continual in time. However, its development is dynamic and changeable, and, as we have mentioned before, the result is quite indeterminate. But the adversary makes an effort to achieve the goal to a certain time. (Bibbona et al. 2008 use the general diffusion Wiener process which was further developed for dynamic processes by Bohner et al., 2010. Doksum et al, 1992 present application of diffusion process in accelerated testing while e.g. Liang et al. 2011 for insurance principles. Therefore I assume Wiener process application is also quite sufficient here. In this case we presume that the attack time has, as a random variable, the inverse Gaussian distribution.
The paper describes adversary´s behaviour in the secured area, but it does not include physical protection systems. 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 – in our case it will be omitted, or will equal 0. 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.
Terrorist attacks are unpredictable for two main reasons (Mueller, 2010):

Please cite this article as: Valis D., 2013, Contribution to diffusion processes utilization for vulnerability assessment, Chemical Engineering Transactions, 32, 271-276 DOI: 10.3303/CET1332046

- Terrorists have many more categories of legitimate targets, as well as worldwide scope, compared to traditional security concerns (which 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 (French et al, 2011).
In our case it is always about an attempt to damage the building, or steal interesting (e.g. nuclear) material.

2. Vulnerability and selected ways of its assessment

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) (Blais et al, 2009). 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) PS given an attack A or probability of the consequence occurring given an event. Mathematical expression is then:

$$V = PS(A) \tag{1}$$

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.
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 work by Eytan (2005):

- Characteristics of the asset itself;
- The protective measures that prevent the attack;
- Access allowed to outsiders and insiders;
- The functional dependencies on internal and external entries;
- Generating scenarios
- Attack methods filtering
- Event/fault tree analysis (recognisability, countermeasures effectiveness, robustness/resistance)
- 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 e.g. in Stewart (2011), "Robustness Index" as mentioned in Zehrt (2003) or Stuziński et al. (2012) and has several degrees on scale – usually 1-10. Some retrofit recommendations for increasing the structure robustness are for instance listed in Stewart (2011) and Rak et al. (2008). Considering the further statements in Jordán (2008), 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. Principles for risk severity is presented e.g. in ISO 31000 while general safety severity assessment is either in MIL-STD-882D and for failures severity e.g. in IEC 60812 and function loss consequences in IEC 61882. In Eytan (2005) 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 our mathematical tool, the vulnerability is associated with the probability the adversary achieves the goal. We do not take into consideration the likelihood of disclosure – disturbance and subsequent detection.

3. Diffusion processes and possible attacks on potential object

Sherif et al. 1980 promoted diffusion processes as part of mathematics in the area of stochastic processes while Smith et al., 1994 used diffusion processes for technical application. Generally, the Brown movement 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.
Rules of the Wiener process might be specified as follows:
A real stochastic process $\{W(t)\ t\in\langle 0;+\infty)\}$ in a probability area (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 the integral of what is in practical applications called a white noise.
In view of adversary´s behaviour and the nature of diffusion processes the Wiener process model might be shown in the graph below:

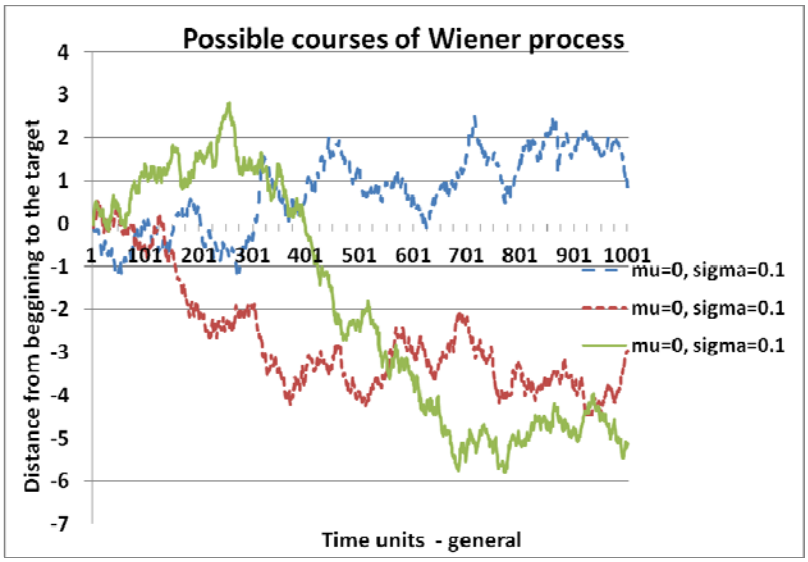

Figure 1: Graphical model of general Wiener process

Let us presume the simplified way of breaking an adversary into a building could be demonstrated by the Wiener process as put in Figures 1 and 2. We also assume that the random variable – the trajectory parameter – has the Inverse Gaussian Distribution.

