Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P603-cd

On the Impact of Epistemic Uncertainty in Scenario Likelihood on Security Risk Analysis

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

Physical protection against deliberate attacks is an essential part of critical infrastructure protection. However, attacks are difficult to predict and evidence is rarely available. A challenge in security analysis is therefore a high degree of complexity and uncertainty regarding the scenarios that may occur, including possible attack sequences. The objective evaluation of physical security requires a sophisticated risk analysis. For an analysis of the security risk, threats must be identified, the effectiveness of security measures must be examined, and possible impacts must be evaluated. The quantification of risk is then subject to aleatoric and epistemic uncertainties. With the approach presented here, we intend to make the influence of uncertainties visible. The approach considers uncertainties regarding threats by a wide range of possible scenarios. In each scenario, uncertainties regarding the effectiveness of security measures are considered in a vulnerability model, taking into account possible attack sequences. The vulnerabilities are then weighted by likelihood of scenario occurrence. In a case study, we investigate the impact of epistemic uncertainties under the assumption of different levels of available information about possible attack scenarios and their likelihoods. The results show that risk quantification differs across scenarios, which would probably have an impact on the design of security measures.

Keywords: Physical Security, Scenario Analysis, Security Risk Analysis, Quantitative Uncertainty Assessment, Vulnerability, Critical Infrastructure Protection.

1. Introduction

Due to current developments, securing critical infrastructures is a pressing issue for their operators. When designing the necessary physical security system, it is important to consider the relevant scenarios in order to effectively reduce the vulnerability of the infrastructures. However, the problem here is that, on the one hand, there are a large number of potential threats from different attacks. On the other hand, there is little evidence for these attacks, which creates a great uncertainty in the design of security measures. One way to address this problem is to define a reference of attack scenarios, a so-called Design Basis Threat. A Design Basis Threat describes attributes and characteristics of potential adversaries against which a physical security system is designed and evaluated. For instance, the International Atomic Energy Agency recommends that state authorities define the threat in the form of a Design Basis Threat (International Atomic Energy Agency, 2011). It should be used as a common basis for the design and implementation of the physical security system. In contrast, Wyss et al. (2010) suggest analyzing a wide range of possible scenarios instead of the Design Basis Threat to enable a comprehensive picture.

However, both variants can lead to problems due to the described baseline situation in the beginning. The use of a Design Basis Threat can lead to an incomplete analysis due to the limited number of threats considered. This can lead to ineffective design if relevant attack scenarios are omitted. For the latter variant, it seems reasonable to weight

the possible scenarios, since a design compromise must be found for the variety of different attack scenarios. However, with low evidence and incomplete information on the threat situation, large uncertainties must be assumed here. Failure to take these uncertainties into account can lead to a strong distortion of the vulnerability of the security measures under evaluation.

In order to address these problems and thus enable a targeted and effective design of security measures, scenario likelihoods should be included as a weighting in an overall vulnerability. For this purpose, it is necessary that the inherent uncertainties are taken into account and made visible. Therefore, we present an approach that separates existing uncertainties in the security risk assessment into two sub-models for threat likelihood and vulnerability and considers them when merging them into a weighted overall vulnerability.

To do so, we proceed in the following steps: first, we introduce the scenario analysis, where we identify potential threats as well as attack paths. In a second step, we describe the used model for vulnerability analysis, in which we are able to calculate weakest attack paths systematically based on a unified time-based and probabilistic metric for detection and intervention. This is followed by a merging of the two models into a scenario-spanning vulnerability. In a case study demonstrating this approach, we show the impact of these uncertainties when applying three exemplary assumptions regarding the available information about possible attack scenarios. We discuss the obtained results before concluding the paper with a summary and an outlook.

2. Background

When analyzing security risks, there are several factors that are affected by uncertainty: the potential threats, the likelihood of threat scenarios and the effectiveness of security measures. Different models have been developed to address these uncertainties.

Threat assessment methods aim to identify specific threat scenarios. Model-based approaches have been developed to systematically describe threats and threat scenarios. For example, Tekinerdoğan et al. (2021) defines feature models to depict the common and variant features of a Design Basis Threat. For a comprehensive generation of scenario descriptions, a morphological analysis (Johansen, 2018) can be applied. Lichte et al. (2020) shows an application to threat scenarios.

