On the Impact of Uncertainty on Quantitative Security Risk Assessment

Daniel Lichte

Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: thomas.termin@uni-wuppertal.de

Kai-Dietrich Wolf

Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

The importance of (physical) security nowadays gets more and more acknowledged in society as well as in the scientific community. In the light of increasing terrorist threat levels, assessments of the security of critical infrastructures are conducted in practice and researchers propose new approaches. While practical security risk assessments (SRA) use mostly qualitative methods, most of the lately proposed approaches are based on quantitative metrics. Rare evidence of actual attacks qualitative and quantitative approaches suffers the fundamental problem of inherent uncertainties regarding occurring threats and capabilities of security measures. This paper focuses on the impact of considering uncertainties in quantitative SRA, especially regarding the robustness of the system against resulting input parameter variance. The impact is analyzed by applying quantitative vulnerability assessment introduced by Lichte and Wolf (2017) as part of the SRA process to an airport structure. Two differing configuration are initially assessed. Additionally, an adapted Variance Based Sensitivity Analysis for first and total order sensitivities is conducted. Finally, a hybrid configuration based on the findings of the prior steps is realized in the sixth step. The results substantiate the assumption regarding the differing influence of the models input parameters. Hence, the approach of Factor Fixing can help in systematically identifying the most influencing factors of the uncertainty considering vulnerability model.

Keywords: Security, Uncertainty, Security Risk Assessment, Vulnerability, Critical Infrastructures, CIP, Variance Based Sensitivity Analysis.

1. Introduction

The importance of (physical) security nowadays gets more and more acknowledged in society as well as in the scientific community. In the light of increasing terrorist threat levels, assessments of the security of critical infrastructures are conducted in practice and researchers propose new approaches. While practical security risk assessments (SRA) use mostly qualitative methods, most of the lately proposed approaches are based on quantitative metrics, e.g. Flammini et al. (2013); Landucci et al. (2017). However, due to rare evidence of actual attacks qualitative and quantitative approaches suffer the fundamental problem of inherent uncertainties regarding occurring threats and capabilities of security measures. An earlier published study by Lichte and Wolf (2018) outlines consequences of considering uncertainties for qualitative methods in SRA.

This 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 makes prediction of future attacks uncertain. Secondly, the performance of security measures against uncertain attackers, which can only be estimated at best. According to Miliken (1987), they 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 an airport structure. A cost optimized and a conservative security configuration using security margins are initially assessed. Additionally, an adapted Variance Based Sensitivity Analysis (VBSA) as shown by Saltelli et al. (2007) is conducted. The results of the VBSA are compared regarding the robustness of the configurations. Finally, the results are discussed considering the influence of uncertainties on the design and optimization of security systems as well as implications on the validity of assessments. Thus, it is described,

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

how the approach can be used to support decision-making by using the above-described levels of uncertainty for optimized allocation of resources within a security system. Additionally, approaches to minimize uncertainty in the assessment process are proposed to tackle this challenge.

2. Background

Due to the increasing number of attacks on critical infrastructures, security-related questions increasingly get in the midst of business and sociopolitical decisions (Alcaraz and Zeadally 2014). Miscalculated taken measures and forecasts will possibly lead at worst to sustained larger damages. Not considered threat scenarios in the system layout and a wrong estimation of influence parameters result in the miscalculation of the real situation (Campbell and Stamp 2004). This might cause bad 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 (Almeida et al. 2017). Assessments that are more objective are possible using quantitative approaches because they rely less on expert knowledge. Moreover, such methods allow a better understanding of the interoperation in security systems. Consequently, the modeling of the behavior of whole security systems is possible so that next to the modeling and quantification, an analytic optimization and a simulation of the system are enabled (Meritt 2008).

When considering uncertainties in SRA a fundamental issue is the classic definition of security risk as a product of the triplet of threat, vulnerability and consequence. This classic definition recently came under discussion, as it is apparently only valid for statistically independent probabilities (Amundrud et al. 2017). In SRA this cannot be assumed, since at least threat and vulnerability are fraught with uncertainty. Thus, it is reasonable to consider the input parameters as degree-of-belief-densities based on Bayesian probability theory. In this way, consideration of uncertainties is made possible being formally in accordance with established probability theory (Beyerer and Geisler 2016).

