European Journal for Security Research
https://doi.org/10.1007/s41125-021-00075-3

ORIGINAL ARTICLE

Representing Uncertainty in Physical Security Risk Assessment

Considering Uncertainty in Security System Design by Quantitative Analysis and the Security Margin Concept

Daniel Lichte[1] · Dustin Witte[2] · Thomas Termin[2] · Kai-Dietrich Wolf[2]

Received: 20 June 2021 / Accepted: 12 November 2021

Abstract
The importance of (physical) security is increasingly acknowledged by society and the scientific community. In light of increasing terrorist threat levels, numerous security assessments of critical infrastructures are conducted in practice and researchers propose new approaches continuously. While practical security risk assessments (SRA) use mostly qualitative methods, most of the lately proposed approaches are based on quantitative metrics. Due to little evidence of actual attacks, both qualitative and quantitative approaches suffer from the fundamental problem of inherent uncertainties regarding threats and capabilities of security measures as a result from vague data or the usage of expert knowledge. In quantitative analysis, such uncertainties may be represented by, e.g., probability distributions to reflect the knowledge on security measure performance available. This paper focuses on the impact of these uncertainties in security assessment and their consideration in system design. We show this influence by comparing the results of a scalar evaluation that does not take into account uncertainties and another evaluation based on distributed input values. In addition, we show that the influence is concentrated on certain barriers of the security system. Specifically, we discuss the robustness of the system by conducting quantitative vulnerability assessment as part of the SRA process of an airport structure example. Based on these results, we propose the concept of a security margin. This concept accounts for the uncertain knowledge of the input parameters in the design of the security system and minimizes the influence of these uncertainties on the actual system performance. We show how this approach can be used for vulnerability assessment by applying it to the initially assessed configuration of the airport structure. The results of this case study support our assumptions that the security margin can help in targeted uncertainty consideration leading to reduced system vulnerability.

Extended author information available on the last page of the article

Published online: 28 November 2021

Keywords Security · Uncertainty · Security risk assessment · Security margin · Vulnerability · Critical infrastructures

1 Introduction

Physical security risk assessment (SRA) has gained importance in recent years; in particular, the vulnerability of critical infrastructures against terrorist threats is regularly assessed. For this purpose, new approaches emerged aiming at the introduction of quantitative metrics, e.g., by Flammini et al. (2013) and Landucci et al. (2017). In practice, however, qualitative SRA is still very common. Yet, a lack of evidence of actual attacks with a terrorist background leads to inherent uncertainties regarding threat scenarios as well as the capabilities of security systems (Abrahamsen et al. 2015). As a result, SRA is often backed by only vague data or elicited expert knowledge that may represent a rather subjective perspective.

The occurrence of inherent uncertainties in risk assessment and decision-making is well known in the general fields of risk science and resilience, e.g., in Flage et al. (2014) and Aven and Zio (2021). In this context, especially the role of these uncertainties is discussed when considering decision-making for risk-reducing measures (Aven and Zio 2011; Yoe 2019). An earlier published study by Lichte and Wolf (2018) outlines consequences of considering uncertainties for qualitative methods in SRA that rely on expert knowledge.

Especially in SRA, the described inherent uncertainties have a potentially significant influence on the results and thus the possible outcome of occurring attacks. Here, the mere determination of qualitative or scalar values without considering the uncertain database or subjective expert knowledge for the characterization of security measures can lead to a fatal overestimation of the actual security level. Thus, the presented paper focuses on the impact of considering uncertainties in quantitative SRA, especially regarding the robustness of the system against resulting input parameter variance. Therefore, two levels of uncertainty can be distinguished: Firstly, the small basis of evidence, which increases uncertainty in the prediction of future attacks. Secondly, the performance of security measures against uncertain attackers, which can only be estimated at best. According to Milliken (1987), the aforementioned levels can be referred to as effect uncertainty (level 2) and response uncertainty (level 3), respectively. The impact of both levels is analyzed by applying an earlier approach to quantitative vulnerability assessment introduced by Lichte and Wolf (2017) as part of the SRA process to a notional airport structure.

Initially, we introduce a security measure configuration represented by probability density functions (pdfs) characterizing the performance of comprised components based on the subjective perspective of experts. Herein, the variance is a metric to describe uncertainties regarding measure efficiency in deterring potential attacks as a result from differing or vague expert opinions or scattered data. A first assessment only takes into account the mean values of normal probability density functions (npdfs), and thus uncertainties are not considered. Additionally, we assess the configuration incorporating given variances of the npdfs resulting from expert knowledge elicitation for uncertainty consideration. A comparison shows the influence on

the resulting vulnerability on system level. In a further step, we conduct a Variance Based Sensitivity Analysis (VBSA) as demonstrated by Saltelli et al. (2004) to quantify the influence of the introduced uncertainties on barrier level. Here, we analyze the influence of protection, observation and intervention measures on system vulnerability to reveal their potential impact on the effectiveness of the security system.

Based on this analysis, we propose and formalize a security margin. The concept of the security margin aims at the consideration of uncertainties introduced by either vague data or expert knowledge elicitation in SRA. By considering the systemic and barrier specific impact on security system effectiveness it is introduced to support optimized security system design. The security margin is derived in two steps. In a first step, the influencing security measures are identified by conducting a VBSA of the initial configuration of a security system. Then, the actual security margin is derived, only depending on the introduced uncertainty resulting from measure characterization and a reasonable target effectiveness based on efficiency considerations. Finally, we demonstrate the benefits of the approach for decision-making by optimizing the vulnerability of the initial configuration using the security margin concept.

2 Background

The issue of uncertainties in risk assessment is widely discussed within the general field of risk assessment, especially in the field of safety, e.g., by Fjaeran (2021) and Aven and Zio (2021). In recent years, risk science extended its scope further on risk management of complex systems facing greater hazards, i.e., natural extremes or man-made disasters, e.g., in Aven (2018). The consideration of uncertainty is even more important for these high impact low probability events, as their assessment often relies on vague data and information regarding likelihood of occurrence and temporal development.

