Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R26-02-269-cd

An Approach to the Consideration of Uncertainties in Cost-Benefit Optimal Design of Physical Security Systems

Dustin Witte

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

Daniel Lichte

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

Kai-Dietrich Wolf

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

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 and researchers continuously propose new approaches. Moreover, consideration is given to how security measures need to be (re)designed to address the findings of the assessments, taking into account the potentially costly nature of security investments. At the same time, however, assessments suffer from the fundamental problem of inherent uncertainties regarding threats and capabilities of security measures due to little evidence of actual attacks. In this paper, we combine previous work on the concept of security margins with an approach for cost-benefit optimal allocation of available resources considering budgetary constraints to form a three-step approach. In a first step, a security system is assessed for potential vulnerabilities. If such are found, most relevant model parameters are identified on barrier level via sensitivity analysis in a second step. In a third step, security margins are determined for these parameters by optimization, taking into account uncertainties in the assessment as well as cost constraints due to total available budget. The approach is demonstrated using a notional airport structure as an example. The optimization is performed for various budgets to investigate the influence of the budget on system vulnerability and allocation of resources to security measures.

Keywords: Physical Security, Uncertainty, Security Risk Assessment, Quantitative Uncertainty Assessment, Security Margin, Vulnerability, Critical Infrastructure Protection, Cost-Benefit Optimization.

1. Introduction

Increasing awareness of terrorist activity has brought the security of critical infrastructures into the focus of operators as well as politics. New risk policies and laws result in a growing demand for security risk assessment (SRA) and cost-benefit oriented optimization methods to ensure the (physical) security of critical infrastructures. Field experience shows that assessment and optimization remain difficult tasks, mostly covered by qualitative methods. In contrast, quantitative methods and models for assessment are rarely used, although new approaches have emerged, e.g. those by Flammini et al. (2013) and Landucci et al. (2017). Despite the fact that quantitative results allow for more detailed analysis, the main reasons for this limited application are the complexity of implementation and the availability of quantitative data.

Additionally, SRA and corresponding cost-benefit optimization is fraught with inherent uncertainties. The reason is a lack of evidence of actual attacks with a terrorist background regarding threat scenarios as well as the capabilities of security systems (Abrahamsen et al., 2015). Thus, the subsequent optimization is often backed by vague data or elicited expert knowledge that may represent a rather subjective perspective. As shown in Lichte et al. (2021), the outlined uncertainties can have a significant impact on the effectiveness of a security system. The approach described there takes these uncertainties into account in the form

of security margins and a predefined level of security measure effectiveness. In the presented paper, we enhance the approach by adding basic cost functions for security measure effectiveness. These underlying cost functions represent life cycle costs. The enhanced security margin concept is then applied to cost-benefit optimization under budgetary constraints using an evolutionary algorithm.

We demonstrate the benefit of the approach using the example of a notional airport infrastructure. Critical barriers within the analyzed security system are revealed via sensitivity analysis and improved security configurations are derived by optimization for various budgets. The optimization results are discussed.

2. Background

2.1. *Cost-benefit analysis and optimization in physical security analysis*

Generally, a cost-benefit analysis of security measures proves to be difficult as the benefits of measures are hard to evaluate (Butler, 2002). Thus, the support of decision-making concerning security investments is a continuously developing field of research (Abrahamsen et al., 2015). In addition, cost-benefit estimations are hampered by the underlying inherent uncertainties in SRA which already complicate the evaluation of the effectiveness of the security system (Lichte et al., 2021).

Only a few approaches exist in physical SRA that provide strategies for decision-making with respect to security measures. Wyss et al. (2010) propose a security risk metric based on vulnerability analysis. The approach is based on the idea that applied measures should increase the difficulty of the easiest paths towards a successful attack considering the constraints of costs, operational and programmatic restrictions. The variety of possible security measures and their threat specific effectiveness lead to a large search space for appropriate solutions. Genetic algorithms are used to address this optimization problem. For instance, Flammini et al. (2011) determine an optimal coverage of specified security measures at a site regarding their return on investment and a budget constraint. While different threats are considered, the effect mechanisms of security measures are modeled in a highly simplified way. Also based on return on investment and a budget constraint, but relying on a barrier-oriented and time-based vulnerability model, Lichte et al. (2019) optimize the effectiveness of security measures at barriers along attack paths using an evolutionary algorithm. Here, measures are described by their effectiveness and costs are related by cost functions.