Quantification of attack likelihoods might be reached by estimating the annual rate of occurrence of a scenario (McGill et al., 2007). However, this data may not be available. Another approach is the usage of relative likelihoods among all scenarios. For example, Paté-Cornell and Guikema (2002) describe a Bayesian network which weights the likelihoods of scenarios based on the expected utility for the attacker. Witte et al. (2020) describe how to build such a Bayesian network on top of a morphological analysis.

The effectiveness of security measures depends on the actual behavior of the attacker. In general, multiple attack paths are possible. Garcia (2008) suggests to construct an Adversary Sequence Diagram, a layer based graphical representation of the security system, to get an overview of potential paths. There are even more detailed models, which derive paths from the spatial description of the security system (Jang et al., 2009). Given an attack path, the effectiveness of security measures is analyzed along these paths, based on the probability of detection and a probabilistic time game of intrusion time and time needed to interrupt the attacker (Garcia, 2008; Lichte et al., 2021).

3. Approach

The structure of the approach is based on the steps of risk assessment in ISO 31000 (2018): identify risk and quantify risk. However, the approach is limited to a consideration of the likelihood of attacks and their success. Consequences of a successful attack are not analyzed. We demonstrate the approach using the security system of a notional site as an example.

3.1. *Attack scenario identification*

First, potential attack scenarios are identified. For this purpose, potential threats and attack paths are developed in a morphological analysis and spatial analysis respectively.

3.1.1. *Morphological threat analysis*

The objective of the morphological threat analysis is to develop a comprehensive list of potential offenders in specific scenarios. In a morphological threat analysis we describe scenarios which comprise information about different key features. Each feature covers a part of the threat description.

We start the analysis by defining a general scenario description. The scenario description contains all the features that are considered in the following analysis. We use the following simple scenario description for our example:

> An offender with an *intention* tries to reach a *target* object by using *resources*.

After defining the scenario features, possible characteristics are collected. All relevant types of offenders should be considered. For our example, we consider a highly simplified list of characteristics presented in Table 1.

Table 1. Scenario characteristics in morphological box

Feature	Characteristic
Intention	Disturbance
	Financial gain
Target	Building room
	Plant component
Resources	Hand tools
	Pickup truck

The combination of characteristics results in a variety of scenarios. Table 3 shows the scenarios derived from Table 1.

3.1.2. *Spatial security system analysis*

The objective of the spatial security system analysis is to comprehensively consider potential attack paths. An attack path describes a way in which an offender can overcome the security system and reach the protected asset. We describe an attack path by its spatial course derived from a model of the security system.

Our model of the security system comprises two spatial elements: zones and barriers. These represent the effective areas of measures. We distinguish several types of zones according to the security function of the corresponding measures. We describe the following elements:

Protected zone: area which can be entered by an offender.

Observed zone: subarea of one or more protected zones in which an the offender can be detected.

Intervention zone: subarea of one or more protected zones in which an offender can be interrupted.

Barrier: border between protected zones at which an offender is delayed.

Asset: location within a protected zone that an offender attempts to reach.

For the sake of simplicity, we assume a single, system-wide intervention zone in the following steps.

Figure 1 shows a notional security system of a company site. It has a building on the left side and a plant on the right side. The two assets are the target objects within the morphological threat analysis: building room and plant component.

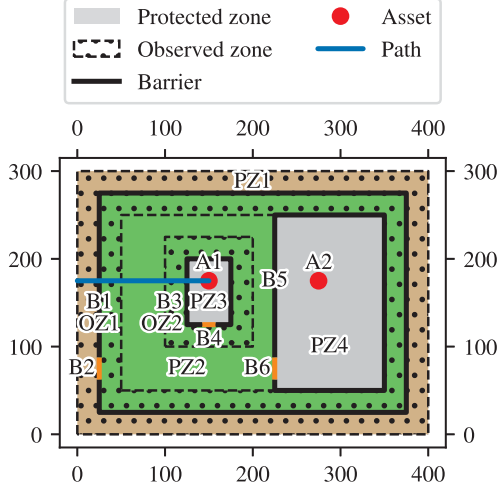


Fig. 1. Spatial model of security system

Physical attack paths can be derived from the spatial model. As an example, a path from outside left to the building room is shown in Fig. 1. The approach to systematically derive weakest attack paths is described in Section 3.2.1 in conjunction with the vulnerability model.