This lack of knowledge, mostly referred to as epistemic uncertainty, may be considered critical for decision-making, as the development of a hazard scenario is decisive for its outcome. Thus, suited measures rely on little available information (Aven and Zio 2021). Within such scenarios, the rising number of attacks on critical infrastructures led to an increasing focus on security-related questions in business and sociopolitical decision-making, e.g., in Alcaraz and Zeadally (2015), Zsifkovits and Pickl (2016) and Guerra et al. (2008).

In actual security threat scenarios, faultily designed measures and miscalculated forecasts will, at least, lead to substantially larger damages at the asset under consideration. Threat scenarios missed out in system layout and deficient estimation of influence parameters result in misrepresentation of real situations (Campbell and Stamp 2004). This might lead to poor decisions in security investments. While in practice, qualitative methods are commonly used for the assessment, quantitative methods are developed in science and gain more advantages (Queirós et al. 2017). Such methods allow a better understanding of the interdependencies in security systems. Consequently, modeling of the behavior of entire security systems is feasible today, enabling analysis, optimization and simulation of the system (Meritt 1999).

Although quantitative methods may depend on the same vague data or expert knowledge as qualitative methods, they allow, however, to consider the resulting uncertainties explicitly, which may lead to a significantly different outcome of the analysis. Thus, quantitative methods can therefore bring decisive advantages in SRA. An improvement in security performance can be achieved by considering the uncertainties in analysis and design. Additionally, it potentially reveals to which extent large uncertainties, when taken into account, lead to cost-intensive over-optimization.

Despite potential problems in quantification, it is obviously important to consider uncertainties in SRA since they are likely to influence its results significantly, especially because the reliance on vague data or expert knowledge in SRA induces such uncertainties. Yet, it is reasonable to consider the input parameters by degree-of-belief-densities based on subjective probabilities, where probability distributions can be obtained by eliciting expert knowledge (EFSA 2014; Meyer and Booker 2001). In this way, representation of uncertainties is made possible while formally complying with probability theory (Beyerer and Geisler 2016).

Unfortunately, there are only few quantitative models considering uncertainties in security-related systems, e.g., the vulnerability assessment introduced by Lichte and Wolf (2017) or the approach introduced by McGill et al. (2007). The influence of these uncertainties on the SRA process is not yet analyzed. A first approach to analyze its impact on the output of a quantitative model was introduced by Lichte and Wolf (2018).

A framework proposed by Abrahamsen et al. (2015) considers uncertainties by including them into decision-making in security strategies. Depending on the grade of expected uncertainties and consequences, different strategies for decision-making are proposed. These strategies vary from extensive SRA at lower levels of uncertainty, precautionary approaches at medium levels of uncertainty to discursive style decisions. The last strategy should especially be adopted at high levels of uncertainty, e.g., when considering measures of counterterrorism, where cause-effect relationships are broadly discussed (van Dongen 2011).

For more complex quantitative models, uncertainty consideration can also be achieved by sensitivity analysis, which is used for assessing the influence of the input on the output of a system (Henkel et al. 2012). Within sensitivity analysis, the variability of the model inputs is related to the outputs with regard to their cause-and-effect chain. Thus, uncertainties of an output parameter are tracked back to the input. Especially if non-linear models are considered, the scattering of input and output factors is very challenging (Saltelli et al. 2004).

3 Methods and Exemplary Infrastructure

3.1 Variance Based Sensitivity Analysis

A procuring approach to analyze the influence of uncertainties is the conduction of Variance Based Sensitivity Analysis (VBSA) on the model under study. The VBSA was introduced by Saltelli et al. (2004) and is a numerical method to assess the relative importance of model input factors by measuring the sensitivity across the

complete input space. For this purpose, the effect of uncertainty in the output of a model is analyzed regarding different sources of uncertainty inputs (Henkel et al. 2012). The objective of this method is to find the parameters that have the largest impact on a predefined target function, e.g., the model output.

Within the scope of the presented approach, the numerical scenario analysis tool Monte Carlo Simulation (MCS), based on probability theory and statistics, is used with sampling based on Sobol sequences for realizing the VBSA (Saltelli et al. 2010). Within VBSA, total effect sensitivity indices $S_{\mathrm{T}i}$ are used to analyze linear and nonlinear effects of the input parameters $X_1, X_2, \ldots, X_k$ on the model output $Y = f(X_1, X_2, \ldots, X_k)$. For the i-th parameter, $S_{\mathrm{T}i}$ is defined as follows:

$$S_{\mathrm{T}i} = 1 - \frac{V_{\mathbf{X}_{\sim i}}\left(E_{X_i}\left(Y \mid \mathbf{X}_{\sim i}\right)\right)}{V(Y)} \tag{1}$$

$\mathbf{X}_{\sim i}$ refers to the sample matrix of all input parameters excluding the i-th parameter, E_{X_i} refers to the mean value taken over X_i and $V_{\mathbf{X}_{\sim i}}$ refers to the variance taken over all parameters but X_i.

In a combined risk assessment, e.g., for security-related investments, the interaction of the design parameters of the security system with regard to the interoperated risk might be very important for decision-making.

3.2 Applied Vulnerability Model

The vulnerability model applied in this paper is based on four basic assumptions, which characterize the most relevant behavior of a security system in an infrastructure (Lichte and Wolf 2017). These assumptions are used in the probabilistic description of the system's relations.

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 break-through 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 (see Fig. 1 (bottom)).

Considering the four stated principles, the model consists of three main input parameters that characterize the system capabilities provided by the installed security measures on barrier level: protection (P), observation (O) and intervention (I). Each of these parameters is described as a time-based probability density function (pdf). Capabilities are described as relations between these parameters. Figure 1 (top) shows the configuration of barriers along attack paths.

