ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/325654821

A Study on the Influence of Uncertainties in Physical Security Risk Analysis

Conference Paper · June 2018

CITATIONS
4

READS
1,794

2 authors:



Daniel Lichte
German Aerospace Center (DLR)
43 PUBLICATIONS **75** CITATIONS
SEE PROFILE



Kai-Dietrich Wolf
Bergische Universität Wuppertal
38 PUBLICATIONS **96** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Uncertainty analysis View project

Project Risk assessment of automotive mobile access systems View project

All content following this page was uploaded by Daniel Lichte on 26 June 2019.

The user has requested enhancement of the downloaded file.

A Study on the Influence of Uncertainties in Physical Security Risk Analysis

D. Lichte & K.-D. Wolf
Institute for Security Systems, University of Wuppertal, Velbert, Germany

ABSTRACT: In security risk analysis and assessment, uncertainties regarding occurring threats, consequences and the capabilities of security systems to mitigate vulnerability are enormous. Although some quantitative approaches exist in security risk analysis that allow the consideration of these uncertainties, most practical assessments are based on expert knowledge in semi-quantitative or qualitative models. This paper presents a study on the influence of uncertainties in physical security risk analysis using the example of a semi-quantitative risk assessment of a notional production infrastructure. Therefore, a procedure is suggested as a systematic approach to transfer differing expert ratings into a pdf-based description for a quantitative approach. The influences of uncertainties on the exemplary assessment are calculated and discussed regarding the validity of the results. To visualize these results and to support the decision-making process, a three-dimensional risk matrix is proposed.

1 INTRODUCTION

In security risk analysis and assessment, uncertainties regarding occurring threats, consequences and the capabilities of security systems to mitigate vulnerability are high. Although some quantitative approaches exist in security risk analysis that allow the consideration of these uncertainties, most practical assessments are based on expert knowledge in semi-quantitative or qualitative models.

As uncertainties are hardly or not completely considered, these models do not allow an estimation of their influence on the validity of a conducted assessment. Additionally, the influence of occurring events with a very low probability of occurrence and disastrous consequences, e.g. black swan events, are possibly not considered in these models, as they are very uncertain.

This paper investigates the influence of uncertainties on physical security risk analysis for the example of a semi-quantitative risk assessment of a notional production infrastructure.

To demonstrate the described lack of consideration of uncertainties, the state of the art regarding security risk assessment and vulnerability assessment is outlined. Existing approaches are briefly introduced and the occurring difficulties regarding the use of expert knowledge are described.

For analysis purposes a simple semi-quantitative model for security risk assessment is set up and a transition to a quantitative approach based on (Lichte & Wolf 2017) is introduced. This approach uses probability density functions (pdfs) to describe the abilities of security measures as well as the probability of occurrence of a threat and also the level of possible consequences. The variance of the security measure-related pdfs can be interpreted as the uncertainty concerning the capabilities of the considered measures that are part of the security system. At the same time, differing ratings by experts reflect a rising level of uncertainty that consequently lead to a higher level of variance of the generated pdfs.

Besides the intended purpose of the analysis, the transition is developed to suggest a systematic approach to transfer differing expert ratings to the pdf-based description for the quantitative approach. Subsequently, the influences of the resulting uncertainties on the exemplary assessment are calculated and discussed regarding the validity of the results. To visualize these results and to support the decision-making process, a three dimensional risk matrix is proposed. Finally, the study is summarized and discussed in the

general context of security risk assessment and the consideration of uncertainties.

2 STATE OF THE ART

2.1 *Security Risk Analysis*

Security risk analysis is conducted by experts from different fields of expertise, as security is a holistic term (Harnser Group 2010). The protection of infrastructures against intentional physical attacks is covered by the subdomain of physical security (Beyerer et al. 2010). In detail, the protection of infrastructures is implemented by security measures intended to prevent attackers from reaching their targets or assumed infrastructure assets. The measures include different means of protection, detection and intervention and additionally resilient structures to mitigate the consequences of successful attacks (Garcia 2008).

A possible definition of security risk is formulated as a function of the triplet threat, vulnerability and consequence (Contini et al. 2012, McGill et al. 2007):

Risk= Threat x Vulnerability x Consequence

This definition is the common basis for mostly all semi-quantitative methods for risk assessment that are used in the field. Recently, this classic definition was discussed e.g. in (Amundrud et al. 2017), regarding its lack to consider uncertainties inherent to its parameters. If the above introduced formulation for security risk is considered as a multiplication of quantitative values, it is apparently only valid for stochastically independent discrete probabilities. Usually, these preconditions are not given, as at least threat and vulnerability are fraught with uncertainty. It may even be discussed whether the description of these parameters as probabilities in the sense of classical frequentist probability theory is justified. However, probability theory is an established concept to handle uncertain quantities. Additionally it can be extended in accordance to the axioms of Kolgomorov in a suitable manner to use it according to the above outlined constraints in security risk assessment. For example, the interpretation of the risk definition based on Bayesian probability theory enables the modeling of the parameter triplet by the formulation as degree-of-belief-densities, thus enabling the consideration of inherent uncertainties formally compliant with probability theory (Beyerer & Geisler 2016).

