Advances in Reliability, Safety and Security, Part 7 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-19-7 (printed), ISBN 978-83-68136-06-7 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

An Approach To The Analysis Of Security Measure Robustness Considering Epistemic Uncertainty In Scenario Likelihood

Dustin Witte[a], Daniel Lichte[b], Kai-Dietrich Wolf[a]

[a]*Institute for Security Systems, University of Wuppertal, Germany*
[b] *Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany*

Abstract

The current dynamic development of the security situation is pushing the risk of attacks on critical infrastructures further into the focus of both, operators and the authorities. Legislation requires critical infrastructure operators to take appropriate physical security and resilience measures. In this context, there are increased efforts to develop concepts for securing critical infrastructures against possible attacks. However, the lack of knowledge regarding the likelihood of threat scenarios causes epistemic uncertainty that impacts risk analysis. In previous work, we proposed a combination of models to make the influence of uncertainties visible: a threat model that describes a wide range of potential scenarios, a threat likelihood model, in which a probability distribution over these scenarios represents scenario likelihood, and a vulnerability model that enables the assessment of security measure effectiveness in these scenarios. Here, we extend that approach, thereby enabling the analysis of security measure robustness against vulnerability from scenarios with uncertain likelihood. For this purpose, we represent uncertain knowledge regarding that likelihood via prior distributions. Based on a notional example, we calculate vulnerability for three alternative configurations of security measures in a set of scenarios and weight that vulnerability by uncertain scenario likelihood. The resulting probability distributions show that the degree of variance in overall security measures effectiveness depends on the configuration of the security measures. Introducing simple robustness indicators, we compare the probability distributions and discuss their relevance for the robustness of security measures.

Keywords: physical security, security risk analysis, vulnerability, critical infrastructure protection, quantitative uncertainty assessment, robustness

1. Introduction

The current dynamic development of the security situation is pushing the risk of attacks on critical infrastructures further into the focus of both their operators and the authorities. Legislation requires operators to take appropriate physical security and resilience measures, for instance Directive (EU) 2022/2557. In this context, there are increased efforts to develop concepts for securing critical infrastructures against possible attacks. Most security risk analysis approaches represent risk by three factors: the likelihood of an attack, the vulnerability, i.e. the probability of an attacker reaching the asset, and the consequences of damage to or loss of that asset (McGill et al., 2007). A peculiarity of security analysis is the presence of intelligent actors. For risk analysis, this means that the number of potential threats is unbounded (Baybutt, 2017). At the same time, there is little evidence for attacks, which leads to significant uncertainties regarding the likelihood of attacks and actual effectiveness of measures in security concepts.

Since these uncertainties result to a large extent from the lack of knowledge regarding the likelihood of threat scenarios, it is therefore crucial to include a wide range of scenarios in the security risk analysis (Baybutt, 2017). Approaches that refer to a few selected scenarios in the analysis, such as the Design Basis Threat approach (Garcia, 2008; IAEA, 2021), can only incompletely map the existing security risks from this perspective. This leads to an incomplete security risk analysis and therefore to concepts that might not be risk-appropriate. At the same time, when a large number of scenarios are included, there is the problem that the actual probability of occurrence of scenarios is uncertain. This raises the question of how uncertainties can be dealt with in a comprehensive analysis.

At best, a resulting security concept would be robust against the uncertainties described, i.e. it would provide the best possible protection against a wide range of uncertain threat scenarios.

In Witte et al. (2023), we proposed an approach that aims for considering the existing uncertainties regarding occurring threat scenarios and the vulnerabilities in these scenarios. Additionally, we have shown that uncertainties in scenario likelihood can have an impact on risk quantification. Here, we extend that approach to enable the analysis of security measure robustness against vulnerability from scenarios with uncertain likelihood. For this purpose, we represent uncertain knowledge regarding that likelihood via prior distributions. Using a notional example, we calculate vulnerability for three alternative configurations for the design of security measures in a set of scenarios and weight that vulnerability by uncertain scenario likelihood. We compare the resulting probability distributions and discuss their relevance for the robustness of security measures.

2. Background

Some approaches to quantify security risk have been developed. For vulnerability, a widely used model bases on the approach described by Garcia (2008). In that approach, potential intrusion paths are identified first. Then, 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. Experts estimate probabilities and times in the respective scenarios.