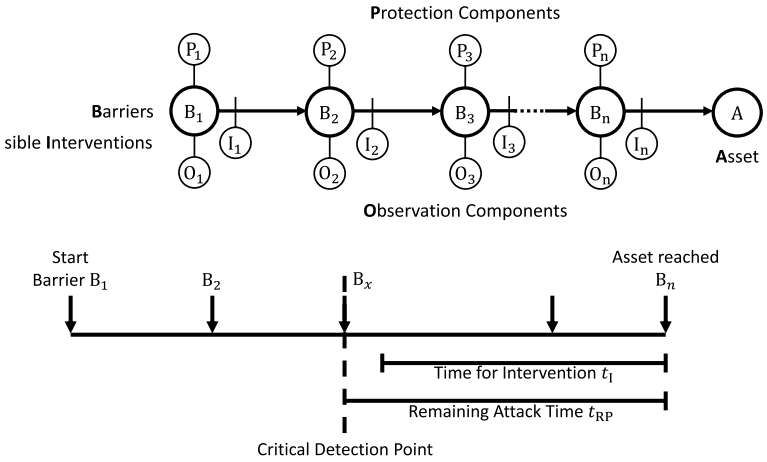

Fig. 1 Principle of security measures based on Garcia (2008). *Source*: Lichte and Wolf (2017)

A detection of an attacker is triggered if the protection measure at a barrier prevents an attacker from a break-through until an observation is completed with detection. This is described by the conditional probability D:

$$D = P(t_{\mathrm{O}} < t_{\mathrm{P}}) \tag{2}$$

Herein t_{P} and t_{O} denote the distributed time for protection and observation.

Timely intervention is the second key relation in the vulnerability model. It is based on the time needed for intervention t_{I} and the residual protection t_{RP}. The residual protection t_{RP} is the sum of all protection measures along the residual barriers of the system on an attack path.

$$t_{\mathrm{RP}} = \sum_{j=i}^{n} t_{\mathrm{P},j} - t_{\mathrm{O}i} \tag{3}$$

The conditional probability for timely intervention T is thus defined by:

$$T = P(t_{\mathrm{I}} < t_{\mathrm{RP}}) \tag{4}$$

Both main principles and the resulting relations between the pdfs of the incorporated parameters are shown in Fig. 2.

The vulnerability of a barrier V_{B} is then represented by

$$V_{\mathrm{B}} = 1 - D \cdot T \tag{5}$$

The product of the barrier-specific vulnerabilities leads to the vulnerability of the whole attack path V_{P}:

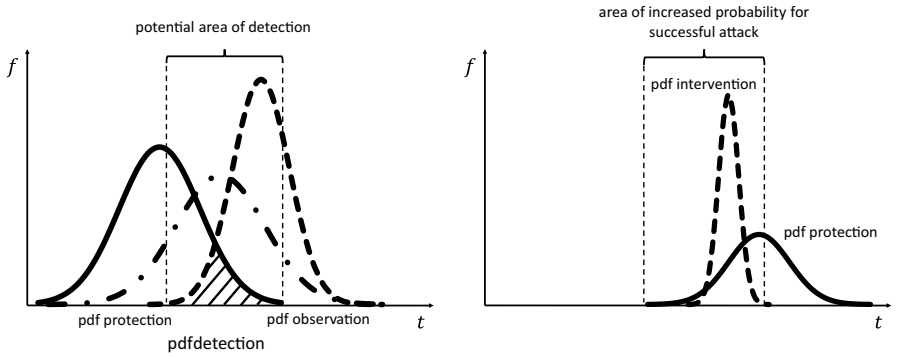

Fig. 2 Application of normal pdf (npdf) for t_P, t_O, t_I

$$V_P = \prod_{j=1}^{n} V_{B,j} \tag{6}$$

Referring to the first assumption, the system vulnerability V_S is determined by the weakest path:

$$V_S = \max(V_{P,1}, \ldots, V_{P,m}) \tag{7}$$

In case of numerical sampling, e.g., Monte Carlo, we reformulate the definition of system vulnerability due to the binary characteristic of path vulnerability at each sample. At a sample, the system is defined to be vulnerable, when any path is vulnerable. The mean of all samples then describes the overall system vulnerability.

3.3 Exemplary Airport Structure and Security System

The airport system and the identified security barriers are depicted in Fig. 3. Additionally, the figure outlines feasible attack paths within this structure. The structure is based on a notional airport which was subject to a security risk assessment in Lichte and Wolf (2017).

4 The Impact of Uncertainties in Security Vulnerability Assessment

In this section, we show how uncertainties influence the results of vulnerability assessment. For this purpose, we analyze an initial configuration of the introduced notional airport structure regarding general model sensitivity to added variance on system parameters. The initial configuration is described in Table 1. The defined values are assumed to be the result of expert knowledge elicitation. Subsequently, we quantify the monitored impact on barrier level by applying a VBSA on all input parameters characterizing the capabilities of the security system.

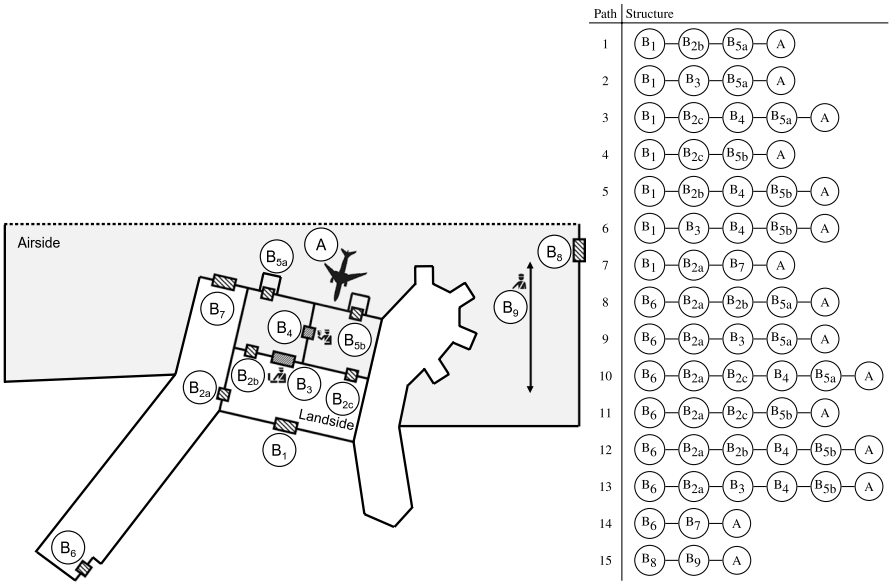

Fig. 3 Notional airport structure with feasible attack path, based on: Lichte and Wolf (2017)