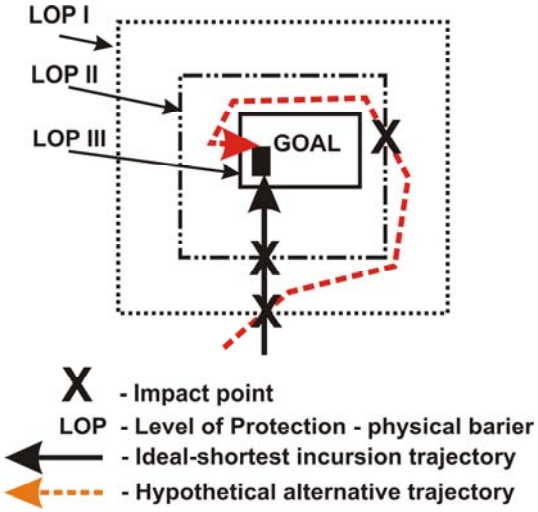

Figure 2: Possible way of incursion of an adversary into a building

As for the incursion of an adversary into a building, his effort might be crippled by time limits. The adversary wants to achieve his goal as soon as possible (it does not mean that the goal could not be achieved more quickly). His main effort is to complete mission (as fast/smoothly as possible) and not to be detected by 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. FPT (First Passage Time) is the moment when the adversary achieves his goal – it is not set and might be of different nature („the sooner the better" or „Rome was not built in a day…"). The behaviour of an adversary in view of overcoming single protection layers towards the goal is put in Figure 3.

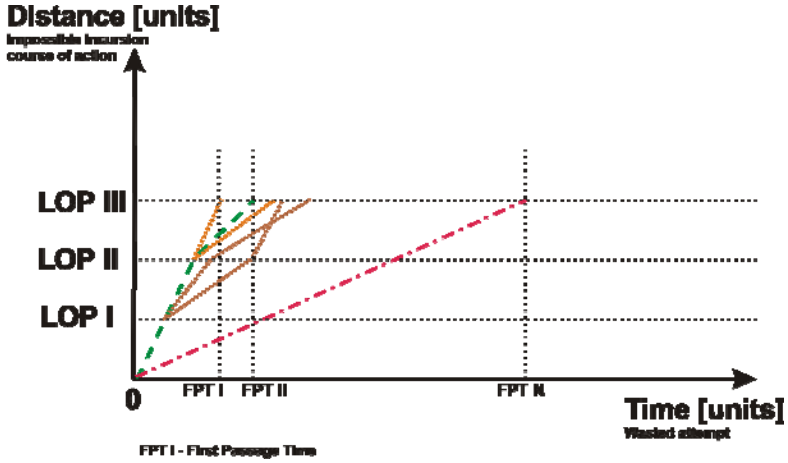

Figure 3: Possible way of incursion into a building by an adversary

Example of the solution of a possible adversary´s attack on an object of interest

On the basis of monitoring and testing a possible attack on an object of our interest we have found the following times of completing the attack successfully. The times are put in hours: 0.05; 0.36; 0.63; 1.02; 1.28; 1.55; 1.64; 1.92; 2.15; 3.42; 3.73. Let us presume these values are results of a Wiener process and it is a random variable with inverse Gauss distribution (IGD). The formulae (2) and (3) introduced below are used for parameters estimating using maximum likelihood method for μ and λ:

$$\hat{\mu} = \hat{X} = \frac{1}{n}\sum_{t=1}^{n} X_i \tag{2}$$

$$\hat{\lambda}^{-1} = \frac{1}{n-1}\sum_{1}^{i}\left(\frac{1}{X_i} - \frac{1}{\overline{X}}\right) \tag{3}$$

As we see all the values of the random variable are bigger than 0. The equation put below (4) will be used for determining the value of a probability density function IGD.

$$f(x;\mu,\lambda) = \left(\frac{\lambda}{2\pi x^3}\right)^{\frac{1}{2}} .\exp\left(-\frac{\lambda(x-\mu)^2}{2\mu^2 x}\right) \tag{4}$$

To estimate correlation between theoretical distribution and measured data, we have applied the standard Kolmogorov-Smirnov test. The resulting values are as follows:

$\hat{\mu} = \hat{X} = 1.614;\ \hat{\lambda}^{-1} = 2.211;\ \sigma^2 = 1.358$ and $\sigma = 1.165$.

The calculated critical value of the Kolmogorov-Smirnov statistics is 0.048, and a tabular value for 11 elements in the set and 5 % confidence level is 0.391. Following the results above it might be stated that the found attempt times and completed attacks really have IGD with a confidence level of 95 %. An assumed course of a pdf and CDF function for the estimation introduced above could be like this one in Figure 4.