Thus, the definition combines in a quantitative manner consequences of attacks and probabilities of threat scenarios with the risk of success of individual attacks defined as vulnerability. The above quantitative definition of risk may help to deduce acceptable risks and necessary measures to reduce risks (Broder & Tucker 2012). Inherent uncertainties regarding the three risk factors should be cautiously considered (Campbell & Stamp 2004).

Various approaches to security risk assessment have been developed, which may be divided into qualitative, quantitative and hybrid methods (Meritt 2008). Qualitative methods are mostly based on expert knowledge, while existing quantitative methods use discrete probabilities. Additionally, some quantitative methods aiming at cost-benefit analysis have been developed. Typically, cost-benefit analyses of security measures compute potential financial losses as a result of an attack, the probability of occurrence of various attack scenarios and the vulnerability of the security system (Flammini et al. 2009). This analysis yields accurate results but raises the complexity compared to qualitative methods (Landoll 2011).

2.2 *Vulnerability Assessment*

Quantitative vulnerability analysis as part of the quantitative risk analysis is mostly based on methods adapted from reliability and general risk analysis. Here, the considered model is dependent on given attack scenarios (French & Gootzit 2011). This dependency is detrimental to a comprehensive analysis as knowledge about the behavior of a potential attacker may be insufficient (Cox Jr. 2009). The different modeling approaches can be further split up into mainly analytical but also formal methods. An overview of approaches is given by Nicol et al. (Nicol et al. 2004). Analytical methods are often based on attack trees, which can be seen as a derivative of the fault trees known from reliability analysis. Attack trees were first used by Schneier (Schneier 1999) for IT-security analysis and since then have been further developed by different authors, summarized e.g. by Vintr et al. (Vintr et al. 2012).

Contini et al. have introduced incoherent attack trees to characterize the dynamic behavior of the considered system (Contini et al. 2008). Additionally, they integrated simple probability distributions for protection into attack trees to investigate the chronologic sequence of attacks. Hence, it is possible to analyze the security system's ability for an attack intervention by comparing the probabilities of residual protection and system's response (Contini et al. 2012).

Garcia describes this relation (Garcia, 2008), where feasible attack paths as part of different attack scenarios and corresponding barriers are used. The model is time-based and introduces the critical detection point, which is the latest possible point of detection that ensures a successful intervention against the potential attacker.

A quantitative model that further develops the approaches of Contini et al. (Contini et al. 2012) and Garcia (Garcia, 2008) was introduced in (Lichte et al. 2016) and applied to an infrastructure in (Lichte & Wolf 2017). The suggested vulnerability model uses

pdfs to describe the characteristics of security measures and uses a path-based barrier model. Additionally it uses the principle of the weakest path. The developed approach in this paper uses this vulnerability model as a basis.

Summarizing, the different existing approaches to analytical modeling and analysis of vulnerability as well as security risk analysis are lacking the consideration of uncertainties in the system parameters and overall behavior. Additionally a great number of these approaches relies on expert knowledge, causing various problems that are described in the next paragraph.

2.3 *Expert Knowledge and Uncertainty in Security Risk Assessment*

The elicitation and use of expert knowledge is an often used approach in risk assessment, e.g. to determine point estimates for unknown parameters (Kaplan 1992). Especially, this approach is used to develop and parametrize models for risk assessment in case the available database is very small or there is a lack of objective data (Bolger & Wright 2017).

Therefore, methods for the elicitation of expert knowledge are developed to minimize subjectivity and uncertainty in parameter estimation. Though, the use of expert knowledge itself generally raises the problem of uncertainties in probabilistic risk assessment that should cautiously be analyzed (Rausand 2013) (Aven & Zio 2013). Latest developments in general risk assessment are focusing on uncertainty as a key concept of risk assessment (Aven 2016). Especially in the analysis of rare events that may lead to catastrophic consequences with large uncertainties, different approaches to deal with uncertainty have been suggested and analyzed, e.g. in (Flage et al. 2014).

Especially security risk assessment is often accompanied by great uncertainties, as there is a lack of evidence of threats, consequences and the abilities of security measures. Thus, qualitative or semi-quantitative models that strongly rely on expert knowledge are often used, although these models can lead to misleading or even wrong results (Landoll 2011). Consequently, an analysis of the described resulting uncertainties should be conducted for security risk assessment. This paper discusses an approach of a transition from a semi-quantitative to a quantitative model, which enables further analysis in this direction.