Table 1 Initial configuration of notional airport security system

Barrier	t_P		t_O		t_I	
	μ_P (s)	σ_P(s)	μ_O(s)	σ_O(s)	μ_I(s)	σ_I(s)
2a	120	18	100	15	172	21
2b	120	18	100	15	115	18
2c	120	18	100	15	115	18
3	108	18	90	15	115	18
4	36	6	30	6	115	18
5a	144	24	120	18	115	18
5b	144	24	120	18	115	18
6	288	45	240	36	172	27
7	216	33	180	27	172	27
8	216	33	180	27	288	75
9	360	54	300	45	288	45

4.1 Impact of Uncertainties on System Vulnerability

In this analysis, we initially replace the pdfs with scalars to describe the performance of security measures without changing the basic barrier-oriented structure. Thus, the parameters are fully described by the mean values: $t_{Pi} = \mu_{Pi}$, $t_{Oi} = \mu_{Oi}$ and $t_{Ii} = \mu_{Ii}$ (compare Table 1).

In a second assessment, we additionally add the uncertainty regarding the security measure performance at the single barriers represented by the variance σ^2. Table 1 shows the npdf-based values for the respective system parameters. It should be noted that we assume that no security measures are associated with barrier 1. Hence, it is excluded from the assessment.

With the now established npdfs for t_{Pi}, t_{Oi} and t_{Ii}, we conduct a re-assessment of the vulnerability considering the added uncertainties. For this purpose, we compute the vulnerability by MCS. The obtained results for both assessments are listed in Table 2.

The weakest path determines the system vulnerability V_S. We calculate the results for both cases: $V_{S,nv}$ for no variance consideration and $V_{S,v}$ using the npdfs.

$$V_{S,nv} = 0 \tag{8}$$

$$V_{S,v} = 0.811 \tag{9}$$

The assessment of the vulnerabilities of the feasible attack paths, as well the system vulnerability for both versions, reveals highly variable results. The difference in $V_{S,nv}$ and $V_{S,v}$ on system level is solely caused by the introduced uncertainties, since the vulnerability model and the mean values of the input parameters remain unchanged. Thus, estimation and consideration of uncertainties is important, as system layout based on scalars can lead to misleading results, which can lead to fatal decisions. Additionally, a more detailed understanding of the uncertainty impact is needed for a rational and cost-efficient security system layout. For this reason, we carry out further analyses on barrier and parameter level in the next section.

Table 2 Path vulnerabilities with and without uncertainty consideration

Path	V_P	
	No variance	Variance
1	0	0.234
2	0	0.260
3	0	0.065
4	0	0.235
5	0	0.065
6	0	0.073
7	0	0.233
8	0	0.010
9	0	0.011
10	0	0.003
11	0	0.010
12	0	0.003
13	0	0.003
14	0	0.222
15	0	0.282

4.2 Uncertainty Impact Assessment on Barrier Level

In this step, we analyze which uncertain parameters impact system vulnerability. By applying a VBSA, we reveal the influence of all parameters on barrier level. For this purpose, we investigate the total effect sensitivity indices S_{Ti} of the model output V_S to the input parameters t_{Pi}, t_{Oi} and t_{Ii}. By generating samples based on Sobol sequences and calculating the sensitivity indices using the software SALib (Herman and Usher 2017), we obtain the results for all input parameters of the optimized configuration shown in Table 3.

On the one hand, the results reveal that the uncertainty added to some of the input factors does not have an impact on the model output of system vulnerability, as the total effect sensitivity indices are zero or near zero, e.g., all input factors at barrier 4. On the other hand, the uncertainty of some input factors seems to have an impact on the results, e.g., at the barriers 2a, 2b, 2c, 3, 6 and 8. However, it can be concluded that uncertain parameters for security measures only have an impact on certain points, i.e., barriers within a security system.

5 Approach Toward a System Layout Considering Uncertainty

In this section, we propose an approach that optimizes system security by considering the influence of uncertainties analyzed in Sect. 4. For this reason, we introduce a security margin concept that is set up in two consecutive steps. In a first step, we argue to use the VBSA-based total effect sensitivity indices S_{Ti} to identify barriers and security measures relevant for optimization. In a second step, we derive a security margin for the performance of the identified measures to account for associated uncertainties. The process is run successively for detection and intervention capabilities. As security margins applied to protection or observation measures change the residual protection on certain attack paths (see Eq. 3), the sequence enables optimized adjustment of the security margin for intervention measures. The security margins for all measures are

Table 3 Total effect sensitivity indices S_{Ti} for all parameters

Barrier	$S_{T,P}$	$S_{T,O}$	$S_{T,I}$
2a	0.199	0.168	0.032
2b	0.198	0.166	0.035
2c	0.209	0.171	0.035
3	0.219	0.180	0.035
4	0.001	0.001	0.001
5a	0.091	0.002	0.002
5b	0.057	0.001	0.000
6	0.204	0.161	0.018
7	0.063	0.002	0.002
8	0.217	0.177	0.107
9	0.079	0.001	0.001

based only on the characteristics of the involved pdfs and a targeted level for detection and timely intervention capability. We additionally demonstrate the possible correlation between effort needed to consider uncertainties and achievable security level which becomes visible through this approach. This can be used for further assessment of optimization efficiency.

5.1 Step 1: Variance Influence Assessment on Measure Performance at Barrier Level

A rational optimization of security systems should consider the boundary conditions of feasibility, cost-benefit ratio and financial budget constraints. A sensitivity analysis, especially a VBSA for nonlinear systems, is a reasonable first step for cost-benefit considerations, as it provides qualitative knowledge about the influence of system's variables on its output. Hence, influencing variables can be identified and chosen for further optimization to concentrate resources and thus maximize their benefit.

Here, we use the VBSA as shown in Sect. 4.2 to find input parameters that influence the system vulnerability by comparing the calculated total effect sensitivity indices $S_{\mathrm{T}i}$.