Despite potential problems in quantifying uncertainties, it is obviously important to consider them in SRA because of their eventual influence on its results. However, there are only a 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). However, 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). In the case of very complex models with lots of input parameters, numerical methods, such as the sensitivity analysis, are used for assessing the influence of the input on the output of a system (Henkel et al 2012). Within a sensitivity analysis, the variability of the model inputs is related to the outputs with regard to their cause-and-effect chain. In doing so, individual parameters are varied specifically. Thus, uncertainties of an output parameter are led back to the input. For investment decisions, the input factors who are uncertain are the most important ones because their value lie within an interval that allows no clear statement about their actual status (Saltelli et al. 2007). Especially if non-linear models with conditions are considered, the scattering of input and output factors is very challenging. Not least because of time-limited and financial restricted resources, risk-reducing measures have to be taken wisely (Saltelli et al. 2007).

A framework proposed by Abrahamsen et al. (2015) considers uncertainties by including them into decision-making in security strategies. Depending on the level of expected uncertainties and consequences, different strategies for decision-making are proposed. These strategies vary from extensive SRA at lower uncertainties, precautionary approaches at a medium level 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 even cause-effect relationships are discussed in greater depth (Dongen 2009).

One procuring approach to analyze this influence is the conduction of Variance Based Sensitivity Analysis (VBSA) on the model under study. The VBSA was introduced by Saltelli et al (2007) 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 2013). The objective of this method is to find the parameter that has the greatest impact on the target figure. Within the scope of the presented approach, the numerical scenario analysis tool Monte Carlo Simulation (MCS) (Saltelli et al. 2010), based on probability theory and statistics, is used with SOBOL sampling for realizing the VBSA (Burhenne et al 2011). Thereby, these SOBOL samples are generated from the input factors which are represented with density functions in order to determine the impact on the output of the model. This process

is repeated for every possible functional value of the input to identify the associated uncertainties of one or more input factors.

The parameters of a model are defined as statistically independent random variables X_i that are expressed by the corresponding probability density function Y (Saltelli et al. 2007). In order to determine the influence of one input parameter on the output, the first order effect is calculated by:

$$First\ Order = Var[E(Y|X_i)] \quad (1)$$

The first order effect represents the variance if factor X_i is fixed. It leads, divided by the total variance, to the first order sensitivity index S_i with a value between 0 and 1:

$$S_i = \frac{Var[E(Y|X_i)]}{Var[Y]} \quad (2)$$

Additionally, sensitivity indices of a higher order describe the impact of more than one parameter on the output of the model, e.g. as shown for the second order effect:

$$Second\ Order = Var[E(Y|X_i, Y_i)] \quad (3)$$

Divided by the total variance of the model parameters, the second order sensitivity index can be calculated gradually and so forth. In general, VBSA-models are differentiated between additive and non-additive relations:

$$Additive\ models := \sum_{i=1}^{r} S_i = 1 \quad (4)$$

$$Non-Additive\ models := \sum_{i=1}^{r} S_i \leq 1 \quad (5)$$

In the latter case, the impact of the input parameters is, with respect to variance decomposition, not separable, as shown for the sensitivity indices:

$$V(Y) = \sum_i V_i + \sum_{i,j>i} V_{ij} + \cdots + V_{123\ldots k} \quad (6)$$

Due to the dependencies of more than one parameter on the uncertainty of the model, sensitivity indices of a higher order must be considered. The interactions between all parameters can be calculated by the total order sensitivity index that considers the sum of all partial sensitivity effects:

$$S_{Ti} = \frac{Var[E(Y|X_{-i})]}{Var[Y]} \quad (7)$$

In this case, X_{-i} refers to the amount of all input variables excluding the i-th parameter that is fixed. In a combined risk assessment, e.g. for security-related investments, the interaction of the parameters with regard to the interoperated risk might be very important for decision-making.

3. Approach

In this approach, we analyze the influence of uncertainties in a procedure of six consecutive steps. In these six steps, two different configurations of the security system of a notional airport structure are analyzed regarding the sensitivity of the model output vulnerability to the consideration of uncertainties. The first step briefly describes the model used to describe and analyze the vulnerability as a part of SRA. Additionally it introduces the notional airport security structure. The second step is used to describe the setup of two different configurations, for which we compute and analyze results. Following, uncertainties are added to the model and applied to the configurations. The fifth step consists of a VBSA for first and total order sensitivities of the model output. Finally, a hybrid configuration based on the findings of the prior steps in the sixth step.