3.2. *Quantification of attack successfulness*

A common model to quantify security risk expresses risk R by the likelihood of attack T, the likelihood of success given attack V, and the consequence of a successful attack C (McGill et al., 2007):

$$R = T \times V \times C \tag{1}$$

Based on the identified attack scenarios, we quantify the likelihood of each attack scenario and its success. As we do not consider consequence in this paper, we combine T and V to the probability of a successful attack:

$$L = T \times V \tag{2}$$

We represent T by a scenario-defining threat likelihood model and V by a scenario-open vulnerability model.

3.2.1. *Vulnerability model*

The vulnerability model represents the sequence of an attack along a path in a specific scenario. The security system can stop the attack if it can detect and interrupt the offender. The security system's capabilities to detect and intervene are analyzed along the offender's progress over time, taking into account spatial information. Uncertainties for the effectiveness of security measures are represented by probability density functions for the model parameters. The path-time diagram in Fig. 2 illustrates the model described in the following using the path depicted in Fig. 1 as an example.

Along a path, an offender moves through zones and overcomes barriers. We denote the time in which an offender crosses a protected zone PZ*k* by $t_{\mathrm{P,PZ}k}$. We describe this in terms of the offender's average speed $v_{\mathrm{P,PZ}k}$ and the distance covered $s_{\mathrm{P,PZ}k}$:

$$t_{\mathrm{P,PZ}k} = \frac{s_{\mathrm{P,PZ}k}}{v_{\mathrm{P,PZ}k}} \tag{3}$$

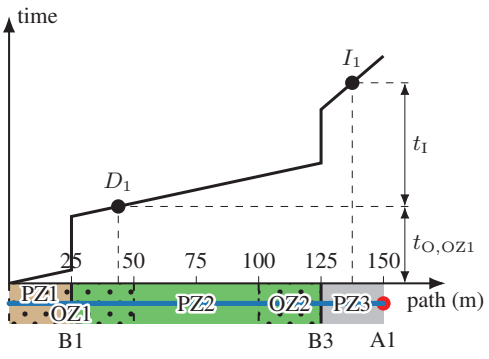


Fig. 2. Path-time diagram along an attack path

We refer to the time the offender is delayed in overcoming a barrier B*j* as $t_{\mathrm{P,B}j}$.

Detection takes place in observed zones. The event that an offender is detected in an observed zone OZ*i* is called D_i. We describe the probability of D_i by the time $t_{\mathrm{O,OZ}i}$ that the security system needs to detect the offender in the observed zone and the time $t_{\mathrm{P,OZ}i}$ that the offender is in the observed zone:

$$P(D_i) = P(t_{\mathrm{O,OZ}i} < t_{\mathrm{P,OZ}i}) \tag{4}$$

$t_{\mathrm{P,OZ}i}$ is the sum of the protection times of barriers and protected zones located in the observed zone.

We denote the event that an offender is interrupted after detection in OZ*i* by I_i. We describe the probability of I_i by the time t_I that the security system takes to interrupt the offender and the time $t_{\mathrm{RP,OZ}i}$ between detection and the event that the offender reaches the asset.

$$P(I_i \mid D_i) = P(t_\mathrm{I} < t_{\mathrm{RP,OZ}i}) \tag{5}$$

$t_{\mathrm{RP,OZ}i}$ is the remaining protection time starting at the observed zone OZ*i*. It is composed of the parts of protected zones and barriers that are in the observed zone and on the remaining attack path.

A path is vulnerable if the offender is not interrupted after moving through all observed zones. The probability of a path being vulnerable, the path vulnerability V_{Path}, is:

$$V_{\mathrm{Path}} = P\Big(\bigcup_i \bar{I}_i\Big) \tag{6}$$

We describe system vulnerability as the path vulnerability along the weakest path, i.e. the highest path vulnerability:

$$V_{\text{System}} = \max_{n}(V_{\text{Path},n}) \tag{7}$$

We use the spatial model of the security system to calculate the weakest path among the potential ones. To do this, we derive a graph of possible movement by discretizing the spatial model. The graph is shown in Fig. 3.