5.2 Step 2: Security Margin Definition

Identified influencing security measures are optimized to improve the overall security system performance in the second step. This is reached by adding a security margin M considering the uncertainty, i.e., the variance of the characterizing pdfs. The new parameters for protection $t_{\mathrm{P}i}^*$ and intervention $t_{\mathrm{I}i}^*$ are then given as follows:

$$t_{\mathrm{P}i}^* = t_{\mathrm{P}i} + M_{\mathrm{P}i}\left(\sigma_{\mathrm{P}i}, \sigma_{\mathrm{O}i}, D_i^*\right) \tag{10}$$

$$t_{\mathrm{I}i}^* = t_{\mathrm{I}i} - M_{\mathrm{I}i}\left(\sigma_{\mathrm{I}i}, \sigma_{\mathrm{RP}i}, T_i^*\right) \tag{11}$$

Herein, σ^2 marks the variance of the respective pdf at the i-th barrier. D_i^* and T_i^* describe a targeted level of probability for detection and timely intervention at barrier i, respectively.

The definition of M depends on the underlying pdfs used to describe the performance of the security measures. Based on the level of knowledge, different pdfs may be suitable, e.g., uniform, triangular or normal distributions. The derivation of M for normal distributions is described in the following based on mean and variance of measure performance as well as the targeted level of the dependent capability. Here, we restrict ourselves to normal distributions, since these are mathematically straightforward to handle.

For all distribution types, the starting point is derived from Eqs. 2, 4, 10 and 11, respectively:

$$D^* = P(t_{\mathrm{O}} < t_{\mathrm{P}} + M_{\mathrm{P}}) \tag{12}$$

$$T^* = P(t_\mathrm{I} - M_\mathrm{I} < t_\mathrm{RP}) \tag{13}$$

As shown in Lichte and Wolf (2017), D and T can be expressed by pdfs, here extended to include the security margin:

$$D^* = \int_{-\infty}^{\infty} f_\mathrm{O}(t) \int_{t}^{\infty} f_\mathrm{P}(\tau - M_\mathrm{P})\,\mathrm{d}\tau\,\mathrm{d}t \tag{14}$$

$$T^* = \int_{-\infty}^{\infty} f_\mathrm{I}(t + M_\mathrm{I}) \int_{t}^{\infty} f_\mathrm{RP}(\tau)\,\mathrm{d}\tau\,\mathrm{d}t \tag{15}$$

Herein, f_RP is obtained by consecutively convoluting the pdfs for protection of the remaining barriers on the attack path. Additionally, we used the following definition to treat the distributed time for first observation at barrier i:

$$(f \bar{*}\, g)(t) := \int_{-\infty}^{\infty} f(\tau)\, g(\tau - t)\,\mathrm{d}\tau \tag{16}$$

Hence, we obtain:

$$f_\mathrm{RP}(t) = \left(f_{\mathrm{P}i} * \cdots * f_{\mathrm{P},n} \bar{*} f_{\mathrm{O}i}\right)(t) \tag{17}$$

For npdfs parametrized by mean μ and variance σ^2, the security margin for protection M_P follows from Eq. 14:

$$M_\mathrm{P} = \mu_\mathrm{O} - \mu_\mathrm{P} - \sqrt{2\left(\sigma_\mathrm{O}^2 + \sigma_\mathrm{P}^2\right)} \cdot \mathrm{erf}^{-1}(1 - 2D^*) \tag{18}$$

Herein, erf^{-1} refers to the inverse error function.

Analogously, M_I follows from Eq. 15. Since the residual protection time t_RP is the result of the convolution of npdfs (Eq. 17), t_RP is normally distributed as well:

$$M_\mathrm{I} = \mu_\mathrm{I} - \mu_\mathrm{RP} - \sqrt{2\left(\sigma_\mathrm{I}^2 + \sigma_\mathrm{RP}^2\right)} \cdot \mathrm{erf}^{-1}(1 - 2T^*) \tag{19}$$

The distribution parameters for t_RP are:

$$\mu_\mathrm{RP} = \sum_{j=i}^{n} \mu_{\mathrm{P},j} - \mu_{\mathrm{O}i} \tag{20}$$

$$\sigma_\mathrm{RP}^2 = \sum_{j=i}^{n} \sigma_{\mathrm{P},j}^2 + \sigma_{\mathrm{O}i}^2 \tag{21}$$

It should be noted that detailed optimization of the introduced security margins requires an enhanced cost-benefit assessment using cost functions. However, without an underlying cost function, the ratio between effort and benefit regarding the capabilities of detection and timely intervention depends on the distribution used for description. Figure 4 shows this relation for the introduced npdf in the detection

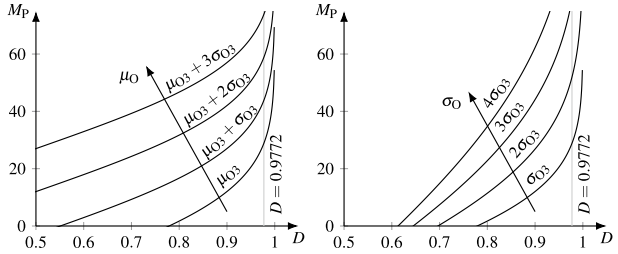

Fig. 4 Security margin as a function of target detection level for barrier 3 and varying distribution parameters of observation time

mechanism. It reveals that the needed security margin M_P grows nearly linearly with rising target detection probability level D^* where the influence of the inverse error function in Eq. 18 is limited. Congruent to the curve shape of npdf, the size of the security margin sharply rises, when $D^* > P(x < \mu + 2\sigma) \approx 97.72\,\%$ is required. This implies a direct dependence of the security margin on the variance σ^2 of the respective npdfs that characterize security measure performance depending on the available level of data or knowledge. The shown dependency can be used for a first efficiency estimation of efforts needed to consider existing uncertainties.

The graphs for higher variances in Fig. 4 underline that higher levels of variance, i.e., the uncertainty regarding measure performance, cannot efficiently be tackled by consideration in security margins when the required target level for detection probability is high. This can also be seen in Eq. 18 since detection probability is a factor of the variances through the inverse error function. For this case, an upstream reduction of uncertainties appears necessary.