Another time-based approach, taking the topology of barriers into account, is given by Čakija et al. (2020). In the optimization outlined there, elements of a predefined set of available security measures are applied to facility elements, with costs assigned to each available measure. Although uncertain model parameters are considered in the underlying vulnerability model in general, the approach does not aim at mitigating the impact of their uncertainties explicitly. In contrast, Lichte et al. (2021) tackled the challenge of addressing the uncertainty regarding the security measure effectivity by proposing the concept of a security margin. The approach is based on variance based sensitivity analysis (see e.g. Saltelli et al., 2004) and a barrier-oriented quantitative vulnerability model (see Section 2.2). This approach allows for minimization of residual uncertainty regarding security barrier effectivity and provides the opportunity to make cost-benefit considerations by extending the approach with cost functions.

2.2. *Underlying vulnerability model*

The vulnerability model underlying the security margin concept relies on basic assumptions, which characterize the most relevant behavior of a security system of an infrastructure (see Lichte and Wolf, 2017). The resulting model consists of three main input parameters that characterize the system capabilities provided by the installed security measures at each of its barriers: protection time t_{P}, observation time t_{O} and intervention time t_{I}. Each of these parameters is described as a random variable with an associated time-based probability density function (pdf). Capabilities are described as relations between these parameters.

Detection of an attacker is triggered if the protection at a barrier prevents an attacker from a break-through until an observation is successfully

completed. This is described by the conditional probability D:

$$D = P(t_{\mathrm{O}} < t_{\mathrm{P}}) \tag{1}$$

Herein t_{P} is the time an attacker needs to overcome the protection and t_{O} the time needed to observe for successful detection.

Timely intervention is the second key relation in the vulnerability model. It is based on the time needed for successful intervention t_{I} and the residual protection time t_{RP}. The residual protection time t_{RP} at a barrier i is the sum of all protection along the residual barriers i to n on an attack path minus the time needed for detection.

$$t_{\mathrm{RP}} = \sum_{j=i}^{n} t_{\mathrm{P},j} - t_{\mathrm{O},i} \tag{2}$$

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

$$T = P(t_{\mathrm{I}} < t_{\mathrm{RP}}) \tag{3}$$

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

$$V_{\mathrm{B}} = 1 - D \cdot T \tag{4}$$

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

$$V_{\mathrm{P}} = \prod_{j=1}^{n} V_{\mathrm{B},j} \tag{5}$$

System vulnerability V_{S} is determined by the weakest path:

$$V_{\mathrm{S}} = \max(V_{\mathrm{P},1}, \ldots, V_{\mathrm{P},m}) \tag{6}$$

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 (see Eq. (6)). The mean of all samples then describes the overall system vulnerability.

3. Approach

In the following, an approach for the consideration of uncertainties in cost-benefit optimal (re)design of physical security systems is presented. The approach utilizes the vulnerability model described in Section 2.2 and is demonstrated by applying it to a notional airport structure which was subject to a SRA in Lichte and Wolf (2017). This structure was also used in the derivation of the usage of security margins in Lichte et al. (2021). The airport system and the identified security barriers are depicted in Fig. 1. Additionally, the figure outlines feasible attack paths within this structure.

The approach consists of three steps. First, the current airport security system is assessed for potential vulnerabilities. If such are found, most relevant model parameters are identified on barrier level via sensitivity analysis in a second step. In a third step, the optimal allocation of security margins to the parameters are determined by an optimization based on cost functions and a specified budget.

3.1. *Vulnerability assessment of exemplary airport structure and security system*

The initial security measure performances and the associated uncertainties are assumed as in Lichte et al. (2021). Herein, the security parameters are characterized by normal pdfs with mean values $\mu_{\mathrm{P}i}$, $\mu_{\mathrm{O}i}$, $\mu_{\mathrm{I}i}$ and respective variances $\sigma^2_{\mathrm{P}i}$, $\sigma^2_{\mathrm{O}i}$, $\sigma^2_{\mathrm{I}i}$ that represent the uncertainty. Used input data for the configuration of the security system is shown in Table 1.

Scalar calculation of system vulnerability V_{S} solely based on mean values results in zero vulnerability, i.e. $V_{\mathrm{S}} = 0$. However, if we consider variances according to the relationships given in Section 2.2 and calculate V_{S} by Monte Carlo simulation, we obtain

$$V_{\mathrm{S}} = 0.811 \tag{7}$$

which points to a vulnerable system.

