Determination of the effectiveness of security measures for low probability but high consequence events: A comparison of multi-agent-simulation & process modelling by experts

Florian Brauner
Cologne University of Applied Sciences
florian.brauner@fh-koeln.de

Julia Maertens
Cologne University of Applied Sciences
julia.maertens@fh-koeln.de

Holger Bracker
Airbus Defence & Space
holger.bracker@cassidian.com

Ompe Aimé Mudimu
Cologne University of Applied Sciences
ompe_aime.mudmu@fh-koeln.de

Alex Lechleuthner
Cologne University of Applied Sciences
alex.lechleuthner@fh-koeln.de

ABSTRACT

Due to the increasing danger of terrorist attacks, it is necessary to determine the preventive effects of security measures installed in e.g. public transportation systems. Since, there is no common practice to determine the preventive effects; we developed two different methodologies to analyse those effects, both are suitable for the assessment of security measures. The first method is a semi-quantitative method based on expert-estimations combined with a modelled process of an attack.The second method models the scenarios using a multi-agent-based simulation framework. Simulating a large number of runs, it is possible to derive values for indicators of interest on statistical basis. We show the suitability of both methods by applying them on a practical example of a public transportation system. In this paper we introduce both methodologies, show an exemplary application and present the strengths and weaknesses and how they can be linked to get an increased benefit.

Keywords

Efficient Strategy Planning, Multi-Agent-Simulation, Modelling and Simulation, Prioritizing security measures, Decision Support, Scenario-based Risk Assessment Method

INTRODUCTION

Motivation: Terrorist attacks present a rising danger for the public. In order to cause considerable damage, extremely vulnerable places and infrastructures are targeted. A typical example is a crowded train station in a big city, i.e., a major transportation hub.

To reduce the risk of terrorist attacks, the current practice is to install security

measures (SeMe), either of a preventive nature (such as cameras or patrols, to mention conventional measures) or post-event measures to reduce the effects of an attack (such as walls). In this paper, we will focus on preventive measures.

In order to determine suitable implementations and configurations of SeMe, two prerequisites are required: an indicator to measure the effectiveness of security measures and a methodology to derive values for such an indicator in a reproducible, useful and scientifically sound manner.

However, existing common approaches have significant drawbacks when applied to the depicted scenario of a terrorist attack. In the project RiKoV, we developed and applied two complementary methodologies to overcome these drawbacks in estimating the effectiveness of security measures.

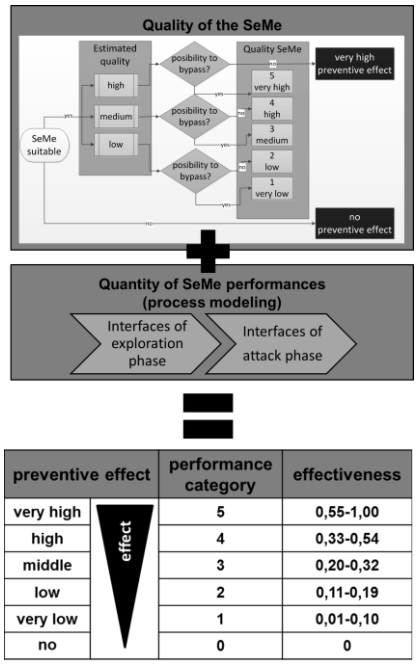
This paper is structured as follows: The first approach is based on an expert-based interview in combination with a process model described in the first section; the second approach is of empiric nature and relies on a multi-agent system, described in the second section. Using a fictive scenario introduced in the third section, the authors show the application of their approaches (fourth section) and discuss possible interfaces (fifth section).

RESEARCH APPROACH / METHODOLOGY

The goal of the ongoing project RiKoV is to develop new risk management approaches to assess anthropogenic events such as terrorist attacks in critical infrastructures. Such rare events, which cannot be defined with statistical probability values, require new approaches for risk assessment (Cox, 2008; Brauner, Baumgarten, Schmitz, Neubecker, Mudimu and Lechleuthner, 2013). One part of this study is the measurement of the effectiveness of security measures in context of preventing an attack in public transportation systems (pts). Currently, there is no methodology to measure the effectiveness of preventive security measures such as smart camera systems, personnel, metal detectors, body scanners, etc.