6 Exemplary Solution for Notional Airport Structure

In the following, we evaluate the introduced security margin approach by applying it to the notional airport infrastructure introduced in Sect. 4. For this purpose, we follow the process outlined in Sect. 5 and set up a new configuration of the security system using calculated security margins. Subsequently, we assess the vulnerability of the newly defined configuration.

Based on the relation between security margin and target level required for detection or timely intervention probability shown in Sect. 5.2, we choose the following values for probability of attacker detection D_i^* and timely intervention T_i^*, respectively:

$$D_i^* = 97.72\,\% \tag{22}$$

$$T_i^* = 97.72\,\% \tag{23}$$

Table 4 Identified barriers and protection measures

Barrier	μ_P (s)
2a	120
2b	120
2c	120
3	108
6	288
8	216

Table 5 Security margins applied to protection measure parameters

Barrier	μ_P (s)	M_P(s)	μ_P^* (s)
2a	120	26.8	146.8
2b	120	26.8	146.8
2c	120	26.8	146.8
3	108	28.8	136.8
6	288	67.2	355.2
8	216	49.2	265.2

6.1 Security Margin for Measures of Detection

6.1.1 Step 1: Assessment of Influencing Variance

In a first next step, barriers with high total effect sensitivity index S_{Ti} (see Table 3) are chosen from the results of the VBSA carried out in Sect. 4.2 for security margin definition. The protection measures with the respective protection times t_{Pi} at the barriers shown in Table 4 are subject of further considerations.

6.1.2 Step 2: Derivation of Security Margin

In the second step, we calculate the security margin for the protection measures identified in the first step by applying the values of the initial configuration given in Table 1 to Eq. 18. For instance, for barrier 8 we get:

$$M_P = 180\,\mathrm{s} - 216\,\mathrm{s} - \sqrt{2 \cdot \left(27^2\,\mathrm{s}^2 + 33^2\,\mathrm{s}^2\right)} \cdot \mathrm{erf}^{-1}(1 - 2 \cdot 0.9772) = 49.2\,\mathrm{s} \tag{24}$$

The results for all considered barriers are given in Table 5. Note that the values with added security margin μ_{Pi}^* are further used for the definition of the security margin for timely intervention.

6.2 Security Margin for Measures of Timely Intervention at Barrier Level

6.2.1 Step 1: Assessment of Influencing Variance

Based on the updated configuration incorporating the security margin for the protection measures defined in Table 5, we additionally revise the security system to incorporate the remaining influence of uncertainties on timely intervention. Thus, we conduct a new VBSA and revise the remaining total effect sensitivity indices for intervention measures $S_{\mathrm{T,I}}$. The results are given in Table 6.

Our results for $S_{\mathrm{T,I}}$ show the influence of intervention measures at barrier 8. In order to identify the weakest path, where vulnerability is influenced by the uncertainties at barrier 8, we additionally break down its influence on attack path level. Table 7 reveals attack path 14 is the only influenced path on which barrier 8 and 9 shape the residual protection distribution (compare Fig. 3).

6.2.2 Step 2: Derivation of Security Margin

The security margin for the remaining influence of barrier 8 on timely intervention is calculated by inserting the respective values from Tables 1 and 5 into Eq. 19. We then obtain:

$$M_{\mathrm{I}} = 288\,\mathrm{s} - (265.2\,\mathrm{s} + 360\,\mathrm{s} - 180\,\mathrm{s}) - \sqrt{2 \cdot \left(75^2\,\mathrm{s}^2 + 33^2\,\mathrm{s}^2 + 54^2\,\mathrm{s}^2 + 27^2\,\mathrm{s}^2\right)} \cdot \mathrm{erf}^{-1}(1 - 2 \cdot 0.9772) = 46.2\,\mathrm{s} \tag{25}$$

The added security margin for the intervention measure at barrier 8 is listed in Table 8.

Table 6 Total effect sensitivity indices $S_{\mathrm{T},i}$ for all parameters with applied M_{P}

Barrier	$S_{\mathrm{T,P}}$	$S_{\mathrm{T,O}}$	$S_{\mathrm{T,I}}$
2a	0.121	0.105	0.049
2b	0.124	0.107	0.050
2c	0.125	0.107	0.048
3	0.125	0.108	0.047
4	0.002	0.000	0.000
5a	0.118	0.001	0.000
5b	0.066	0.001	0.000
6	0.105	0.085	0.017
7	0.091	0.001	0.000
8	0.159	0.136	0.194
9	0.146	0.000	0.000

Table 7 Total effect sensitivity indices $S_{\mathrm{T}i}$ for influence of intervention at barrier 8 on path vulnerability V_{P}

Path	$S_{\mathrm{T,I8}}$
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0.598

Table 8 Security margins applied to intervention measure parameters

Barrier	μ_{I} (s)	M_{I} (s)	μ_{I}^{*} (s)
8	288	46.2	241.8

6.3 Vulnerability Assessment

Finally, we assess the vulnerability of the new configuration according to the procedure given in Sect. 4.1 and compare it to the initially analyzed security system. Table 9 compares path vulnerability of the initial configuration with that resulting from the application of security margins, one time with M_{P} only and one time with both M_{P} and M_{I}.

We calculate the system vulnerability $V_{\mathrm{S,v}}^{*}$ for the newly created system with security margins and compare it to the initial configuration considering variance $V_{\mathrm{S,v}}$:

$$V_{\mathrm{S,v}} = 0.811 \tag{26}$$

$$V_{\mathrm{S,v}}^{*} = 0.210 \tag{27}$$

The results show that the vulnerability of the new configuration is at a low level. Additionally, the comparison to the initial configuration shows that system vulnerability is significantly minimized induced by the application of the security margins. As the total effect sensitivity indices $S_{\mathrm{T}i}$ reveal an impact of added variance or uncertainty, we can use this result to establish a new configuration subjecting only influencing factors to a security margin M. Non-influencing parameter values are kept from the initial configuration. The resulting configuration for our exemplary system containing the security margins is summarized in Table 10.