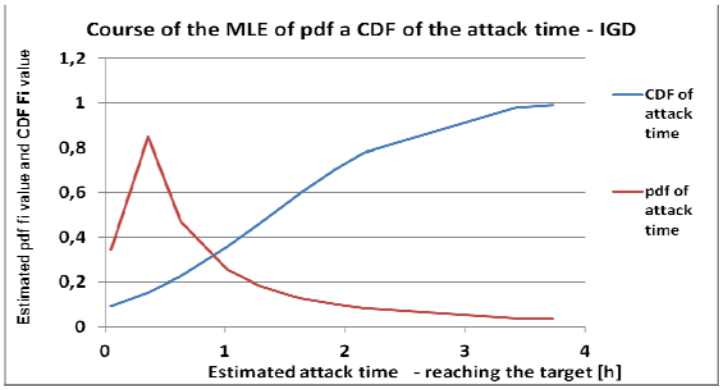

Figure 4: MLE of pdf and CDF of attack time

4. Discussion

Following the suggested way of using the Wiener process, some adversary´s behavioural patterns can be modelled. Mainly, we are not going to focus on a critical trajectory – ideal for achieving the goal. We are going to concentrate on his 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.

5. 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.

Acknowledgements

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).

References

Bibbona E. and Panfilo G. and Tavella P., 2008, The Ornstein-Uhlenbeck process as a model of a low pass filtered white noise. Metrologia, Vol. 45, 117-126. doi:10.1088/0026-1394/45/6/S17.

Blais R.A., Henry M.D., Lilley S.R., Pan J.A., Grimes M., Haimes Y.Y., 2009, Risk-based methodology for assessing and managing the severity of a terrorist attack, IEEE Systems and Information Engineering Design Symposium, SIEDS '09 , art. no. 5166175, 171-176.

Bohner M., Sanyal S., 2010, The Stochastic Dynamic Exponential and Geometric Brownian Motion on Isolated Time Scale. Community Mathematical Anals, 8, 120-135.

Doksum K. A., Hóyland A., 1992, Models for Variable-Stress Accelerated Life Testing Experiments Based on Wiener Processes and the Inverse Gaussian Distribution. Technometrics, 34(1), 74-82.

Eytan R., 2005, Cost effective retrofit of structures against the effects of terrorist attacks -the Israeli experience, Proceedings of the Structures Congress and Exposition , 2161-2172.

French G.S., Gootzit D., 2011, 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 , 782-789.

Jordán F., 2008, Predicting target selection by terrorists: A network analysis of the 2005 London underground attacks, International Journal of Critical Infrastructures 4(1-2), 206-214.

IEC 60812:2007 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), Geneva: IEC, available e.g. from http://webstore.iec.ch/?ref=menu

IEC 61882:2005 Hazard and operability studies (HAZOP studies) - Application guide, Geneva: IEC, available e.g. from http://webstore.iec.ch/?ref=menu .

ISO 31 000:2009 Ed.1.0 - Risk management — Principles and guidelines on implementation, ISO: Vienna, available e.g. from http://www.iso.org/iso/home/store.htm .

MIL-STD-882D Standard Practice for System Safety. US MoD: Washington, available e.g. from https://assist.daps.dla.mil/online/start/

Liang Z. and Yuen K. Ch. and Guo J., 2011, Optimal Proportional Reinsurance and Investment in Stock Market with Ornstein-Uhlenbeck Process. Insurance: Mathematics and Economics, Vol. 49, p. 207-215. ISSN: 0167-6687.

Mueller J.,2010, Assessing Measures Designed to Protect the Homeland, POLICY STUDIES JOURNAL 38(1), 1-21.

Rak J., Pietrucha-Urbanik K., 2008, Some factors of crisis management in water supply system. Environment Protection Engineering, 34(2), 57-65.

Sherif Y. S., Smith M.L., 1980, First-Passage Time Distribution of Brownian Motion as a Reliability Model. IEEE Transaction on Reliability, R-29(5), 425-426, ISSN 0018-9529.

Smith Ch. E., Lánský P., 1994, A reliability application of a mixture of inverse Gaussian distributions. Applied Stochastic Models and Data Analysis, 10, 61-69. ISSN 8755-0024.

Stewart M.G., 2011, Life-safety risks and optimisation of protective measures against terrorist threats to infrastructure, Structure and Infrastructure Engineering,7(6): 431-440.

Studziński A., Pietrucha-Urbanik K., 2012, Risk Indicators of Water Network Operation. Chemical Engineering Transactions, 26, 189-194. DOI: 10.3303/CET1226032.

Zehrt Jr. W.H., Acosta P.F., 2003, Analysis and design of structures to withstand terrorist attack, Proceedings of the Structures Congress and Exposition, Seattle, WA; United States; 29 May 2003 through 31 May 2003, 585-592.