3.1 *Step 1: Applied Vulnerability Model and Used Structure*

The basic principles of the used model for vulnerability, already introduced in Section 2 as well as the security system of the considered notional airport structure are described in the following section. The structure of a notional airport was subject to a security risk assessment in (Lichte and Wolf 2018).

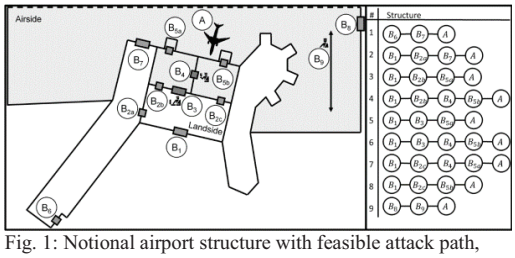

Fig. 1: Notional airport structure with feasible attack path, source: (Lichte and Wolf 2018)

The airport system and the identified security barriers are depicted in Fig. 1. Likewise, the figure outlines feasible attack paths within this structure.

The basic principles of the approach used in the original vulnerability assessment of the structure are briefly shown in Fig. 12. The barrier-oriented approach uses time-based

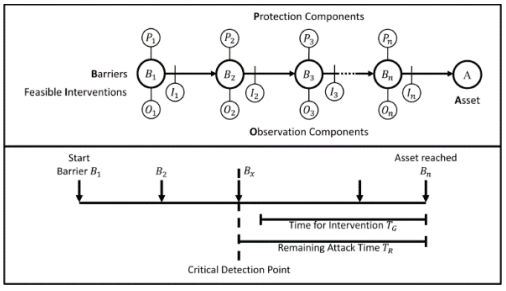

Fig. 2: Principle of security measures based on Garcia (2008), source: (Lichte et al 2019)

distributions based on the parameters tp, tO and tI for the parameters protection (P), observation (O) and intervention (I), respectively as shown in Fig. 3. Hereby, the approach describes the performance of security measures and additionally allows the consideration of uncertainties. It is based on an approach introduced by Garcia (2008).

In this approach, we initially let go of the usage of probability density functions (pdf) and only use discretized values to describe the performance of security measures without changing the basic barrier-oriented structure. Thus, the parameters are fully described by the mean values: $\mu_{p,i}=t_{p,i}$, $\mu_{o,i}=t_{o,i}$ and $\mu_{I,i}=t_{I,I}$ (compare Fig. 3).

On the one hand, this simplifies the setup of the two different configurations. On the other hand, it brings out the effect of the application of

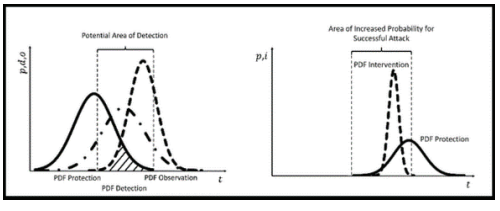

Fig. 3: Application of normal pdf (npdf) for t_p, t_o, t_r

uncertainties in the process of analysis.

3.2 *Step 2: Configuration Setup*

In the following, the setup of the two configurations is described. The first configuration, considered as conservative, introduces a security margin between the different influencing parameters of the system following the basic modelling approach. The second configuration is cost optimized, so that all parameters have the lowest performance possible to enable good theoretic system performance. The starting point of the setup of the configurations is the configuration originally analyzed in (Lichte and Witte 2019) listed in Table 1.

Table 1. Original values for notional airport security system

Barrier	Protection	Observation	Intervention	
	μ (s)	μ (s)	μ (s)	
B2a,b,c	120	10 0	80	
B3	120	90	30	
B4		60	30	3 0
B5a,b		60	120	180
B6		150	240	600
B7		360	180	360
B8		600	180	300
B9		240	300	30

Source: (Lichte and Witte 2019).