Table 9 Comparison of path vulnerabilities for configurations with and without security margins

Path	V_P		
	Initial	M_P	M_P, M_I
1	0.235	0.040	0.040
2	0.260	0.040	0.040
3	0.065	0.008	0.008
4	0.235	0.040	0.040
5	0.065	0.008	0.008
6	0.073	0.008	0.008
7	0.232	0.042	0.042
8	0.009	0.000	0.000
9	0.011	0.000	0.000
10	0.003	0.000	0.000
11	0.009	0.000	0.000
12	0.003	0.000	0.000
13	0.003	0.000	0.000
14	0.221	0.029	0.029
15	0.282	0.078	0.042

Table 10 Configuration of notional airport security system containing security margin

Barrier	t_P		t_O		t_I	
	μ_P (s)	σ_P (s)	μ_O (s)	σ_O (s)	μ_I (s)	σ_I (s)
2a	146.8	18	100	15	172.0	21
2b	146.8	18	100	15	115.0	18
2c	146.8	18	100	15	115.0	18
3	136.8	18	90	15	115.0	18
4	36.0	6	30	6	115.0	18
5a	144.0	24	120	18	115.0	18
5b	144.0	24	120	18	115.0	18
6	355.2	45	240	36	172.0	27
7	216.0	33	180	27	172.0	27
8	265.2	33	180	27	241.8	75
9	360.0	54	300	45	288.0	45

7 Discussion

The analysis carried out in this paper demonstrates how the quantitative approach to SRA can be useful to take uncertainties into account, even if the data situation is vague or the assessment is based only on expert knowledge. Given this, we present an approach that aims to minimize the influence of uncertainties, i.e., the lack of knowledge regarding the performance of security measures, in security system design by using quantitative methods in a targeted manner.

Our analysis shows that the difference between scalar and distribution based vulnerability assessment can be significant. In the example used, the introduced uncertainties lead to a significant rise in vulnerability. Thus, we show that the uncertainty regarding the knowledge of security measure performance may severely influence the results of a SRA and, even more important, the outcome of possible attacks. By applying VBSA to the analyzed security system, we reveal that the influence of the uncertainties is limited to few security barriers and measures within the system in this case. As the underlying vulnerability model is nonlinear, a total effect sensitivity index S_{Ti} gives insight about direct and indirect influence of the analyzed variable and the respective security measure.

The proposed security margin concept aims at tackling the aforementioned influences in security system (re-)configuration. The derivation of the security margin involves two steps that are consecutively conducted for the fundamental capabilities of detection and timely intervention. First, by applying a VBSA, influential security measures are identified. In a second step, the security margin itself is calculated dependent on solely the size of the introduced uncertainty of the measure and target levels for detection and timely intervention. It should be noted that we establish the security margin concept for npdf-based description of security measure performance resulting from expert knowledge in this paper. The formalization for other reasonable pdfs, e.g., equal or triangular distribution, is similar in principal but requires additional computational effort. However, the demonstrated relation of target measure effectiveness and distribution variance, i.e., the introduced uncertainties, can be used to support efficiency considerations.

In the case of npdf, we show that the effort needed to increase the target effect efficiency increases sharply at $P(x < \mu + 2\sigma) \approx 97.72\,\%$. The efficiency estimate for higher variances shows that large uncertainties regarding the properties of security measures entail fundamental problems. On the one hand, taking these uncertainties into account in the system design does not appear to be efficient, since disproportionate effort must be expended to ensure a sufficient security margin. On the other hand, the result shows that poor quality of the input data used, be it a vague data base or expert knowledge, may limit the informational value of the evaluation as well as the proposed security margin concept to the extent that poor (vague) input data lead to questionable results —a valuable insight that is hardly obtained from qualitative methods.

This strongly suggests that the consideration of uncertainties by the security margin is not sufficient for this case. Here, a reduction of the corresponding variances seems necessary first. This could potentially be tackled by a further evaluation of the implemented security measures in real-world tests aiming to decrease the input uncertainty by enhancing the database.

The evaluation of the security margin concept using the airport example illustrates its usefulness in principle. By taking into account the uncertainties based on expert knowledge, only the barriers with influence are provided with a security margin in a modified configuration. A following vulnerability assessment supports the assumption regarding the differing influence of input parameters. The significant reduction of system vulnerability shows the effectiveness of the security margin in reducing the influence of uncertainties on system performance.

8 Conclusion

In this paper, we show the usefulness of the quantitative approach in SRA. This is particularly evident in the use of a vague database or expert knowledge, which is common in security assessment. Unlike qualitative analysis, quantitative analysis allows for consideration of uncertainty.

The analysis carried out in the paper shows the potentially large impact of these uncertainties, represented by variances in pdfs, on the outcome of the SRA and the outcome of possible attacks on the system under consideration. A VBSA shows that this influence can be attributed to certain barriers for the selected configuration. Based on these results, we propose the concept of security margin, in which targeted changes to influential barriers that take into account the uncertainties resulting from, for example, vague data or expert knowledge.

Generally, in SRA sufficient attention should be paid to the level of effect uncertainty and resulting consequences. According to Abrahamsen et al. (2015), potentially severe consequences should lead to precautionary approaches. Here, the introduced security margin can be used for a corresponding security system layout. The introduced formalization supports basic efficiency considerations as well as enhanced optimization methods. However, the results suggest that in the case of large uncertainties, their reduction should be sought first. For this purpose, additional investigation of the security margin concept and its limits is needed. Additionally, the security margin concept should be formalized for different pdfs for carving out additional limitations. For enhanced applicability, the problems of non-continuous change of performance between implementable security measures and dependent financial efforts should be included, thus enabling enhanced cost-benefit analysis and optimization.

In summary, the understanding and consideration of the described inherent levels of uncertainty in effect and response in SRA is important, since their influence on the outcome of analysis and its validity is potentially significant. The proposed security margin concept is a feasible way to cope with such uncertainties by methodical identification and targeted limitation of their influence on vulnerability of security systems.

Authors' contributions The contributions of all authors must be described in the following manner: Theauthors confirm contribution to the paper as follows: DL: Conception or design of the work, data analysis and interpretation,drafting the article, critical revision of the article, final approval of the version to bepublished. DW: data analysis and interpretation, critical revision of the article, finalapproval of the version to be published. TT: critical revision of the article, final approval of the version to bepublished. KDW: critical revision of the article, final approval of the version tobe published.