The calculated weakest paths and their respective vulnerabilities are presented in Fig. 3. For the calculation, we assume the parameter values given in Table 2. These depend on the resources used by the offender as defined in the morphological threat analysis.

Table 2. Security parameters of zones and barriers

Parameter	Value	
	Hand tools	Pickup truck
$v_{\text{P,PZ1}}$ (m/s)	2	15
$v_{\text{P,PZ2}}$ (m/s)	2	15
$v_{\text{P,PZ3}}$ (m/s)	1	1
$v_{\text{P,PZ4}}$ (m/s)	2	10
$t_{\text{P,B1}}$ (s)	$\mathcal{N}(250, 60^2)$	$\mathcal{N}(250, 60^2)$
$t_{\text{P,B2}}$ (s)	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
$t_{\text{P,B3}}$ (s)	$\mathcal{N}(250, 60^2)$	$\mathcal{N}(250, 60^2)$
$t_{\text{P,B4}}$ (s)	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
$t_{\text{P,B5}}$ (s)	$\mathcal{N}(250, 60^2)$	$\mathcal{N}(250, 60^2)$
$t_{\text{P,B6}}$ (s)	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
$t_{\text{O,OZ1}}$ (s)	$\mathcal{N}(100, 60^2)$	$\mathcal{N}(100, 60^2)$
$t_{\text{O,OZ2}}$ (s)	$\mathcal{N}(100, 60^2)$	$\mathcal{N}(100, 60^2)$
t_{I} (s)	$\mathcal{N}(200, 60^2)$	$\mathcal{N}(200, 60^2)$

3.2.2. *Threat likelihood model*

The threat likelihood model weights the scenarios in terms of their likelihoods. Assuming that a scenario occurs, we consider the probability distribution over the scenarios from the morphological threat analysis. The features within the morphological threat analysis are used as random variables, while the characteristics form the possible states of the random variables. The probability distribution of the scenario is the joint probability distribution

Path	V_{System}	Resources	Target
	0.017	Hand tools	Building room
	0.026	Hand tools	Plant component
	0.116	Pickup truck	Building room
	0.192	Pickup truck	Plant component

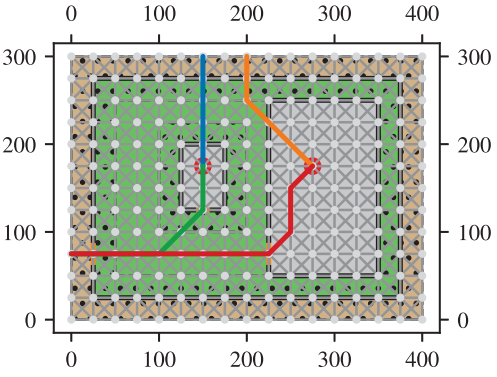


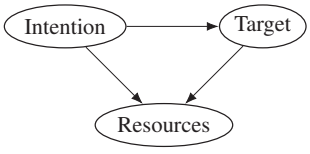
Fig. 3. Weakest attack paths and their vulnerability

P(Target | Intention)

Intention	Target	
	Build. room	Plant comp.
Disturb.	0.4	0.6
Fin. gain	0.8	0.2

P(Intention)

Disturb.	Fin. gain
0.2	0.8



P(Resources | Intention, Target)

Intention	Target	Resources	
		Hand tools	Pickup truck
Disturb.	Build. room	0.3	0.7
Disturb.	Plant comp.	0.1	0.9
Fin. gain	Build. room	0.9	0.1
Fin. gain	Plant comp.	0.8	0.2

Fig. 4. Threat likelihood model

of the scenario characteristics. We represent this in a Bayesian network by conditional probabilities:

$$P(S) = \prod_{k=1}^{K} P(C_k \mid \mathrm{pa}(C_k)) \tag{8}$$

Figure 4 shows the dependency graph and the probability tables of the Bayesian network for the notional example.