3.1.1 *Conservative Configuration*

The conservative configuration is represented by estimations of μ_p, μ_o and μ_I for all *i* barriers of the system, so that security margins $M_{sec,p}$ and $M_{sec,I}$ are established to ensure detection as well as a feasibility of intervention at the barriers of the system. According to the model characteristics, the time $t_{p,i}$ needed for protection is set to exceed the time needed for observation $t_{o,i}$ at every *i*-th barrier by $M_{sec,p}$:

$$M_{Sec,p,i} = t_{o,i} \cdot 0.2 \tag{8}$$

$$t_{p,i} = t_{o,i} + M_{Sec,p,i} \tag{9}$$

Analogously, the time needed for intervention $t_{I,i}$ at every *i*-th barrier is set to exceed the residual protection time $t_{RP,ij}$ on the shortest feasible outgoing attack path *j* by $M_{Sec,I,i}$:

$$M_{Sec,I,i} = t_{RP,ij} \cdot 0.2 \tag{10}$$

$$t_{I,i} = t_{RP,ij} + M_{Sec,I,i} \tag{11}$$

Herein, $t_{RP,ij}$ is:

$$t_{RP,ij} = \sum_{k=i+1}^{n} t_{p,ij} \cdot 0.2 \tag{12}$$

The resulting values of the characterizing parameters for the conservative configuration are shown in Table 2.

Table 2. Values for conservative configuration

Barrier	Protection	Observation	Intervention
	μ (s)	μ (s)	μ (s)
B2a	120	100	172
B2b,c	120	100	115
B3	108	90	115
B4	36	30	115
B5a,b	144	120	115
B6	288	240	172
B7	216	180	172
B8	216	180	288
B9	360	300	288

3.1.2 *Optimized Configuration*

Assuming that better performance of security measures, e.g. lowering the time needed for observation or increasing protection time lead to higher costs, optimizing the cooperation of security measures without considering significant security margins seems economically reasonable. Thus, analogously to the conservative configuration, $t_{p,i}$ and $t_{I,i}$ are chosen to be minimally greater than $t_{o,i}$ and $t_{RP,i}$, respectively. Hence, we define optimized protection time $t_{p,opt,i}$ and intervention time $t_{I,opt,i}$ at every *i*-th barrier as follows:

$$t_{p,opt,i} = t_{o,i} + t_{o,i} \cdot 0.02 \quad (13)$$

$$t_{I,opt,i} = t_{RP,ij} + t_{RP,ij} \cdot 0.02 \quad (14)$$

Table 3 lists the resulting values for the optimized configuration's discrete parameters.

Table 3. Values for optimized configuration

Barrier	Protection	Observation	Intervention
	μ (s)	μ (s)	μ (s)
B2a	102	100	180
B2b,c	102	100	120
B3	92	90	120
B4	31	30	120
B5a,b	123	120	120
B6	245	240	180
B7	184	180	180
B8	184	180	299
B9	206	300	299

3.3 *Step 3: Discrete System Vulnerability Assessment*

The computation of the vulnerability of all attack paths of the system shows the same result for both initial configurations. Based on the assumptions made on the security system performance and the discrete character of the parameters the security system of the airport structure is not vulnerable, as no feasible attack path leads to a successful attack, so that:

$$V_S = 0 \quad (15)$$

$$V_{S,opt} = 0 \quad (16)$$

Based on the Equations (15) and (16) it seems justified to prefer the optimized configuration to the conservative one, as it is probably less expensive and equally secure.

3.4 *Step 4: Uncertainty Considering Vulnerability Analysis*

For reasons of further investigation of the impact of uncertainties on the so far reached results, we add variance to the input parameters for protection, observation and intervention. Thus, we change their character from discrete values to time-based probability distribution functions. According to the used vulnerability model (see Sec. 3.1), we assume normal probability density functions (npdf). As the mean values $\mu_{p,i}=t_{p,i}$, $\mu_{o,i}=t_{o,i}$ and $\mu_{I,i}=t_{I,i}$ of the npdf's to establish are already defined, we only add a variance σ, which is proportional to μ:

$$\sigma = \mu \cdot 0.05 \quad (17)$$

Resulting variances for both configurations are combined in Table 4.