3 APPROACH

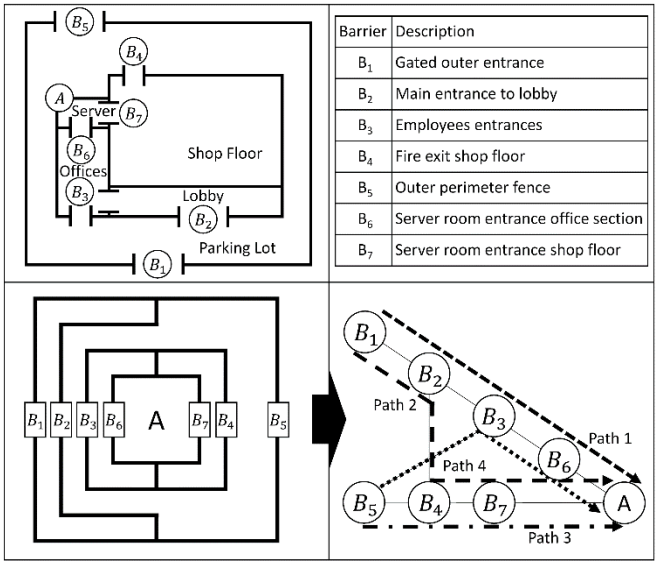
To analyze the influence of uncertainties especially emerging from the dependence on expert knowledge in semi quantitative risk assessment methods, an approach is introduced that allows the transition to a risk model that uses triangular pdfs. Both methods are gradually applied to an exemplary infrastructure depicted in Figure 1. The results of both risk models are analyzed for deviations and possible causes. Therefore, a simplified semi-quantitative approach to security risk assessment is presented first. It is based on existing methods, e.g. (Harnser Group 2010). The part of vulnerability assessment reflects four basic assumptions presented in (Lichte & Wolf 2017):

1 The weakest path of the security system determines the system's vulnerability as the chosen path of the attacker is uncertain.
2 The combination of protection and observation at barriers is necessary as an attacker is always able to break through a barrier given infinite time without being detected.
3 The detection of an attack is possible only if the protection is sufficient to prevent a breakthrough under observation until detection.
4 After detection, an attack can be stopped only if the residual protection along the remaining attack path lasts long enough to prevent the attacker from reaching the asset until intervention is completed.

In a second step, the developed approach is extended to be able to consider various contributions from expert knowledge. Subsequently, a transition is presented that uses triangular pdfs to represent the various semi-quantitative ratings of the experts. Thus, the differences of the experts' assessments are treated as uncertainties. In the last step, possible results for the semi-quantitative model are compared to the transformed model.

3.1 *Exemplary Production Infrastructure*

A basic drawing of the considered production infrastructure is outlined on the upper left of Figure 1. The model only considers security measures located along paths that lead to the server room, which is assumed as the asset of a possible attack. The upper right of Figure 1 denotes the security measures marked in the drawing.



Barrier	Description
B_1	Gated outer entrance
B_2	Main entrance to lobby
B_3	Employees entrances
B_4	Fire exit shop floor
B_5	Outer perimeter fence
B_6	Server room entrance office section
B_7	Server room entrance shop floor

Figure 1. Outline of Infrastructure and Security System

The model depicted on the lower left of Figure 1 (onion layer model) represents the structure and feasible attack paths by means of barriers. Four individual attack paths lead to the asset *A* via barriers B_1-B_7.

All feasible attack paths of the exemplary infrastructure are extracted into a path-based model. The result of the extraction of the attack paths is shown on the lower right of Figure 1. It includes all four attack paths directed towards the asset.

3.2 *Semi-Quantitative Risk Assessment*

The presented semi-quantitative method for security assessment is divided into three submodels. In analogy to the risk definition there are submodels for threat, vulnerability and consequence assessment. The security risk is then indicated in a two dimensional risk matrix, in which the ordinate shows the probability of occurrence of a threat incorporating the vulnerability of the infrastructure against the threat. The axis of abscissas maps estimated consequences.

Threat and consequence assessment are simplified to the estimation of threat probability and level of consequences in ranking scales with five steps, which are described in Table 1.

Table 1. Ranking scale Threat & Consequence

1	2	3	4	5	Expert Score
Scale Threat [probability]					
0.0-0.2	0.2-0.4	0.4-0.6	0.6-0.8	0.8-1.0	2
Scale Consequence [100k $]					
0-1	1-2	2-3	3-4	4-5	4

The presented semi-quantitative model for vulnerability assessment is based on a barrier-oriented view of the infrastructure. Therefore, the commonly used parameters protection, observation and intervention have to be estimated at every security barrier of the infrastructure (Lichte et al. 2016). To realize this, the model uses a five step ranking scale to estimate the time based capabilities of the considered security measures. The ranking scale that is chosen depending on the considered infrastructure as well as the corresponding estimations is shown in Table 2 & 3.