Funding Open Access funding enabled and organized by Projekt DEAL.

Availability of data and material No additional data available.

Code availability Available on request.

Declarations

Conflict of interest The authors declared that they have no conflict of interest.

References

Abrahamsen EB, Pettersen K, Aven T, Kaufmann M, Rosqvist T (2015) A framework for selection of strategy for management of security measures. J Risk Res 20(3):1–14. https://doi.org/10.1080/13669877.2015.1057205

Alcaraz C, Zeadally S (2015) Critical infrastructure protection: requirements and challenges for the 21st century. Int J Crit Infrastruct Prot 8:53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Aven T (2018) The call for a shift from risk to resilience: what does it mean? Risk Anal 39:1196–1203. https://doi.org/10.1111/risa.13247

Aven T, Zio E (2011) Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliab Eng Syst Saf 96:64–74. https://doi.org/10.1016/j.ress.2010.06.001

Aven T, Zio E (2021) Globalization and global risk: how risk analysis needs to be enhanced to be effective in confronting current threats. Reliab Eng Syst Saf. https://doi.org/10.1016/j.ress.2020.107270

Beyerer J, Geisler J (2016) A framework for a uniform quantitative description of risk with respect to safety and security. Eur J Secur Res 1:135–150. https://doi.org/10.1007/s41125-016-0008-y

Campbell PL, Stamp JE (2004) A classification scheme for risk assessment methods. Technical Report. SAND2004-4233, Sandia National Laboratories.https://doi.org/10.2172/925643

EFSA (2014) Guidance on expert knowledge elicitation in food and feed safety risk assessment. EFSA J. https://doi.org/10.2903/j.efsa.2014.3734

Fjaeran AL (2021) Creating conditions for critical trust—how an uncertainty-based risk perspective relates to dimensions and types of trust. Saf Sci. https://doi.org/10.1016/j.ssci.2020.105008

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 Anal. https://doi.org/10.1111/risa.12247

Flammini F, Marrone S, Mazzocca N, Vittorini V (2013) Petri net modelling of physical vulnerability. In: Bologna S, Hämmerli B, Gritzalis D, Wolthusen S (eds) Critical information infrastructure security, vol 6983. Lecture notes in computer science. Springer, Berlin, pp 128–139. https://doi.org/10.1007/978-3-642-41476-3_11

Garcia ML (2008) The design and evaluation of physical protection systems, 2nd edn. Elsevier, Amsterdam. https://doi.org/10.1016/C2009-0-25612-1

Guerra L, Murino T, Romano E (2008) Airport system analysis: a probabilistic risk assessment model. Int J Syst Appl Eng Dev 2:52–65

Henkel T, Wilson H, Krug W (2012) Global sensitivity analysis of nonlinear mathematical models—an implementation of two complementing variance-based algorithms. In: Proceedings of the 2012 winter simulation conference. Institute of Electrical and Electronics Engineers.

Herman J, Usher W (2017) Salib: an open-source python library for sensitivity analysis. J Open Source Softw 2(9):11–15. https://doi.org/10.21105/joss.00097

Landucci G, Argenti F, Cozzani V, Reniers G (2017) Quantitative performance assessment of physical security barriers for chemical facilities. In: Čepin M, Briš R (eds) Safety and reliability. CRC Press, Leiden

Lichte D, Wolf KD (2017) Quantitative multiple-scenario vulnerability assessment applied to a civil airport infrastructure. In: Čepin M, Briš R (eds) Safety and reliability. CRC Press, Leiden

Lichte D, Wolf KD (2018) A study on the influence of uncertainties in physical security risk analysis. In: Barros A, van Gulijk C, Haugen S, Vinnem JE, Kongsvik T (eds) Safety and reliability. CRC Press, Leiden, p 28. https://doi.org/10.1201/9781351174664-175

McGill WL, Ayyub BM, Kaminskiy M (2007) Risk analysis for critical asset protection. Risk Anal Int J 27(5):1265–1281. https://doi.org/10.1111/j.1539-6924.2007.00955.x

Meritt JW (1999) A method for quantitative risk analysis. In: Proceedings of the 22nd national information systems security conference (NISSC)

Meyer MA, Booker JM (2001) Eliciting and analyzing expert judgment. ASA-SIAM series on statistics and applied mathematics. Society for Industrial and Applied Mathematics.https://doi.org/10.1137/1.9780898718485

Milliken FJ (1987) Three types of perceived uncertainty about the environment: state, effect, and response uncertainty. Acad Manag Rev 12(1):133–143. https://doi.org/10.5465/amr.1987.4306502

Queirós A, Faria D, Almeida F (2017) Strengths and limitations of qualitative and quantitative research methods. Eur J Educ Stud 3(9):369–387

Saltelli A, Tarantola S, Campolongo F, Ratto M (2004) Sensitivity analysis in practice. A guide to assessing scientific models. Wiley, Chichester

Saltelli A, Annoni P, Azzini I, Campolongo F, Ratto M, Tarantola S (2010) Variance based sensitivity analysis of model output design and estimator for the total sensitivity index. Comput Phys Commun 181(2):259–270. https://doi.org/10.1016/j.cpc.2009.09.018

van Dongen TW (2011) Break it down: an alternative approach to measuring effectiveness in counterterrorism. J Appl Secur Res 6(3):357–371. https://doi.org/10.1080/19361610.2011.580264

Yoe C (2019) Primer on risk analysis. Decision making under uncertainty, 2nd edn. CRC Press, Boca Raton. https://doi.org/10.1201/9780429021145

Zsifkovits M, Pickl S (2016) Strategic risk management in counter-terrorism for the railbound public transport. In: Proceeding of international conference on security and management

Authors and Affiliations

Daniel Lichte[1] · Dustin Witte[2] · Thomas Termin[2] · Kai-Dietrich Wolf[2]

✉ Daniel Lichte
daniel.lichte@dlr.de

[1] Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Sankt Augustin, Germany

[2] Institute for Security Systems, University of Wuppertal, Wuppertal, Germany