Table 4. Variance σ for both configurations

Barrier	Protection		Observation		Intervention	
	Cons	Opt	Cons	Opt	Cons	Opt
B2a	6	6	5	6	7	9
B2b,c	6	6	5	5	6	6
B3	6	5	5	5	6	6
B4	2	2	2	2	6	6
B5a,b	8	7	6	6	6	6
B6	15	12	12	12	9	9
B7	11	10	9	9	9	9
B8	11	10	9	9	15	15
B9	18	15	15	15	15	15

With the now established npdfs for $t_{p,i}$, $t_{o,i}$ and $t_{I,i}$ we conduct a re-assessment of the vulnerability considering the added uncertainties. For this purpose, we compute the vulnerability by Monte-Carlo-Simulation (MCS) with 100.000 samples and take the mean value over all

samples. The obtained results are listed in Table 5.

Table 5. System vulnerability for both configurations considering uncertainties

Attack Path	V_S	$V_{S,opt}$
1	0.006	0.515
2	0.009	0.486
3	0	0.238
4	0.004	0.522
5	0	0.243
6	0	0.214
7	0.006	0.533
8	0	0.07
9	0	0.074
10	0	0.034
11	0	0.081
12	0	0.026
13	0	0.029
14	0.01	0.456
15	0.008	0.49

The results show a significantly increasing vulnerability on all attack paths of the optimized system. At the same time, the vulnerability of the conservative configuration remains nearly unchanged. The weakest path, determining the system vulnerability V_S, is computed in every sample of the MCS and subsequently the mean of all samples is calculated to:

$$V_S = 0.041, V_{S,opt} = 0.984 \qquad (18)$$

It appears, that the addition of uncertainties has a great influence on the estimated vulnerability of the attack paths, since the vulnerability model and the mean values for the input parameters remain unchanged.

3.5 *Step 5: Variance Based Sensitivity Analysis*

In the next step, we apply a VBSA to both configurations. Hereby, we investigate first (S_i) and total order (S_{Ti}) sensitivity indices of the model output V_S to the input parameters $t_{p,i}$, $t_{o,i}$ and $t_{I,i}$. Using SALib SOBOL sampling (Herman and Usher 2019) with a sample count of 20.000 we get the results for all input parameters of the optimized configuration shown in Table 6.
The non-additive structure of the applied vulnerability model becomes obvious by analyzing the results for Si and corresponding S_{Ti}. While the top marginal variance S_i is generally low, the bottom marginal variance reaches significant values for certain input factors.

Table 6. S_i and S_{Ti} for all parameters in optimized configurations

B		t_p	t_o	t_I
2a	S_i	0	0.0031	0.00285
	S_{Ti}	0.33458	0.29707	0.12153
2b	S_i	0.00854	0.00833	0.00585
	S_{Ti}	0.31057	0.28357	0.04456
2c	S_i	0	0	0.00057
	S_{Ti}	0.31058	0.28357	0.09152
3	S_i	0.00228	0.0061	0
	S_{Ti}	0.30007	0.28207	0.09152
4	S_i	0	0	0
	S_{Ti}	0	0	0
5a	S_i	0	0	0
	S_{Ti}	0.23706	0	0
5b	S_i	0	0	0
	S_{Ti}	0.09602	0	0
6	S_i	0.00875	0.00667	0.00051
	S_{Ti}	0.30457	0.25956	0.06302
7	S_i	0.00249	0	0
	S_{Ti}	0.21605	0	0
8	S_i	0.01531	0.01734	0.0061
	S_{Ti}	0.30607	0.28657	0.11703
9	S_i	0.0029	0	0
	S_{Ti}	0.13203	0	0

Additionally, the results show that the uncertainty added to some of the input factors does not have an impact on the model output of system vulnerability, as sensitivity indices are zero in both configurations, e.g. all input factors at barrier B4. On the other hand, the uncertainty of some input factors seem to have an impact on the results independent of the configuration, e.g. at the barriers B2b, B2c, B6 and B8. However, the level of influence depends on the chosen configuration, e.g. for the protection at barrier B2c:

$$\frac{S_{T,t_{p,2c},opt}}{S_{T,t_{p,2c},cons}} = \frac{0.31058}{0.13804} \approx 2.25 \qquad (19)$$

Input factors with maximum and minimum influence for the optimized configuration are listed in Table 7.