Table 2. Score Descriptions P,O,I

1	2	3	4	5
Scale P,O [s]				
0-90	90-180	180-270	270-360	360-450
Scale I [s]				
0-180	180-360	360-540	540-720	720-900

Table 3. Ranking scale Threat & Consequence

Barrier i	Expert Score		
	P	O	I
1	1	5	3
2	4	1	1
3	2	2	4
4	2	5	5
5	1	5	4
6	5	3	2
7	5	2	2

First, the probability of a detection of the attacker needs to be modeled- Based on the four basic assumptions a high level of protection and observation enables a high probability of a triggered alarm A_i at a barrier, so that:

$$A_i = \frac{P_i + (O_{max} - O_i)}{P_{max} + O_{max}} \quad (1)$$

Herein P_{max} and O_{max} represent the highest possible score in the ranking scale. For the first barrier B_1 of path 1 of the example infrastructure we get:

$$A_1 = \frac{1 + (5-5)}{10} = 0.1 \quad (2)$$

In a second step, the level of security of a barrier is described by the possibility of an intervention taking place before the attacker reaches the asset. This is described by merging the residual protection of a barrier with the estimated duration of an intervention. The residual protection R_i can be interpreted as the sum of all remaining *n* protection times along the considered attack path. Using a floor function to obtain an integer as a result we obtain:

$$R_i = \left\lfloor \frac{\sum_{i=1}^{n} P_i}{n} \right\rfloor \quad (3)$$

$$R_1 = \left\lfloor \frac{1+4+2+5}{4} \right\rfloor = 3 \quad (4)$$

The residual protection is then merged with the duration of intervention I_i of the barrier to obtain the possibility of a timely intervention T_i.

$$T_i = \left(\frac{R_i - I_i}{R_{max} + I_{max}}\right) + 0.5 \,, T \in (0.1, \ldots, 0.9) \quad (5)$$

$$T_1 = \left(\frac{3-3}{10}\right) + 0.5 = 0.5 \quad (6)$$

Using the results for the possibility of a triggered alarm and a timely intervention the vulnerability of the feasible attack paths depicted in Figure 2 is calculated by:

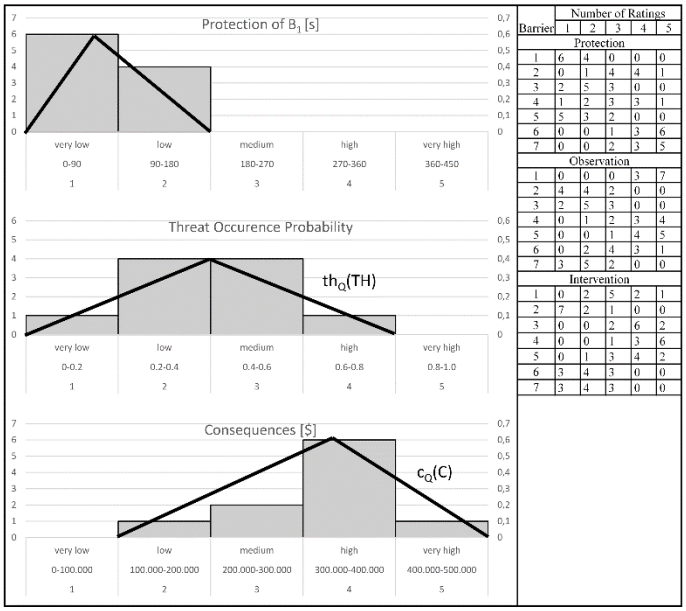
$$V_{Path} = \prod_{i=1}^{n} 1 - (A_i \cap T_i) \quad (7)$$

For path 1 this yields:

$$V_{Path,1} = (1 - 0.3)(1 - 0.35)(1 - 0.25) \cdot (1 - 0.35) = 0.147 \quad (8)$$

3.3 *Consideration of Multiple Expert Knowledge*

In order to analyze the influence of uncertainties in threat, vulnerability and consequence assessments, judgements of multiple experts are now introduced. Hypothetical assessments of k=10 experts are introduced and aggregated in a histogram that shows the frequency of the scores given by the experts. As an example, the histogram of the absolute and relative frequencies for protection measures at B_1 as well as for threat and consequence are shown in Figure 2.