The barriers that cause high vulnerability remain initially unknown. Therefore, sensitivities are further investigated in the second step by analyzing the introduced variances.

3.2. *Uncertainty impact assessment on barrier level*

In this step, we analyze which uncertain parameters impact system vulnerability as shown in

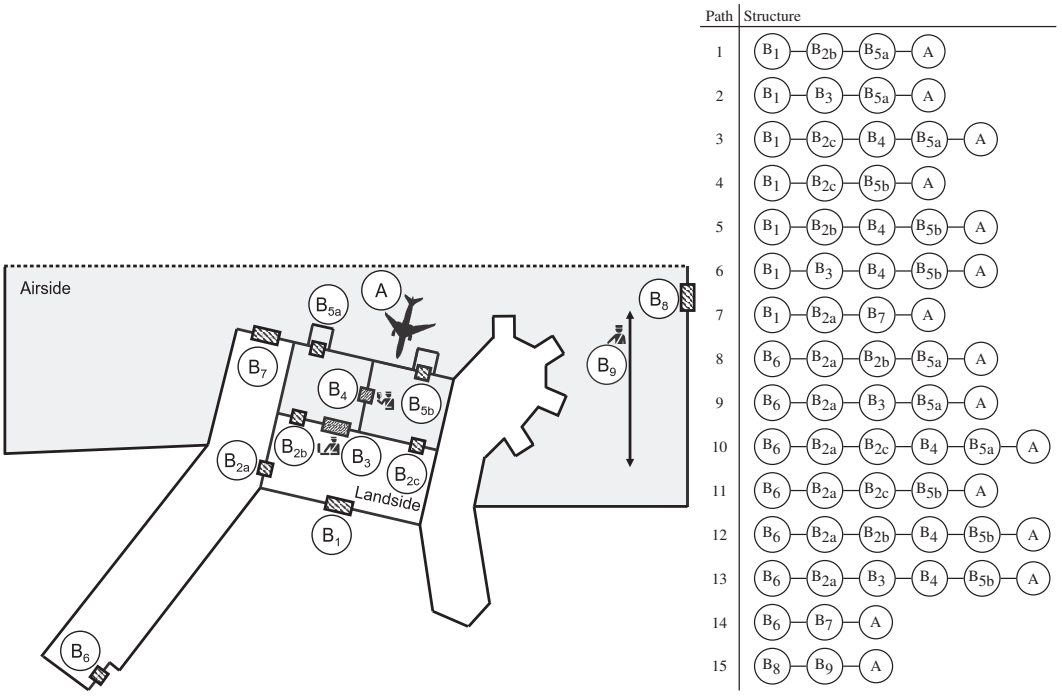

Fig. 1. Notional airport structure with feasible attack paths

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

Lichte et al. (2021). By applying a variance based sensitivity analysis, we reveal the influence of all parameters on barrier level. For this purpose, we investigate the total effect sensitivity indices S_T of the model output V_S to the input parameters t_P, t_O and t_I. By generating samples based on Sobol sequences and calculating the sensitivity indices using the software SALib (Herman and Usher, 2017), we obtain S_T for all input parameters shown in Table 2.

Table 2. Total effect sensitivity indices S_T for all parameters, with values above 0.1 highlighted

Barrier	$S_{\mathrm{T,P}}$	$S_{\mathrm{T,O}}$	$S_{\mathrm{T,I}}$
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

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

3.3. *Optimization of physical airport security*

In order to address the revealed vulnerability, we search for an improved security system design. The new design should minimize system vulnerability while keeping costs low. To do this, we set up an optimization of system vulnerability for fixed budgets. We assume that the security measures currently installed cannot be easily downgraded in order to save costs. Hence, in the optimization, we focus on the most critical model parameters identified in the previous conducted sensitivity analysis. This reduces the number of design variables and restricts cost analyses to certain barriers. For security systems being designed for the first time, it might instead be appropriate to include all barriers to reduce costs where high-effective security measures are not required (see Lichte et al., 2019). For the example, we select the parameters with high sensitivity indices as highlighted in Table 2 for optimization.