In the case of scenario likelihood, two approaches can be distinguished. The first approach quantifies the likelihood of a scenario by an annual rate of occurrence. For instance, McGill et al. (2007) describe a rate based on estimates of the attractiveness of an asset and the attacker's awareness of the respective intrusion path based on perceived expected utility. This approach requires extensive information and assumptions about the behavior of potential attackers. The second approach models the likelihood as a probability distribution over a set of scenarios. Examples for that approach are Sarin (1978), Mahesh and Moskowitz (1990), Gordon (1994) and Witte et al. (2020). Here, only the likelihood relative between the potential scenarios is considered. Particular focus is given to the consistency of the estimates.

A common problem when using these approaches to determine the likelihood of scenarios is, that due to a lack of evidence of actual attacks, they have to rely on elicited expert knowledge. So far, no method is established that explicitly analyzes the robustness of security measures against resulting uncertainty in scenario likelihood estimation in security risk analysis. However, the elicitation of probabilities from expert judgements is a common problem and has been discussed in literature e.g. by O'Hagan et al. (2006). As expert knowledge elicitation is based on the concept of subjective probability as utilized in Bayesian statistics, the latter enables to describe the knowledge about an uncertain quantity, in this case the scenario likelihood, by prior distributions. The description of knowledge by prior distributions is used to estimate probabilities, for example in probabilistic risk assessment (Siu and Kelly, 1998).

3. Approach

In the following, we present an approach that captures uncertainties in the estimation of the likelihood of scenarios in a model by prior distributions and thus enable an analysis of the robustness of security measure configurations against this uncertainty. The approach is based on the models of threat, threat likelihood and vulnerability we described in Witte et al. (2023). Consequences of a successful attack are not analyzed here. We demonstrate the approach using a notional example.

In a first step, we briefly introduce the underlying models. Then, we extend the threat likelihood model to represent uncertainties in the likelihood estimation by prior distributions. Finally, we analyze the robustness of three notional security measure configurations considering these uncertainties given by a hypothetical probability distribution.

3.1. Underlying models

3.1.1. Threat model

The threat model describes potential threat scenarios by using morphological analysis. In that analysis, we identify relevant features for an abstract scenario description. In the following, we refer to a simple example: an attacker with an *intention* tries to reach a *target* object by using *resources*. To describe specific threat scenarios, we collect potential characteristics for each feature. Table 1 shows a simplified example. By combining the characteristics, one for each feature, we can construct a variety of scenarios, here 2^3 scenarios.

Table 1. Scenario characteristics in a morphological box.

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

3.1.2. Threat likelihood model

The threat likelihood model describes a weighting of scenarios in terms of their likelihoods. Assuming that a scenario occurs, we consider the probability distribution over the scenarios derivable from the threat model. We denote the occurring scenario by S and consider the features within the morphological analysis as random variables, denoted by C_n. The characteristics form the possible states of the random variables. The probability distribution over all scenarios is the joint probability distribution of the scenario characteristics. We represent this in a Bayesian network by conditional probabilities:

$$P(S) = \prod_n P\big(C_n \mid \text{parents}(C_n) \big) \tag{1}$$

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

$$T(s_i) = P(S = s_i) \tag{2}$$

3.1.3. Security system model

The security system model describes the effect of security measures for delaying, detecting and interrupting an attack. Zones and barriers represent effective areas of measures, and time-based parameters describe the effectiveness of these measures in each zone or barrier as given in Table 2. Uncertainties for the effectiveness of security measures are represented by probability density functions for the model parameters. Figure 2 shows the layout of a notional security system of a company site. On the left-hand side is a building with control technology, on the right-hand side a plant. The two assets are the target objects within the threat model: control technology room and plant component. For the sake of simplicity, we assume a single, system-wide intervention zone.

Table 2. Elements and parameters of security system model.