Barrier	Number of Ratings 1	2	3	4	5
Protection					
1	6	4	0	0	0
2	0	1	4	4	1
3	2	5	3	0	0
4	1	2	3	3	1
5	5	3	2	0	0
6	0	0	1	3	6
7	0	0	2	3	5
Observation					
1	0	0	0	3	7
2	4	4	2	0	0
3	2	5	3	0	0
4	0	1	2	3	4
5	0	0	1	4	5
6	0	2	4	3	1
7	3	5	2	0	0
Intervention					
1	0	2	5	2	1
2	7	2	1	0	0
3	0	0	2	6	2
4	0	0	1	3	6
5	0	1	3	4	2
6	3	4	3	0	0
7	3	4	3	0	0

Figure 2. Exemplary Histograms and Rankings according to aggregated expert knowledge

On the right-hand side of Figure 2 the ranking of all experts for all barriers of the security system of the example infrastructure is included.

3.4 *Transition to the Usage of Probability Density Functions*

In this step, the semi-quantitative models are transformed into quantitative models. Both types of models use similar operations based on conditional probabilities to describe the security risk of an infrastructure.

Therefore we develop triangular pdfs on the base of the above found histograms that result from the differing ratings of multiple experts. Triangular distributions are widely used in different fields of risk analysis to estimate probability distributions under uncertainty (Haimes 2015). The characteristic parameters of the function are lower limit *a*, upper limit *b* and mode *c*. The determination of the parameters for all input parameters of the risk model are based on the respective histograms of the relative frequency (see fig. 2).

The lower limit *a* and the upper limit *b* for the pdfs of threat and consequence are determined by the minimum and maximum value given in the ranking score for probability of occurrence and costs of a successful attack, respectively. The median interval of the respective histogram is assumed as mode *c*. The resulting fitted triangular pdfs are outlined in Figure 2.

The obtained values for the pdf parameters for threat $th_Q(TH)$ and consequence $c_Q(C)$ are listed in Table 4.

Table 4: distribution parameters for th_Q & c_Q

	a	b	c
th_Q	0	0.8	0.4
c_Q	1	5	3.33

In contrast to the simplified threat and consequence submodels, the transition of the vulnerability submodel is more complex due to the relations between the input parameters. To manage transition, the five ranking scores are transformed to time-based intervals depending on the chosen time-based ranking scales (see Tab. 2) to describe the characteristics of the security measures according to [Lichte & Wolf 2017]:

- Protection is characterized by an estimated time needed for a break-through.
- Observation is the time span needed for a detection.
- Intervention is the period of time until an intervention is completed.

The resulting intervals mark reasonable time steps to describe the time based characteristics and at the same time reflect the assessment of the experts.

In order to ensure comparability within the model, the J=5 time intervals for all protection and observation measures Δt_{ij} at the i barriers of the infrastructure lie in the time span $[0,t_{max})$. The reasonable choice for the value of t_{max} depends on the considered infrastructure. The intervals Δt_{ij} are all of the same size. For the example infrastructure t_{max}=450 [s]

Due to the modeled relations, the time span of the intervention measures can possibly reach higher values. Therefore the upper considered time span for intervention measures is set to $t_{max,I}$=900 [s]. As the number of intervals does not change, the intervals $\Delta t_{I,ij}$ grow proportionally.

Now, a triangular pdf can be fitted into the histograms for protection, observation and intervention measures of the security system. The intended fitting of the function is outlined in Figure 2. Therefore, the

lower limit *a* and the upper limit *b* are defined for protection and observation as the minimum and maximum value for t within the intervals comprised in the scoring of the experts. The lower interval l of the j=5 overall intervals containing expert scores can be found via the following conditions:

$$\sum_{j=1}^{l} k_j > 0 \ and \sum_{j=1}^{l-1} k_j = 0 \quad (9)$$

The conditions for the upper interval u are:

$$\sum_{j=1}^{u} k_j > 0 \, and \sum_{j=u}^{j} k_j = 0 \quad (10)$$

Following, the lower limit a and the upper limit b are determined by:

$$a = t_{min} = \min(\Delta t_{il}) \quad (11)$$

$$b = t_{max} = \max(\Delta t_{iu}) \quad (12)$$

The definition of intervention is equal using $\Delta t_{I,ij}$. The mode *c* for all security measures is determined by means of calculating the median of grouped data. First the median interval of the grouped data can be defined as the interval *m*, which contains the median of the dataset:

$$\sum_{j=1}^{m-1} k_j < \frac{k}{2} \ and \ \sum_{j=1}^{m} k_j \geq \frac{k}{2} \quad (13)$$

Following, the median within the found interval *m* is estimated by linear interpolation assuming an equal distribution as no further information about the distribution within the interval is available. With the lower boundary of the median interval l_m and the upper boundary u_m we obtain:

$$c = t_m = l_m + \frac{\frac{k}{2} - \sum_{j=1}^{m-1} k_j}{k_m} \cdot (u_m - l_m) \quad (14)$$