Table 7. Input factors with minimum and maximum influence

	Min	*Max*
Input Factors	$t_{p,4}$, $t_{o,4}$, $t_{I,4}$, $t_{o,5a}$, $t_{I,5a}$, $t_{o,5b}$, $t_{I,5b}$, $t_{o,7}$, $t_{I,7}$, $t_{o,9}$, $t_{I,9}$	$t_{p,2a}$, $t_{o,2a}$, $t_{p,2b}$ $t_{p,2b}$, $t_{p,2c}$ $t_{p,2c}$, $t_{p,6}$ $t_{o,6}$, $t_{p,8}$ $t_{o,8}$ $t_{I,8}$

3.6 *Step 6: Setup of Hybrid Configuration*

As shown above, the first order sensitivity S_i are generally rather low, while there are input factors at certain barriers where the total order sensitivity S_{Ti} reveals an impact of the added variance or uncertainty. We can use this result to establish a hybrid configuration, where only influencing factors are subject to a security margin $M_{Sec,i}$. Non-influencing factors (see Table 7) are carried over from the optimized configuration. To verify the carried over factors we use the necessary and sufficient condition for non-influencing factors defined in the approach of Factor Fixing (Saltelli et al. 2007):

$$S_{Ti} = 0 \tag{20}$$

The resulting hybrid configuration is summarized in Table 8.

Table 8. Values for $t_{p,i}$, $t_{o,i}$ and $t_{l,i}$ of hybrid configuration

Barrier	Protection		Observation		Intervention	
	μ (s)	σ (s)	μ (s)	σ (s)	μ (s)	σ (s)
B2a	120	6	100	5	172	7
B2b,c	120	6	100	5	115	6
B3	108	6	90	5	115	6
B4	31	2	30	2	120	6
B5a,b	123	7	120	6	120	6
B6	288	15	240	12	172	9
B7	184	10	180	9	180	9
B8	216	10	180	9	288	5
B9	306	15	300	15	299	15

Analogously to the other configurations, we compute the vulnerability of all attack paths as well as the system vulnerability considering the added variance. The results are shown in Table 9.

Results show a massive reduction of vulnerability in comparison to the optimized configuration (see Table 5). Hence, the hybrid configuration assumedly performs significantly better than the optimized one, although only ten out of 30 input parameters have an added security margin. Additionally, the performance level is close to the conservative configuration (see Table 5). Initially, this points to a good estimation of which input factors have greater importance to the output factor VS. Further, the results reveal differing levels of influence of uncertainties for the input factors of the model, since the estimation of input factors is based on a VBSA. Thus, adding M_{sec} to influencing input factors determined by a VBSA can minimize the influence of uncertainties within the model.

Table 9. Results for path and system vulnerability of hybrid configuration

Attack Path	$V_{S,\,hybrid}$
System	0.07
1	0.015
2	0.025
3	0.001
4	0.006
5	0.002
6	0.007
7	0.011
8,9,10,11, 12,13	0
14	0.012
15	0.005

4. Conclusion

The presented approach shows the influence of uncertainties on quantitative security risk assessment. Additionally, it outlines how the application of a VBSA helps to identify important input factors of the model to minimize shown influence. Therefore, six consecutive steps are conducted. We apply vulnerability analysis to a notional infrastructure and investigate the influence of added variance describing uncertainties to discrete model input factors. Analysis of two differing configurations, in which only one comprises a security margin, reveals the influence of the added uncertainties. The results points to a significant configuration dependent influence of added uncertainties. The additionally conducted VBSA shows differing influences of the various input factors and their uncertainty. Further, the non-linear character of the used vulnerability model is revealed, as $S_{Ti} >> S_i$. Based on the VBSA, we adapt the most influencing input factors in a hybrid configuration. The results of this configuration substantiate the assumption regarding the differing influence of input parameters. Hence, the approach of Factor Fixing can help in systematically identifying the most influencing factors of the uncertainty considering vulnerability model. Thus, the approach of Factor Fixing can be applied to support decision-making by identifying critical points within a security system and to find feasible optimized solutions. Since at least a good modeling knowledge of modeling regarding the effects of security measures is needed for this detailed analysis, sufficient attention should be paid to the level of effect uncertainty and resulting consequences. According to Abrahamsen et al. (2015) extreme consequences should lead to precautionary approaches. Here, the introduced

security margin can be used. A VBSA may help in evaluating the needed size of the security margin.