Element		Parameter
Protected zone:	area which can be entered by an attacker.	Intrusion speed v_P (m/s)
Detection zone:	subarea of one or more protected zones in which an attacker is observed and can be detected.	Observation time t_O (s)
Intervention zone:	subarea of one or more protected zones in which an attacker can be interrupted.	Intervention time t_I (s)
Barrier:	border between protected zones at which an attacker is delayed.	Protection time t_p (s)
Asset:	location within a protected zone that an attacker attempts to reach.	–

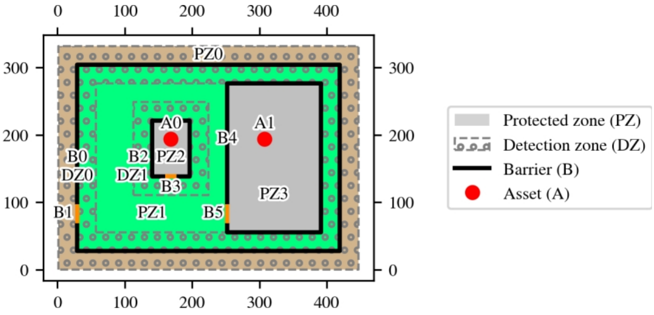


Fig. 1. Layout of notional security system.

3.1.4. Vulnerability model

The vulnerability model describes the probability of an attack being successful along an intrusion path, i.e. the attack is not stopped by an intervention. The security system can stop the attack if it can detect and interrupt the attacker in time, e.g. by security forces. The security system's capabilities to delay, detect and intervene are analyzed along the attacker's progress over time based on the spatial and time data from the security system model. This results in the probability of a path being vulnerable, i.e. the path vulnerability V_{Path} (Witte et al., 2023).

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

$$V_{\mathrm{System}} = \max_{m}(V_{\mathrm{Path},m}) \tag{3}$$

Using the spatial model of the security system, we are able to calculate the weakest path among the potential ones.

3.2. Extension to the threat likelihood model

We extend the threat likelihood model introduced in section 3.1.2 to represent uncertainties in the estimation of the likelihood of scenarios. As described by equation (1), the Bayesian network decomposes the probability of a threat scenario into a joint probability of scenario features. In that context, we consider the scenario features as random variables using categorical distributions. These distributions describe that one out of a set of K characteristics occurs, parametrized by the probabilities $p_1, \dots, p_{K-1}$ for the respective characteristic:

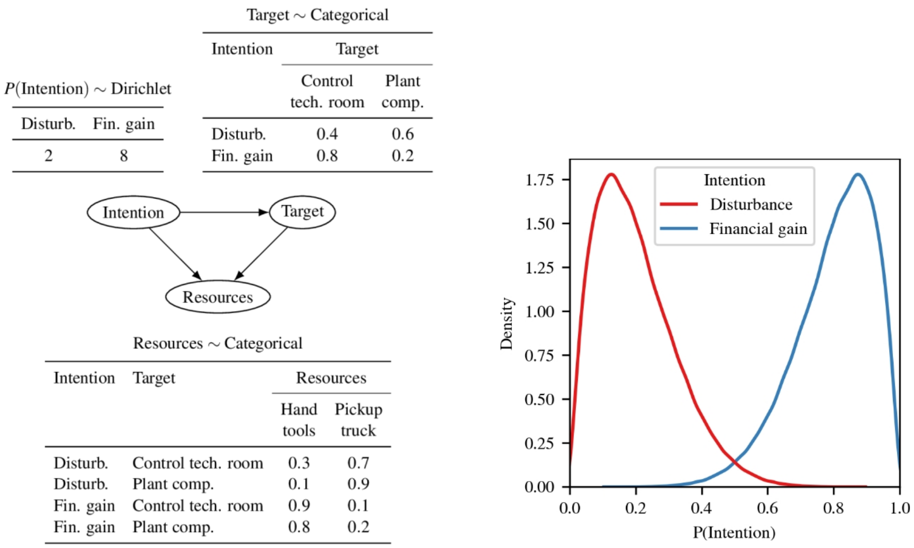
$$C_n \sim \mathrm{Categorical}(p_1, \dots, p_{K-1}) \tag{4}$$

To take into account that the estimation of the parameters $p_1, \dots, p_{K-1}$ may be subject to uncertainties, we assume the parameters themselves to be random variables. To describe their distribution, we use a Dirichlet distribution (Balakrishnan and Nevzorov, 2003), which is parametrized by $\alpha_1, \dots, \alpha_K$ i.e. one parameter more than the categorical distribution:

$$P(C_n) \sim \mathrm{Dirichlet}(\alpha_1, \dots, \alpha_K) \tag{5}$$

The Dirichlet distribution is the simplest appropriate multivariate distribution and approaches to elicit expert knowledge for Dirichlet distributions are discussed in literature, e.g. by Zapata-Vázquez et al. (2014).