For the derivation of the parameters of the triangular function of the protection measure at barrier B_1 of the example system we obtain:

$$\sum_{j=1}^{l} k_j > 0 \ and \sum_{j=1}^{l-1} k_j = 0 \ \rightarrow l = 1 \quad (15)$$

$$\sum_{j=1}^{u} k_j > 0 \, and \sum_{j=u}^{J} k_j = 0 \ \rightarrow u = 2 \quad (16)$$

$$a = t_{min} = \min(\Delta t_{11}) = 0 \quad (17)$$

$$b = t_{max} = \max(\Delta t_{12}) = 180 \quad (18)$$

$$\sum_{j=1}^{m-1} k_j < \frac{k}{2} \ and \ \sum_{j=1}^{m} k_j \geq \frac{k}{2} \rightarrow m = 1 \quad (19)$$

$$c = t_m = 0 + \frac{\frac{10}{2} - \sum_{j=1}^{1-1} k_j}{6} \cdot (90 - 0) = 75 \quad (20)$$

As all parameters for the triangular pdfs for the vulnerability submodel p(t), o(t) and I(t) are now defined, the calculation of the path vulnerability $V_{Q,Pathi}$. by applying the quantitative model is possible. The characteristic parameters and their relation to each other in the quantitative vulnerability submodel are taken from (Lichte& Wolf 2017).

Inserting the obtained pdfs for the barriers of path 1 of the example system into the quantitative model we obtain for the path vulnerability $V_{Q,Path1}$

$$V_{Q,Path1} = 0.028 \quad (21)$$

3.5 *Results and Analysis*

As the vulnerability of both models is based on the principle of the weakest path, the other three feasible attack paths also have to be calculated. The results for the semi-quantitative and the quantitative model are summarized in Table 5:

Table 5: Vulnerability V_S & V_Q for all attack paths

Path	V_S	V_Q
1	0.147	0.028
2	0.141	0.014
3	0.328	0.209
4	0.341	0.430

The resulting risk is entered into a security risk matrix for both models. The risk matrix for the semi-quantitative model considering the vulnerability of the weakest path 4 is shown in Figure 3.

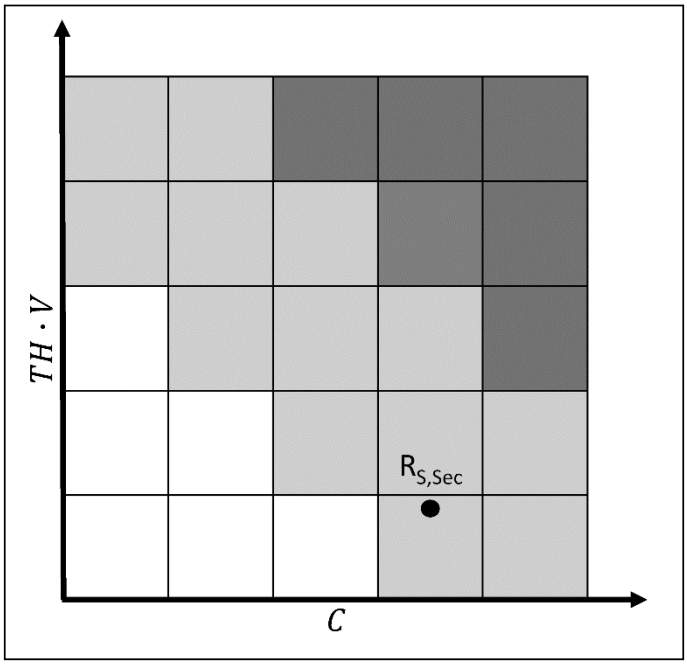


Figure 3. Security Risk Matrix for the Semi-Quantitative Model

The security risk R_S estimated by the semi-quantitative model is calculated to:

$$R_{S,Sec} = \left(TH_S \cdot V_{S,Path4}\right) \cdot C_S = 59{,}752\ \$ \quad (22)$$

As the quantitative model uses pdfs the risk matrix is extended to a three dimensional risk matrix. Basically, the matrix maps the bivariate pdf of the risk $R_{Q,Sec}$. It incorporates the probability of occurrence of a threat considering the vulnerability of the infrastructure and the consequences. The distribution-based

quantitative risk matrix of the example infrastructure is depicted in Figure 4.