In future work, an investigation of the applicability of the VBSA for further analysis of model interactions is meaningful. Anyway, 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 huge.

References

Abrahamsen, E., Gould, K., Aven, T., Kaufmann, M. and T. Rosqvist (2015). A framework for selection of strategy for management of security measures. Journal of Risk Research 1–14.

Alcaraz, C. and S. Zeadally (2014). Critical infrastructure protection: requirements and challenges für the 21st century, *International Journal of Critical Infrastructure Protection*.

Almeida, F., Faria, D. and A. Queirós (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. *European Journal of Education Studies*. 3, 369-387.

Amundrud, O., Aven, T. and R. Flage (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.

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

Burhenne, S., Dirk, J. and G. Henze (2011). Sampling based on SOBOL` sequences for Monte Carlo techniques applied to building simulations. In: *Proceedings of Building Simulation 2011: 12th Conference of International Buildung Performance Simulation Association.*

Campbell, P. H. and Stamp, J. E. (2004). A Classification Scheme for Risk Assessment Methods, p. 25.

Dongen, T. (2009). Break it Down: An Alternative Approach to Measuring Effectiveness in Counterterrorism. Journal of Applied Security Research, vol. 6, no. 23.

Flammini, F., Marrone, S., Mazzona, N. and Vittorini, V. (2013). Petri net modelling of physical vulnerability. In: *Lecture Notes in Computer Science*, Berlin und Heidelberg, pp. 128 – 139. Springer-Verlag.

Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems, 2nd ed. Burlington (USA).

Henkel, T., Wilson, H. and W. Krug (2012). Global sensitivity analysis of nonlinear mathematical models - an implementation of two complementing variance-based algorithms, In *Proceedings of the Winter Simulation Conference.*

Herman, J. and W. Usher (2019). SALib: An open-source Python library for Sensitivity Analysis, University of California, Davis, University of Oxford.

G. Landucci, F. Argenti, V. Cozzani, G. Reniers, 2017. Quantitative performance assessment of physical security barriers for chemical facilities, in: Proceedings of *ESREL 2017 - Safety & Reliability - Theory and Applications* (Cepin, M. and Bris, R.). CRC Press, pp. 1279–1287.

Lichte, D. and Wolf, K.-D. (2017). Quantitative multiple-scenario vulnerability assessment applied to a civil airport infrastructure. In: *Proceedings of ESREL 2017: Safety & Reliability - Theory and Applications* (Cepin M. and Bris, R.), CRC Press.

Lichte, D. and Wolf, K.-D. (2018). A Study on the Influence of Uncertainties on Physical Security Risk Management, In: *Proceedings of ESREL 2018: Safety and Reliability – Safe Societies in a Changing World* (Haugen, S. et al.), CRC Press.

Lichte, D., Wolf, K.-D. and Witte, D. (2019). An Approach to Software Assisted Physical Security Risk Analysis and Optimization, In: *Proceedings of ESREL 2019: 29th European Safety and Reliability Conference* (Beer, M. and Zio, E.), ESRA.

McGill, W. L., Ayyub, B. M. and M. Kaminskiy (2007). Risk Analysis for Critical Asset Protection, vol. 27, no. 5, pp. 1265–1281

Meritt, J. W. (2008). A Method for Quantitative Risk Analysis. In Proceedings of the 22nd National Information Systems Security Conference, Arlington, VA, USA

Milliken, F., (1987). Three Types of Perceived Uncertainty About the Environment: State, Effect, and Response Uncertainty. Academy of Management review, vol. 12, no. 1, pp. 133–143.

Saltelli, A. Tarantola S., Campolongo F. and Ratto, M. (2007). Sensitivity Analysis in Practice - A Guide to Assessing Scientific Models. Chichester, England: John Wiley & Sons.

Saltelli, A., Annoni, P., Azzini, I., Campolongo, F., Ratto, M. and Tarantola, S. (2010). Variance based sensitivity analysis of model output. Design and estimator for the total sensitivity index, Joint Research Centre of the European Commission.