For the sake of simplicity, we assume only the probability of intention to be Dirichlet distributed in the following, but in principle, the parameters of every categorical distribution in the Bayesian network could be Dirichlet distributed. Figure 2a shows a notional dependency graph and parameter tables of the Bayesian network for the example. Figure 2b illustrates the marginal probability density functions (pdf) of the Dirichlet distribution for the chosen parameter values. Note that $P(\mathrm{Intention} = \mathrm{Disturbance})$ is very likely to be greater than $P(\mathrm{Intention} = \mathrm{Financial\ gain})$, but the ratio of the two probabilities is uncertain.



(a)

(b)

Fig. 2. Threat likelihood model: (a) dependency graph and parameter tables, (b) marginal pdf of intention probability.

3.3. Robustness analysis of measure effectiveness

Given the uncertainty in scenario likelihood modeled as above, we can analyze its influence on vulnerability across scenarios. In the following, we do this by comparing the aggregated vulnerabilities of three hypothetical security measure configurations. We assume the parameter values shown in Table 3, representing normal distributed times with given mean and variance for respective measures.

Table 3. Parameters for three configurations of security measures.

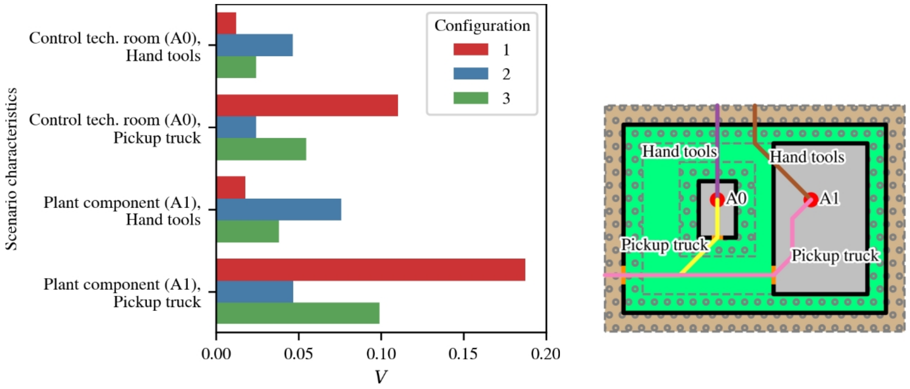
Parameter	Configuration	Resources	
		Hand tools	Pickup truck
$v_{\mathrm{P,PZ0}}$ (m/s)	1/2/3	2	15
$v_{\mathrm{P,PZ1}}$ (m/s)	1/2/3	2	15
$v_{\mathrm{P,PZ2}}$ (m/s)	1/2/3	1	1
$v_{\mathrm{P,PZ3}}$ (m/s)	1/2/3	2	10
$t_{\mathrm{P,B0}}$ (s)	1	$\mathcal{N}(260, 60^2)$	$\mathcal{N}(360, 60^2)$
	2	$\mathcal{N}(200, 60^2)$	$\mathcal{N}(300, 60^2)$
	3	$\mathcal{N}(230, 60^2)$	$\mathcal{N}(330, 60^2)$
$t_{\mathrm{P,B1}}$ (s)	1	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
	2	$\mathcal{N}(380, 60^2)$	$\mathcal{N}(280, 60^2)$
	3	$\mathcal{N}(340, 60^2)$	$\mathcal{N}(240, 60^2)$
$t_{\mathrm{P,B2}}$ (s)	1/2/3	$\mathcal{N}(250, 60^2)$	$\mathcal{N}(250, 60^2)$
$t_{\mathrm{P,B3}}$ (s)	1/2/3	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
$t_{\mathrm{P,B4}}$ (s)	1/2/3	$\mathcal{N}(250, 60^2)$	$\mathcal{N}(250, 60^2)$
$t_{\mathrm{P,B5}}$ (s)	1/2/3	$\mathcal{N}(300, 60^2)$	$\mathcal{N}(200, 60^2)$
$t_{\mathrm{O,DZ0}}$ (s)	1/2/3	$\mathcal{N}(100, 60^2)$	$\mathcal{N}(100, 60^2)$
$t_{\mathrm{O,DZ1}}$ (s)	1/2/3	$\mathcal{N}(100, 60^2)$	$\mathcal{N}(100, 60^2)$
t_{I} (s)	1/2/3	$\mathcal{N}(200, 60^2)$	$\mathcal{N}(200, 60^2)$