We describe the likelihood of a threat T by the likelihood that a certain scenario s_i occurs:

$$T(s_i) = P(S{=}s_i) \tag{9}$$

3.2.3. *Aggregation of attack successfulness*

The vulnerability model and threat likelihood model quantify the likelihood of an attack and its success for each individual scenario:

$$L(s_i) = T(s_i) \cdot V(s_i) \tag{10}$$

We denote the likelihood that one attack is successful out of several potential scenarios L_{agg}:

$$L_{\text{agg}} = \sum_i L(s_i) \tag{11}$$

L_{agg} represents the vulnerability weighted across scenarios. Table 3 shows the calculated values of V, T, L and L_{agg} across all scenarios for the example.

4. Case Study

In the following, we use the model described in Section 3 to comparatively study the influence of epistemic uncertainties in the scenario likelihood due to varying levels of available information. For this purpose, we define three cases representing different levels of knowledge about scenarios and their likelihoods. For each case, we assume different threat likelihoods by changing the probabilities in the threat likelihood model. The other models remain unchanged. The amount of available information increases from case 1 to case 3:

Case 1: knowledge about most likely scenarios. In the first case, we assume that no systematic scenario analysis was carried out, but instead only two plausible scenarios were set up for the two intentions of disturbance and financial gain. We assume that these are the two most likely scenarios in Table 3. To do this, we set the conditional probabilities for intention and target to 0 and 1, respectively, so that the scenarios occur with certainty. The marginal distribution of intention remains unchanged.

Case 2: knowledge about potential scenarios. In the second case, we assume that potential scenarios have been identified in a morphological threat analysis, but there is no information about probabilities of

Table 3. Attack successfulness by scenarios

Scenario			V	T	L
Intention	Target	Resources			(L_{agg})
Disturbance	Building room	Hand tools	0.017	0.024	0.000
Disturbance	Building room	Pickup truck	0.116	0.056	0.007
Disturbance	Plant component	Hand tools	0.026	0.012	0.000
Disturbance	Plant component	Pickup truck	0.192	0.108	0.021
Financial gain	Building room	Hand tools	0.017	0.576	0.010
Financial gain	Building room	Pickup truck	0.116	0.064	0.007
Financial gain	Plant component	Hand tools	0.026	0.128	0.003
Financial gain	Plant component	Pickup truck	0.192	0.032	0.006
					(0.055)

target and resources. We set these stochastically independent in the Bayesian network with uniformly distributed marginal distributions.

Case 3: knowledge about likelihoods of potential scenarios.

In the third case, we assume that potential scenarios have been identified in a morphological threat analysis and conditional probability distributions of all scenario characteristics are available. We use the values given in Fig. 4.

We calculate T, V and L for all three cases. The results are presented in Table 4. T and L are specific for each case (T_1, T_2, T_3 and L_1, L_2, L_3), while V remains unchanged. For a comparison across multiple scenarios, we also show L_{agg} for the intentions of disturbance and financial gain, as well as L_{agg} across scenarios in the analysis.

A comparison shows that all results for L_{agg} of case 3 are between case 1 and case 2. Across all scenarios: $L_{1,\text{agg}} < L_{3,\text{agg}} < L_{2,\text{agg}}$. When comparing the intentions, it is noticeable that the order of L_{agg} differs depending on the intention (disturbance: $L_{2,\text{agg}} < L_{3,\text{agg}} < L_{1,\text{agg}}$, financial gain: $L_{1,\text{agg}} < L_{3,\text{agg}} < L_{2,\text{agg}}$).

5. Discussion

Assuming that information about potential scenarios and their likelihoods is available and that uncertainties can be accurately modeled as in case 3, the risk by intended disturbance is overestimated and the risk by financial gain is underestimated in the example if only the most likely scenarios are considered in case 1. If potential scenarios are not weighted according to their likelihoods in case 2 this is the other way around in the example. The over- and underestimation may be strengthened by the fact that the vulnerability differs significantly depending on the used resources. An analysis of the influence considering a larger number of scenarios could lead to further insights into how likelihoods distribute and which scenarios get prioritized as a result.