Neither quantitative values such as false alarm rates, detection time and coverage can be sufficiently described by manufacturers, nor the effectiveness of the measures in a specific scenario plus environment. In this article, we describe two different methodologies to estimate the needed effectiveness of such security measures. A validation cycle allows the comparison of the results as well as the integration of the results to optimize the estimation of the effectiveness.

A. Process modelling and expert interview (eMoE)



preventive effect	performance category	effectiveness
very high	5	0,55-1,00
high	4	0,33-0,54
middle	3	0,20-0,32
low	2	0,11-0,19
very low	1	0,01-0,10
no	0	0

effect

Figure 1. eMoE methodology

To identify the effectiveness of the installed security measures, the pts operator has to apply a two-step methodology at every station, which might be interesting for terrorist attacks.

First step - Quality of Effectiveness: The methodology consists of a structural questionnaire, which the operator has to follow: Firstly, the quality of every implemented security measure has to be determined. To ensure this, the preventive measures have to be suitable for the scenario and the considered station. In the next step, the operator has to estimate the quality of every suitable security measure into the categories (low, medium, high), expressed as Q_s. Security measures that do not have any effectiveness at all or are not suitable for the evaluated scenario, are dismissed. This will automatically lead to no preventive effect, or respectively, the performance category zero. If a security measure is estimated with a high quality, is suitable and cannot be bypassed, the preventive security effectiveness for this specific scenario is automatically set to very high, or respectively, the performance category five (see Figure 1). This procedure has to be executed for all SeMe. The overall quality and the possibility to bypass the security

measurement lead to a quality index Q_s. However, this index does not consider any quantitative data of effectiveness in the investigated environment. Therefore, we developed a process model that allows the pts operator to execute a process analysis of the attack mode in a second step.

Second step - Quantity of Effectiveness: Using a generic process model of an attacker and the scenario description, the operator can evaluate the preventive effectiveness of the chosen SeMe in consideration of the environment (e.g. station). This means the preventive SeMe has to physically detect the attacker and/or the weapon. Currently, there is no adequate methodology to support this estimation. We provide a generic process model based on the attack mode that analyses possible interfaces of SeMe effects. The process model of the terrorist's plan of attack consists of the exploration phase and the terroristic attack phase. According to the attack mode (e.g. immediate-/delayed initiation, direct or remote initiation), a six, eight or ten interface pathway has to be chosen. For each preventive SeMe, the interface of a physical detection I_s has to be determined, to gain the effectiveness eff_s. The quantity of positive interfaces I_s multiplied with the quality index Q_s is set in relation to the maximum level.

$$eff_s = \frac{Q_s * I_s}{Q_{max} * I_{max}} \quad (1.1)$$

The result is a decimal value that represents an expert-based eMoE (expert-based measurement of effectiveness) for every single SeMe. To determine a result for the combination of different preventive SeMe, we use an algorithm which is described in the following paragraph.

To determine the preventive effect of a combination of security measures we use an approach comparable with the calculation of stochastic independences. This algorithm ensures that the effectiveness of a combination of SeMe is equal or higher than the highest effectiveness of every implemented SeMe. To determine the effectiveness the decimal value $\mathrm{eff_s}$ is used to determine the index $\bar{S}_S$. It is calculated by using the following formula.

$$\bar{S}_s = 1 - \mathrm{eff_s} \quad (1.2)$$

The following formula is used to calculate the preventive effectiveness $\mathrm{eff_{total}}$ of the combination of security measures.

$$\mathrm{eff_{total}} = 1 - (\bar{S}_1 * \bar{S}_2 * \ldots * \bar{S}_n) \quad (1.3)$$

The calculated preventive effectiveness $\mathrm{eff_{total}}$ is converted into the related performance category according to a predefined scale (see Figure 1). In a last step, the effectiveness of the measurement package is evaluated with a question-based algorithm which includes the possibility that some SeMe influence each other in forms of reinforcing or degrading. According the estimation of the expert the calculated performance category can be revised.

B. Multi-Agent-Simulation (MAS)

Figure 2. Fictitious main train station

Multi-agent systems (MAS) are a well suited approach to model a scenario. The depicted scenario about a terrorist attack in a train station can be seen as a complex adaptive system. An appropriate method to model and simulate such complex adaptive systems is an agent based approach, which is realized in form of MAS. A general state-of the-art overview on MAS from a conceptual point of view is given in Weyns, Parunak, Michel, Holvoet and Ferber, 2004. With respect to existing MAS software frameworks, Fonseca, Griss and Letsinger (2002) give an overview on the most popular MAS frameworks. The MAS framework which is used in the context of this work is a proprietary framework called PAXSEM, developed by Airbus Defence and Space for the German Armed Forces. Many of the required scenario elements are already available in PAXSEM, which is the obvious reason for choosing this tool.