3.3.1. *Security margins, objective and budget constraint*

We take the configuration of the analyzed security system and apply security margins M to the selected model parameters t. This results in new parameter values t' for protection, observation and intervention:

$$t'_{\mathrm{P}} = t_{\mathrm{P}} + M_{\mathrm{P}} \tag{8}$$

$$t'_{\mathrm{O}} = t_{\mathrm{O}} - M_{\mathrm{O}} \tag{9}$$

$$t'_{\mathrm{I}} = t_{\mathrm{I}} - M_{\mathrm{I}} \tag{10}$$

where margins are defined to be positive:

$$M_{\mathrm{P}} \in [0, \infty) \tag{11}$$

$$M_{\mathrm{O}} \in [0, t_{\mathrm{O}}) \tag{12}$$

$$M_{\mathrm{I}} \in [0, t_{\mathrm{I}}) \tag{13}$$

In doing so, the application of security margins represents an improvement of security measures.

The objective of the optimization is minimizing system vulnerability. Thus, we define the optimization problem by

$$\min_{\vec{M} \in X} (V_{\mathrm{S}}), \tag{14}$$

where V_{S} is the objective, $\vec{M}$ the vector of design variables, i.e. the security margins, and X the design space as given by Eq. (11) to (13).

Rationally, the value of security margins is limited. Here, we define an available budget C_{budget}. We assume that any security margin causes costs that can be described by a corresponding cost amount C_i. Both, budget and cost refer to the same time period. The requirement that the sum of all expenditures must be within the budget is then a constraint on optimization:

$$\sum_{i=1}^{n} C_i \leq C_{\mathrm{budget}} \tag{15}$$

3.3.2. *Cost functions of security margins*

In order to include costs in the optimization, we establish a relation between the level of security margin M and the corresponding costs C_i. For this purpose, we define cost functions that are assumed to be the result of separate cost analyses. We use a simple polynomial for modeling a disproportional increase in costs over security margin. This model reflects the assumption that more and more effort is needed to increase the effectivity of security measures. Further, we add a separate cost increase ΔC that reflects additional costs for modifying the measures currently installed, but is zero if no security margin is applied ($\Delta C = 0$ if $M = 0$). The cost functions for the different security parameters

Table 3. Parameters of cost functions for notional airport structure

Barrier	t_P			t_O			t_I		
	C_P (€)	m_P (€/s)	ΔC_P (€)	C_O (€)	m_O (€/s)	ΔC_O (€)	C_I (€)	m_I (€/s)	ΔC_I (€)
2a	100 000	10 000	10 000	120 000	−2 000	30 000	—	—	—
2b	100 000	10 000	10 000	120 000	−2 000	30 000	—	—	—
2c	100 000	10 000	10 000	120 000	−2 000	30 000	—	—	—
3	1 000 000	40 000	100 000	1 000 000	−40 000	100 000	—	—	—
6	150 000	10 000	20 000	200 000	−5 000	50 000	—	—	—
8	500 000	50 000	300 000	1 500 000	−20 000	200 000	2 000 000	−30 000	100 000

are then:

$$C'_\mathrm{P} = c_\mathrm{P} \cdot (t_\mathrm{P} + M_\mathrm{P})^{d_\mathrm{P}} + \Delta C_\mathrm{P} \tag{16}$$

$$C'_\mathrm{O} = c_\mathrm{O} \cdot (t_\mathrm{O} - M_\mathrm{O})^{d_\mathrm{O}} + \Delta C_\mathrm{O} \tag{17}$$

$$C'_\mathrm{I} = c_\mathrm{I} \cdot (t_\mathrm{I} - M_\mathrm{I})^{d_\mathrm{I}} + \Delta C_\mathrm{I} \tag{18}$$

It should be noted that, in principle, other cost functions can be utilized that may better reflect the outcome of cost analyses carried out.

We use the current system design as a reference point and calculate c and d from the current costs C attributed to the model parameter and the local cost gradient m:

$$d = \frac{m \cdot t}{C} \qquad c = \frac{C}{t^d} \tag{19}$$

Figure 2 illustrates the parameters used to describe the cost functions. For the airport example, hypothetical values are given in Table 3.