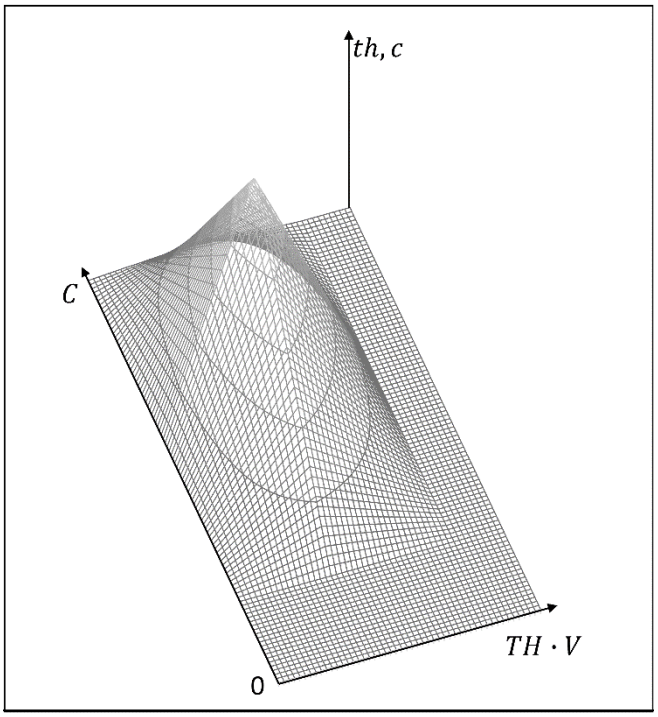


Figure 4.3D Security Risk Matrix

The security risk estimated by the use of the quantitative model is received by the cumulated bivariate pdf. For the example infrastructure we obtain:

$$R_{Q,Sec}(c_Q, th_{V,Q}) = \int_0^{c_Q} \int_0^{th_{V,Q}} f_{C_Q,TH_{V,Q}}(C_Q, TH_{V,Q})\, dC_Q\, dTH_{V,Q}\,,\quad TH_{V,Q} = TH_Q \cdot V_{Q,Path4} \tag{23}$$

Thus it is possible to calculate the overall security risk.

$$R_{Q,Sec} = 133{,}344\ \$ \tag{24}$$

Other results for interesting boundaries of the distribution variables can also be obtained For example we chose two especially important risk cases to be considered:

- Very high estimated consequences C>400,000 $
- Black swan events with a very low probability of occurrence of the threat TH<0.05 and very high consequences C>400,000 $

When calculating according to (23) we are able to obtain a probability P for the special case, given the overall scenario as well as the resulting risk in terms of consequence:

$$R_{Q,1} = 29{,}920\$\,, P_{Q,1} = 0{,}07 \tag{25}$$

$$R_{Q,2} = 1029\$\,, P_{Q,2} = 0.0024 \tag{26}$$

The analysis shows that the semi-quantitative model covers a smaller window of possibly occurring security risks and estimates a significantly lower overall risk. As a result, the model only provides a risk point estimate. Therefore, information about certain cases, e.g. rare events, is neither visible nor can be considered in the risk assessment.

This is especially shown by the two risk cases applied to the considered scenario and the example infrastructure. In contrast to the quantitative model, the information about a probability of occurrence of such events is not comprised in the results of the semi-quantitative model. This information is visualized in the three dimensional risk matrix of the quantitative model (see fig. 4). It shows the probability of occurring risk cases at the boundaries of the considered scenario besides an average risk, e.g. black swan scenarios like in $R_{Q,2}$.

Furthermore, this is reflected in the differing results of the vulnerability analysis. Although the trend for the vulnerability of the single attack paths of the considered infrastructure is similar, the absolute results differ. The reason for this difference is again a result of the consideration of uncertainties within the vulnerability assessment resulting from the elicitated expert knowledge.

Both findings underline the importance to consider uncertainties to be aware of possible boundary cases, e.g. of rare events with great consequences in a complete risk analysis and decision-making process.

4 CONCLUSION AND OUTLOOK

The paper shows the influence of uncertainties on physical security risk assessment and the resulting need for a consideration of uncertainties. Therefore the paper outlines the state of the art in the field of security risk assessments and expert knowledge especially regarding resulting uncertainties. It is shown that semi-quantitative modeling using expert knowledge is a common used practice though these models lack a consideration of uncertainties so far. To tackle this problem, an approach is introduced that enables a transition towards quantitative modeling using expert knowledge as a basis.

Following, the approach is further detailed and step by step applied to a notional production infrastructure. Therefore a simplified semi-quantitative security risk assessment method is introduced and the transition using triangular pdfs is shown. In a last step a three dimensional risk matrix based on a bivariate pdf resulting on threat, vulnerability and consequences is set up. Subsequently, a comparison of the results of the example infrastructure for both modeling approaches is conducted. Hereby, differing results for the risk analysis and the possible influence of uncertainties are revealed.

The presented approach shows the influence of uncertainties to physical risk analysis and proposes a three dimensional risk matrix that visualizes possible rare events at the boundaries of estimated threats. Additionally it presents a method for elicitation and use

of expert knowledge in the context of physical security risk assessment. Continuously this approach can be further developed to support profound decision-making based on a comprehensive security risk assessment.

Nevertheless, the approach needs further enhancement especially in detailing the input parameters for threats and consequences. The further analysis of the vulnerability is needed also. Here, the influence of uncertainties on the vulnerability assessment should be analyzed, e.g. by Monte-Carlo simulation and sensitivity analysis. The applicability of other modeling approaches like info-gap models should be investigated.