Generally, agents are entities with the following properties: a) Autonomy: the behaviour of the agents is triggered by their own internal ruleset; b) individual and limited perception of the environment; c) the agents interact with other agents and

environment d) show intelligent behaviour e) pursue their goals independently. This way, it is possible to model the dynamic behaviour of a complex adaptive system, as it is depicted by the scenario described below (Jennings, 2000).

EXAMPLE / SCENARIO DESCRIPTION

In the chosen scenario a suicide terrorist enters a fictitious main train station. The station is shown in Figure 2. The situation at the station shows a scene from everyday life. People enter and leave the station through the four main entrances. Within the crowd, a fictitious terrorist carries a nail bomb hidden in a suitcase. He passes the entrance hall and walks to a platform, where a train is waiting for the departure. Finding the perfect spot, he walks along the platform, until he triggers off the bomb in suicidal intent.

Installed security measures are camera surveillance (CCTV), plain-clothes officers (PCO), and metal detection devices (MDD). The cameras are placed on several places in the station and connected to a control room, where the personnel analyse the pictures to detect possible threats. If a terrorist is detected, the personnel alert the PCO, who will try to catch the terrorist. Otherwise the PCO are patrolling in the station. The MDD are combinations of walk-through detectors and X-ray scanners for luggage. The personnel interpret the images of the MDD unit controlling station. The MDD units are placed next to the entry barriers, which separate the entrance hall and the train platforms. So, every passenger who wants to travel has to pass this MDD check point. If the device sounds an alarm, the personnel will alert the PCO immediately and CCTV will focus on the specific MDD unit.

A. Results of the process-model-based expert interviews (eMoE)

The described scenario and security measures have been evaluated with the eMoE methodology as follows:

Camera surveillance (CCTV): The preventive security quality of conventional cameras in context of detection of the terrorist or the weapon in this scenario is estimated as low. According to the experts' estimations, only cameras in combination with observers are able to identify the terrorist as a passenger. Even if a warning is expressed through authorities, a recognition of the terrorists in-between all the passengers is difficult caused by insufficient characteristic features of terrorists. As a result, there are no positive interfaces in the process model. This leads to no effectiveness of camera surveillance as a SeMe to prevent this scenario.

Plain-clothes officers (PCO): The quality of the PCO based on expert estimations is medium, because PCO are highly adaptable to the environment and active SeMe which can influence processes in forms of prevention. Similar to camera surveillance, PCO can hardly differentiate between passengers and a terrorist. In this scenario, the terrorist shows no special behaviour which makes him indistinguishable. Therefore, the effectiveness of the security measure PCO in context of terror attack prevention is zero.

Metal detector devices (MDD): The preventive quality of the MDD in this scenario is estimated as high. This estimation is based on the research results of Kuznetsov, Averianov, Evenin, Gorshkov, Iurmanov et al. (2014) who determined a MDD detection rate for metal in backpacks of 96% to 100% with a false alarm rate under 12%. Singh and Singh published similar results with a false alarm rate of roughly 20% in 2002. Considering the process model, the nail bomb can only be detected when the terrorist passes the MDD at the entrance to the platforms. As a result, there is one positive interface in the process model that has to be considered. Based on the high reliability of the MDD and the fact, that the MDD cannot be bypassed, the effectiveness of the security measure MDD concerning the eMoE methodology is very high. Although the effectiveness of this security measurement is very high, it has to be noted that MDD cause waiting times according the density of passengers and the duration of each individual check. As a result, passengers may have to

Preventive Effectiveness of Security Measures		Performance category
Camera Surveillance (CCTV)	no preventive effect	0
Plain-clothes Officers (PCO)	no preventive effect	0
Metal detection devices (MDD)	very high preventive effect	5
Reinforcement of Effect (combination CCTV-PCO-MDD)		
Total	very high preventive effect	5

Figure 3. Result of eMoE methodology

stand in cues in front of the MDD units, which will be uncomfortable for them. Furthermore, the passengers are restricted in travelling with metal object (cp. aviation transportation system). These inconveniences are not considered in this paper.