The configurations differ in the delay measures at the perimeter. In configuration 1, the fence offers a longer delay. In configuration 2, the gate offers a longer delay. In configuration 3, the delay at the fence and at the gate is between those in the other two configurations. The specific delay times depend on the resources used by the attacker as defined in the threat model: hand tools and pickup truck.

We calculate system vulnerability for each scenario and configuration according to the vulnerability model. The resulting weakest paths and their respective vulnerability V are presented in Fig. 3. Additionally, we calculate the scenario likelihood T according to the extended threat likelihood model for each derivable scenario. As a result, we obtain probability density functions of T for each scenario. Figure 4 shows a violin plot of the probability densities for the distributions of T on the left side. Given these calculations, we weight the vulnerabilities V by scenario likelihood T and call the result attack successfulness L:

$$L = T \times V \tag{6}$$

Figure 4 shows a violin plot of the distributions of L calculated by weighting V with T for each security measure configuration on the right side. Note that for better readability, we have normalized the probability density in the violin plot, as there are large differences in the density depending on the scenario and configuration. The differences can still be recognized by the different spread of the density.



(a)

(b)

Fig. 3. Vulnerability of weakest paths: (a) vulnerability values, (b) spatial course of weakest paths.

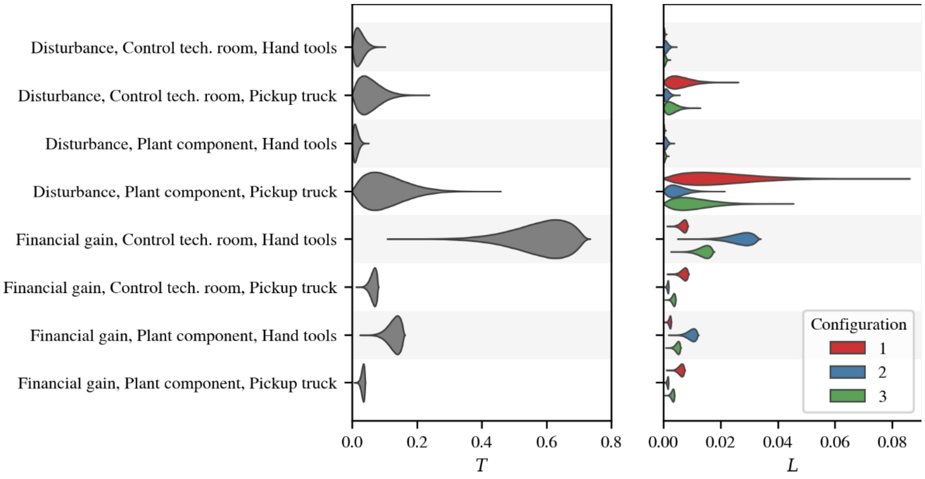


Fig. 4. Probability density of threat likelihood T and attack successfulness L for each scenario.

Note that by weighting the vulnerabilities by scenario likelihood, we consider two factors of the three-factor risk model: V by a scalar value in each scenario, and T by a random variable representing the uncertainty in expert knowledge in each scenario. We omit consequences for the sake of simplicity.

To compare the weighted vulnerabilities across all scenarios we aggregate L over all scenarios:

$$L_{\mathrm{agg}} = \sum_i L(s_i) \tag{7}$$

Figure 5 shows the probability density of L_{agg} for each security measure configuration. The distributions show the influence of the variance induced uncertainty in scenario likelihood. The lower the expected value $\mathrm{E}(L_{\mathrm{agg}})$, the greater the reduction in vulnerability across all scenarios as a result of the respective security measures. The lower the variance $\mathrm{Var}(L_{\mathrm{agg}})$, the lower the influence of uncertainty in scenario likelihood on that vulnerability reduction. Additionally, we can compare the robustness of the security measure configurations. For this purpose, we calculate the probability that a configuration reduces aggregated attack successfulness more than another configuration does: $P(L_{\mathrm{agg},j} < L_{\mathrm{agg},i})$. Table 4 lists these indicators calculated from the distributions of the example.