5 REFERENCES

Amundrud, O. & Aven, T. & Flage, R. 2017. How the definition of security risk can be made compatible with safety definitions. In: Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231(3): 286–294.

Aven, T. 2016. Risk assessment and risk management: Review of recent advances on their foundations. European Journal of Operational Research 253 (1): 1-13.

Aven, T. & Zio, E. 2014. Foundational Issues in Risk Assessment and Risk Management. Risk Analysis 34 (7):1164-1172.

Beyerer, J. & Geisler, J. 2016. A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security. In: European Journal for Security Research 1: 135-150.

Beyerer, J. & Geisler, J & Dahlem, A. & Winzer, P. 2010. Sicherheit: Systemanalyse und Design. In: Sicherheitsforschung – Chancen und Perspektiven. Berlin: Springer.

Bolger, F. & Wright G. 2017. Use of expert knowledge to anticipate the future: Issues, analysis and directions. International Journal of Forecasting 33 (1): 230-243.

Broder, J. F. & Tucker, E. 2012. Risk Analysis and the Security Survey, 4th ed. Waltham: Butterworth-Heinemann.

Campbell, P. L. & Stamp J. E. 2004. A Classification Scheme for Risk Assessment Methods. Albuquerque: Sandia National Laboratories.

Contini, S. & Cojazzi, G. G. M. & Renda, G. 2008. On the use of non-coherent fault trees in safety and security studies. Reliability Engineering and System Safety 93 (12): 1886-1895.

Contini, S. & Fabbri, L. & Matuzas, V. & Cojazzi, G. 2012. Protection of Multiple Assets to Intentional Attacks. A Methodological Framework. In: 11th Probalistic Safety Assessment 2012, Proc. intern. conf., Helsinki.

Cox Jr., L. A. 2009. Risk Analysis of Complex and Uncertain Systems. New York: Springer.

Flage R. & Aven, T. & Zio, E. & Baraldi, P. 2014. Concerns, Challenges, and Directions of Development for the Issue of Representing Uncertainty. In: Risk Assessment-. Risk Analysis 34 (7): 1196-1207.

Flammini, F. & Gaglione, A. & Mazzocca, N. & Pragliola, C. 2009. Quantitative security risk assessment and management for railway transportation infrastructures. In: Critical Information Infrastructure Security. Berlin: Springer.

French, G. S. & Gootzit, D. 2011. Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack. In: Vulnerability, Unvertainty and Risk: Analysis, Modeling and Management, Proc. conf., Hyattsville.

Garcia, M. L. 2008. The Design and Evaluation of Physical Protection Systems. 2nd ed. Burlington: Butterworth-Heinemann.

Haimes, Y. 2015. Risk modeling, assessment, and management. In: Wikey series in systems engineering and management, 4th ed. Hoboken:Wiley.

Harnser Group (Ed.) 2010. A Reference Security Management Plan for Energy Infrastructure. Brussels: European Commission.

Kaplan, S. 1992. 'Expert Information' versus 'expert opinions'. Another approach to the problem of eliciting/combining/using expert knowledge in PRA. Reliability Engineering & System Safety 35 (1): 61-72.

Landoll, D. J. 2011. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, 2nd ed. Boca Raton: CRC Press.

Lichte, D. & Marchlewitz, S. & Wolf, K.-D. 2016. A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

Lichte, D. & Wolf, K.-D. 2017. Quantitative Multiple-Scenario Vulnerability Assessment Applied to a Civil Airport Infrastructure. In: 27th European Safety and Reliability Conference ESREL 2017, Proc. intern. conf., Portoroz, Slovenia.

McGill, W. L. & Ayyub, B. M. & Kaminskiy, M. 2007. Risk Analysis for Critical Asset Protection. Risk Analysis, 27 (5), 1265–1281.

Meritt, J. W. 2008. A Method for Quantitative Risk Analysis. In: 22nd National Information Systems Security Conference, Proc. nat. conf., Arlington.

Nicol, D. M. & Sanders, W. H. & Trivedi, K. S. 2004. Model-based evaluation: from dependability to security. IEEE Transactions on Dependable and Secure Computing 1 (1): 48-65.

Rausand, M. 2013. Risk Assessment Theory, Methods, and Applications. New York:Wiley.

Schneier, B. 1999. Attack Trees. In: Dr. Dobbs Journal 24 (12): 21–29.

Solano, E.: Methods for Assessing Vulnerability of Critical Infrastructure, Institute for Homeland Security Solutions.

Vintr, Z. & Valis, D. & Malach, J. 2012. Attack tree-based evaluation of physical protection systems vulnerability. In: 2012 IEEE International Carnahan Conference on Security Technology (ICCST), Proc. intern. conf., Carnahan.

View publication stats