Effectiveness of the security measure package CCTV-PCO-MDD: As the CCTV has no positive interfaces of preventive effectiveness; it cannot influence the PCO by giving an alarm on the one hand. However on the other hand, the PCO can be influenced by the MDD. After the MDD detect combat agents, an alarm is sent to the PCO and CCTV (control centre). The combination of MDD, PCO and CCTV reinforce each other to prevent the attack.

Total: As a result the combination of CCTV, PCO and MDD the total effectiveness of the security measurement package is **very high** to prevent this scenario (see Figure 3). The authors note: Not considered are other efficiencies e.g. the indirect effect of security measures on the terrorist in forms of deterrence or mitigation, as well as basic limitations such as luggage restrictions.

B. Results of Multi-Agent-Simulation (MAS)

Within the simulation, the environment is represented by a 3D geometry model. The course of the scenario as follows: On the way to the track platform, the attacker risks entering areas that are illuminated by sensors (CCTV or MDD). If this is the case (+ terrorist stays sufficiently long in the sensor cone), an alarm will trigger the PCO with a certain probability, which will then try to arrest him. This is successful when the alarmed PCO reach the attacker in time or the attacker may be spotted by the PCO directly during their patrolling. The outcome of the scenario is simply measured by a true or false flag indication of a successful ignition of the bomb or not.

For our simulation experiments, we configured the above described scenario with reasonable parameters. With respect to the detection probability of the different security elements, we have chosen the following values:

- p(MDD) = 0.95 which is a conservative estimation acc. Kuznetsov et al. (2014).
- p(CCTV) = 0.01 which is supposed to represent the fact that the prevention capability of a single camera is rather low.
- p(PCO) = 0.02 which is supposed to represent the fact that the prevention capability of a PCO is rather low, but better than a single camera.

The values for p(CCTV) and p(PCO) may be arguable, but we are focusing more on the order of magnitude than on the absolute value. The security elements are set up in the following way: two MDD at the entrance to the platform, two patrols each consisting of two PCO, and ten CCTV located at central positions within the train station.

Obviously, one single simulation run cannot provide any significant results or insights, as it represents only one possible course of action. Therefore, we performed more than five thousands of simulation runs, with each run showing a different course of action. The different scenario evolutions are caused not only by the detection probabilities, but also by the large variety of paths a) the terrorist can take and b) the PCO can take. Due to the large number of simulation results that can be gathered this way (cp. data farming Horne and Schwierz, 2008), an overall probability of prevention can be derived. This probability of prevention can then be assessed either by experts or used to assess the effectiveness of security measures.

The different combinations of SeMe are displayed in Table 1.

SeMe	simulation runs	prevented explosions	prevention probability
PCO+CCTV+MDD	5,250	2,673	50.9%
PCO+MDD	5,236	2,602	49.7%
PCO+CCTV	5,250	292	5.6%
PCO	5,209	107	2.1%

Table 1. Results of multi-agent-simulation (MAS)

In this case, the results show a dependency between the prevention probability and the SeMe combinations. The combination has an increased prevention rate. Especially the combination of MDD as detection device and PCO as intervention SeMe has a very high prevention probability. This constellation already yields a

high degree of prevention, leaving only little room for further detection by CCTVs. The combination of PCO and CCTV shows also a positive effect, but much less in extent than PCO+MDD. The combination of PCO+CCTV+MDD reveals an increase of just 1% in comparison to PCO+MDD. These results allow operators of public transportation systems to decide whether an additional SeMe is efficient or not.

COMPARISION OF RESULTS

The MAS delivers very accurate quantitative results in comparison to the eMoE, which presents semi-quantitative results. Both methods are suitable to proof the effectiveness of SeMe in different resolution. The MAS requires a very precise input in the right magnitude of value. Although, the simulation is stable until a certain magnitude, it is nevertheless difficult to receive such data for some SeMe. The eMoE accepts more input tolerance, but presents results classified in five categories. The application of the results depends on the user requirements of resolution.

The effort and complexity to run MAS is very high and can only be executed in selected scenarios. The MAS simulation runs of the selected scenarios depict the reality in high definition (dependent of agent definition) which makes it difficult to transfer results. The eMoE can easily be implemented (smaller effort). Otherwise the eMoE is highly reliant on the expertise of the expert. The authors suggest summarizing different expert's opinions to ensure reliability.