For a risk-appropriate and effective design of security systems, the weakest path is an important design criterion for balanced protection. However, in the case study, the distribution of successful attacks over the assets varies depending on the available information. When considering only a few most likely scenarios in case 1, the risk of an attack on a plant component is high. However, when more scenarios are considered in case 2 and case 3, the risk of attacks on a building

Table 4. Comparison of attack successfulness for the case study

Scenario			V	T_1	T_2	T_3	L_1	L_2	L_3
Intention	Target	Resources					($L_{1,\text{agg}}$)	($L_{2,\text{agg}}$)	($L_{3,\text{agg}}$)
Disturbance	Building room	Hand tools	0.017	—	0.050	0.024	—	0.001	0.000
Disturbance	Building room	Pickup truck	0.116	—	0.050	0.056	—	0.006	0.007
Disturbance	Plant component	Hand tools	0.026	—	0.050	0.012	—	0.001	0.000
Disturbance	Plant component	Pickup truck	0.192	0.200	0.050	0.108	0.038	0.010	0.021
							(0.038)	(0.018)	(0.028)
Financial gain	Building room	Hand tools	0.017	0.800	0.200	0.576	0.014	0.003	0.010
Financial gain	Building room	Pickup truck	0.116	—	0.200	0.064	—	0.023	0.007
Financial gain	Plant component	Hand tools	0.026	—	0.200	0.128	—	0.005	0.003
Financial gain	Plant component	Pickup truck	0.192	—	0.200	0.032	—	0.038	0.006
							(0.014)	(0.070)	(0.027)
							(0.052)	(0.088)	(0.055)

room increases in comparison. This changes the importance of security measures along paths with this target and may have an impact on the design of security measures.

From the above, it becomes clear that epistemic uncertainties in the scenario likelihood can have an impact on decisions about the design of a security system. Therefore, it seems reasonable to take these uncertainties into account in the practical application of a security risk analysis. By making these uncertainties visible and analyzable, the proposed approach could serve as a basis for this application.

6. Conclusion

We presented an approach to comprehensively develop threat scenarios via a morphological analysis and analyze the vulnerability in each scenario via a unified time-based and probabilistic metric for detection and intervention along weakest paths. The weakest paths are derived from a pool of possible paths via a spatial analysis of the security system. We then use a model of scenario likelihood to weight the scenario-specific vulnerabilities identified, taking into account the uncertainties introduced in both steps.

The case study carried out shows that epistemic uncertainties in the scenario likelihood can lead to a different quantification of risk across scenarios. This can have an impact how risk is assessed, so that uncertain expert knowledge can lead to ineffective security design. Therefore, scenario uncertainties should be taken into account when optimizing security measures.

To better estimate and minimize distortion of results due to epistemic uncertainties, it appears to be rational to take a closer look at how the likelihood of the scenarios can be determined on the basis of expert knowledge elicitation.

References

Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems* (Second ed.). Amsterdam: Butterworth-Heinemann.

International Atomic Energy Agency (2011). Nuclear security recommendations on physical protection of nuclear material and nuclear facilities (INFCIRC/225/revision 5). IAEA Nuclear Security Series 13.

International Organization for Standardization (2018). Risk management – guidelines. ISO 31000.

Jang, S.-S., S.-W. Kwan, H.-S. Yoo, J.-S. Kim, and W.-K. Yoon (2009). Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection effectiveness (sape). *Nuclear Engineering and Technology 41*(5), 747–752.

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting & Social Change 126*, 116–125.

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 (2020). Comprehensive security hazard analysis for transmission systems. In A. Hughes, F. McNeill, and C. W. Zobel (Eds.), *ISCRAM 2020 Conference Proceedings, 17th International Conference on Information Systems for Crisis Response and Management*, pp. 1145–1153. Virginia Tech.

McGill, W. L., B. M. Ayyub, and M. Kaminskiy (2007, October). Risk analysis for critical asset protection. *Risk Analysis: An International Journal 27*(5), 1265–1281.

Paté-Cornell, E. and S. Guikema (2002). Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research 7*(4), 5–23.

Tekinerdoğan, B., K. Özcan, S. Yağız, and I. Yakın (2021, September). Model-based development of design basis threat for physical protection systems. In *2021 IEEE International Symposium on Systems Engineering (ISSE)*.

Witte, D., D. Lichte, and K.-D. Wolf (2020). Threat analysis: Scenarios and their likelihoods. In P. Baraldi, F. Di Maio, and E. Zio (Eds.), *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, pp. 4589–4595.

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.