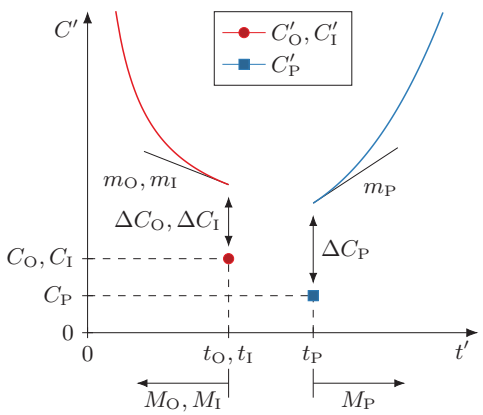

Fig. 2. Parameterization of cost functions

3.3.3. *Optimization strategy*

Besides the potentially large number of design variables, $V_\mathrm{S}(\vec{M})$ shows non-linear, non-smooth and non-convex behavior caused by the underlying vulnerability model. Therefore, we choose an evolutionary algorithm for optimization. We use the differential evolution algorithm (Storn and Price, 1997) implemented in SciPy (Virtanen et al., 2020). The budget constraint is enforced according to the approach by Lampinen (2002). We set the algorithm to terminate when standard deviation of population is less then or equal to 0.01. Apart from that, we use default options.

One problem caused by the optimization algorithm is to find solutions where security margins M are exactly zero. Therefore, we assume that no security margin is applied if $M < 1\,\mathrm{s}$. Accordingly, we set $\Delta C = 0$ if $M < 1\,\mathrm{s}$.

3.4. *Optimization results for different budgets*

To study the impact of additional budget on vulnerability reduction as well as the allocation of security margins, we set several hypothetical budgets and perform optimization for each of them. Each optimization yields a new configuration of the security system. In the example, we increase the amount of additional budget in steps of 0.5 million € to a maximum of 3.5 million €, starting from the initial configuration. Figure 3 plots the resulting vulnerability and security margins against the additional budget.

The resulting system configurations show a continuously decreasing vulnerability with respect

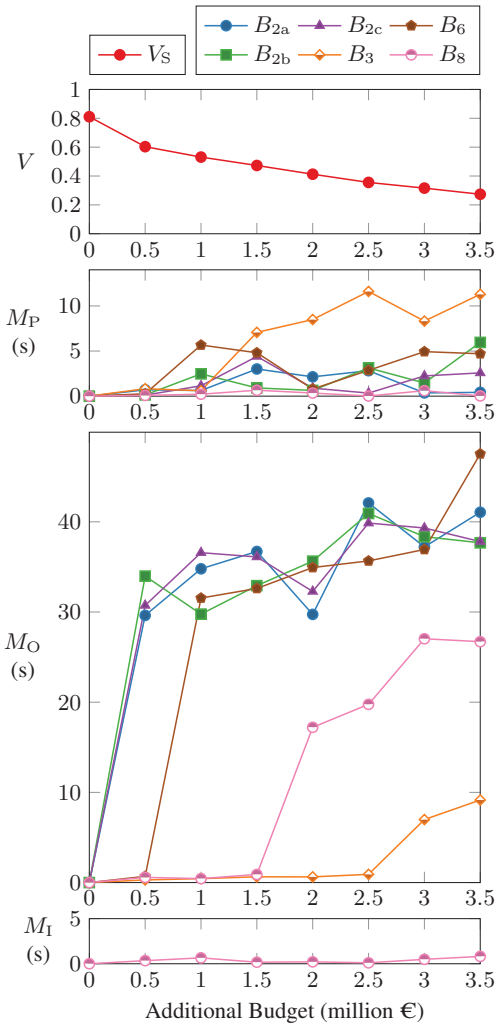

Fig. 3. Vulnerability and optimal allocation of security margins for different budgets

to the available budget. Furthermore, the transition between the values of single security margins is reasonably smooth. Both indicate that the optimization algorithm provides consistent results. In addition, the sum of all costs is close to the limit of the budget. However, due to the nature of evolutionary algorithms, global optima are not guaranteed.

Figure 3 shows that the allocation of security margins varies depending on the budget: when the budget is low, security margins are concentrated on a few parameters (see $M_{O,2a}$, $M_{O,2b}$, $M_{O,2c}$, $M_{P,6}$, $M_{O,6}$), while security margins are applied to more parameters as the budget increases (see $M_{P,3}$, $M_{O,3}$, $M_{O,8}$). Besides the effect of the cost functions, this hints to the varying impact of the different barriers for system vulnerability that is taken into account by the proposed optimization procedure.

Additionally, also the allocation of security margins to protection, observation and intervention may be significantly different and even lead to partially reduced security margins for increasing budget. For many barriers, security margins concentrate to observation parameters (see B_{2a}, B_{2b}, B_{2c}, B_6, B_8), but there is also a barrier where, depending on the budget, security margin of protection dominates or security margins of protection and observation are similar (see B_3).