The major advantage of MAS is the possibility to use the quantitative data for different scenario questions (described in the next section). This possibility cannot be provided by eMoE.

OUTLOOK / PERSPECTIVES

Within the research project RiKoV these results are used to help decision-makers prioritize security measures according their risk reduction (effectiveness), their costs and social acceptance. A multi-criteria decision analysis (MCDA) is used to weight the different options among each other (cp. Lin, Brauner, Muenzberg, Meng and Moehrle, 2013). The comparison of SeMe allows ranking recommendations of the best SeMe according own preferences in the MCDA. It allows no recommendations about a required minimum prevention probability; the decision-maker is responsible to define this level considering organizational conditions.

This is a first, rather simple approach in order to examine the preventive effect of SeMe using a simulation based methodology and an eMoE. In our future research, we will conduct sensitivity analyses to research the robustness of the comparison. Furthermore, we will combine both methods in such a way that eMoE provides the possibility to perform a fast preliminary analysis to check possibilities for MAS.

It looks very promising that we will continue our research in order to tackle further, obvious questions: How sensitive do prevention probabilities depend on detection probabilities? How strong is the influence of false alarm rates? In order to check and discuss our procedure and the chosen scenario configurations; we will involve security experts from relevant domains.

ACKNOWLEDGMENTS

Parts of the presented research were financially supported by Federal Ministry of Education and Research of Germany within the Research project RiKoV. We are grateful for this support. In addition, we thank Prof. Dr. Stefan Pickl, Project Coordinator, Mario Dally and Martin Weiderer of the University of the Federal Armed Forces Munich for their great collaboration and dedicated support.

REFERENCES

1. Brauner, F., Baumgarten, C., Kornmayer, T., Bentler, C., Mudimu, O.A., and Lechleuthner, A. (2014) A Methodology for a vulnerability analysis of public transportation systems in context of terrorist attacks. *9th Future Security, Security Research Conference*; Berlin, Germany.
2. Brauner, F., Baumgarten, C., Schmitz, W., Neubecker, K.A., Mudimu, O.A., and Lechleuthner, A. (2013) RiKoV – Risk analysis of terrorist threats to rail-bound public transportation: Development of an integrated planning solution

for efficient economic and organisational measures. *10th World Congress on Railway Research 2013*; Sydney, Australia.

3. Cox, L.A. Jr. (2008) Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *RISK ANALYSIS*, 28, 6, pp 1749–1761.
4. Fonseca, S.P., Griss, M.L., and Letsinger, R. (2002) Agent Behavior Architectures - A MAS Framework Comparison, in *AAMAS '02 Conference on Autonomous agents and multiagent systems*.
5. Horne, G. E., and Schwierz, K.-P. (2008) Data Farming around the world overview. *Winter Simulation Conference*, pp 1442-1447.
6. Horne, G.E. and Meyer, T.E. (2005) Data farming: discovering surprise, in *Winter Simulation Conference*, ACM, pp 1082-1087.
7. Jennings, N.R. (2000) on agent-based software engineering, *Artificial Intelligence*, 117, pp 277-296.
8. Kuznetsov, A., Averianov, V., Evenin, A., Gorshkov, I., Iurmanov, P. et al. (2014) Automatic Standoff Detection Of Threats in Crowded Areas; *9th Future Security Conference*, Berlin, Germany.
9. Lin, L., Brauner, F., Muenzberg, T., Meng, S., and Moehrle, S. (2013) Prioritization of security measures against terrorist threats to public rail transport systems using a scenario-based multi-criteria method and a knowledge database. *8th Future Security Conference*, Berlin, Germany.
10. Singh, S., and Singh, M. (2003) Explosives detection systems (EDS) for aviation security, *Signal Processing*, 83, pp 31–55.
11. Weyns, D., Parunak, H.V.D., Michel, F., Holvoet, T., and Ferber, J. (2004) Environments for Multiagent Systems State-of-the-Art and Research Challenges. in Weyns, D., Van Dyke, Parunak, H. and Michel, F. (ed.) *'E4MAS'*, Springer, pp 1-47.
12. Wieneke, M., and Koch, W. (2009) Combined person tracking and classification in a network of chemical sensors, *International Journal of Critical Infrastructure Protection*, 2, 1-2, pp 51-67.
13.