In general, security margins increase as the budget increases. However, a slight reduction in some security margins is observable in tandem with the initial application of security margin to another parameter, e.g. the initial increase of $M_{O,8}$ at 2 million €. One possible explanation is that the cost increase ΔC first inhibits the application of security margin, but the lower cost gradient m, once overcome, then leads to a partial focus on this parameter.

4. Conclusion

The paper presents an approach to reach a cost-benefit optimal (re)design for security systems. The process is explained in detail by applying it to a notional airport infrastructure and the results of the conducted optimization are discussed.

The approach extends the previously introduced concept of security margins to address uncertainties regarding the effectiveness of security measures by combining it with cost functions. In this way, budgetary restrictions are considered in the determination of optimal security margins. At the same time, the determination takes into account the structure of the security system, since the impact of the individual barriers on system vulnerability is an inherent part of this approach. In the presented approach, the optimal characteristics of security measures at the respective barriers are described by the introduced security margins. This concept

enables a solution-neutral derivation of appropriate measures, while e.g. the approach of Čakija et al. (2020) is limited to a premade selection.

The example calculation shows that the allocation of security margins to the individual barriers and effect mechanisms is based on their impact as well as on the ratio of costs and benefits, i.e. the reduction of vulnerability. It is shown that the allocation focuses on specific measures and can differ depending on the available budget.

In future work, the approach could be extended to include varying consequences in different scenarios to broaden the presented vulnerability consideration and analyze profitability of the security system on the basis of risk.

References

Abrahamsen, E. B., K. Pettersen, T. Aven, M. Kaufmann, and T. Rosqvist (2015, July). A framework for selection of strategy for management of security measures. *Journal of Risk Research 20*(3), 1–14.

Butler, S. A. (2002). Security attribute evaluation method: A cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering (ICSE)*, New York, NY, USA, pp. 232–240. IEEE.

Flammini, F., A. Gaglione, N. Mazzocca, and C. Pragliola (2011, February). Optimization of security system design by quantitative risk assessment and genetic algorithms. *International Journal of Risk Assessment and Management 15*(2/3), 205–221.

Flammini, F., S. Marrone, N. Mazzocca, and V. Vittorini (2013). Petri net modelling of physical vulnerability. In S. Bologna, B. Hämmerli, D. Gritzalis, and S. Wolthusen (Eds.), *Critical Information Infrastructure Security*, Number 6983 in Lecture Notes in Computer Science, Berlin, pp. 128–139. Springer.

Herman, J. and W. Usher (2017). Salib: An open-source python library for sensitivity analysis. *Journal of Open Source Software 2*(9), 11–15.

Lampinen, J. (2002). A constraint handling approach for the differential evolution algorithm. In *Proceedings of the 2002 Congress on Evolutionary Computation*, Volume 2, pp. 1468–1473 vol.2. IEEE.

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

Lichte, D., D. Witte, T. Termin, and K.-D. Wolf (2021, December). Representing uncertainty in physical security risk assessment. *European Journal for Security Research 6*(2), 189–209.

Lichte, D., D. Witte, and K.-D. Wolf (2019). An approach to software assisted physical security risk analysis and optimization. In M. Beer and E. Zio (Eds.), *Proceedings of the 29th European Safety and Reliability Conference*, pp. 3949–3956.

Lichte, D. and K.-D. Wolf (2017). Quantitative multiple-scenario vulnerability assessment applied to a civil airport infrastructure. In M. Čepin and R. Briš (Eds.), *Safety and Reliability*, Leiden, the Netherlands. CRC Press.

Saltelli, A., S. Tarantola, F. Campolongo, and M. Ratto (2004). *Sensitivity Analysis in Practice*. Chichester, England: John Wiley & Sons.

Storn, R. and K. Price (1997, December). Differential evolution, a simple and efficient heuristic for global optimization over continuous spaces. *Journal of Global Optimization 11*(4), 341–359.

Čakija, D., v. Ban, M. Golub, and D. Čakija (2020). Optimizing physical protection system using domain experienced exploration method. *Automatika 61*(2), 207–218.

Virtanen, P. et al. (2020, March). SciPy 1.0: fundamental algorithms for scientific computing in python. *Nature Methods 17*(3), 261–272.

Wyss, G. D., J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton, and K. W. Mitchiner (2010). Risk-based cost-benefit analysis for security assessment problems. In D. A. Pritchard (Ed.), *IEEE International Carnahan Conference on Security Technology (ICCST)*, Piscataway, New Jersey, United States, pp. 286–295. IEEE.