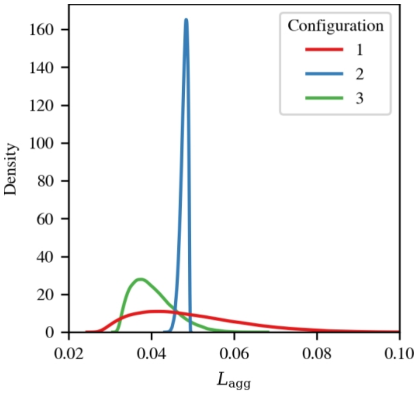


Fig. 5. Probability density of aggregated attack successfulness.

Table 4. Comparison of aggregated attack successfulness for security measure configurations.

Indicator	Configuration j		
	1	2	3
$\mathrm{E}(L_{\mathrm{agg},j})$	0.049	0.048	0.040
$\mathrm{Var}(L_{\mathrm{agg},j})$	0.013^2	0.001^2	0.005^2
$P(L_{\mathrm{agg},j} < L_{\mathrm{agg},1})$	–	0.470	0.890
$P(L_{\mathrm{agg},j} < L_{\mathrm{agg},2})$	0.530	–	0.883
$P(L_{\mathrm{agg},j} < L_{\mathrm{agg},3})$	0.110	0.117	–

4. Discussion

The three configurations of security measures examined show clear differences in robustness against uncertainty in scenario likelihood. Configurations 1 and 2 have almost the same expected value for aggregated attack successfulness but the respective variance differs significantly (see Fig. 5). This is mainly due to the scenario, in which an attacker with an intention of disturbance tries to reach a plant component by using a pickup truck, as vulnerability in configuration 1 is outstanding high in that scenario (see Fig. 3) but scenario likelihood is uncertain (see Fig. 4). On the one hand, this shows that uncertainty in scenario likelihood can have a considerable impact on the validity of the results of the security risk analysis, but on the other hand, it also shows that the influence of these uncertainties can be reduced by selecting appropriate security measures, e.g. as in configuration 2 where variance is low. In our example, no best configuration can be determined, as the attack successfulness does not allow for a clear distinction due to its variance. However, configuration 3 reduces vulnerability most robust in comparison, as the probability that the attack successfulness is lower compared to the other configurations is high (see Table 4).

In order to reliably reduce the influence of uncertainties, they must first be accurately considered when eliciting expert knowledge. The approach presented here assumes that this can be achieved by representing the knowledge in Dirichlet distributions. However, as Zapata-Vázquez et al. (2014) point out, experts can make statements that cannot be represented by a Dirichlet distribution. Generalizations of the Dirichlet distribution could provide a solution, yet expert statements must be consistent with the axioms of probability theory.

5. Conclusion

We presented an approach to represent uncertainties in the estimation of scenario likelihood and analyze the influence of the variance in that estimation on the robustness of security measure effectiveness by using prior distributions. In a notional example, we analyzed the robustness of vulnerability reduction for three configurations of security measures. The analysis builds on a threat model that describes a wide range of potential scenarios, a threat likelihood model, in which a probability distribution over those scenarios represents scenario likelihood, and a vulnerability model that enables the assessment of security measure effectiveness in those scenarios.

The analysis results show that the degree of variance in overall security measures effectiveness depends on the configuration of the security measures. To enable the estimation of the robustness of configurations considering this influence, we propose simple indicators.

Although we restrict ourselves to the use of Dirichlet distributions, other forms of distribution to represent the uncertainties are possible. It is reasonable to assume that these tend to increase the effect of uncertainties on robustness. A more in-depth analysis of a more complex system could provide further insights here. Especially if suitable prior distributions for elicited knowledge are used for a broader range of scenarios.

Nevertheless, our approach has the potential to support the selection of the best possible configuration that considers the uncertain state of knowledge regarding threat scenario likelihood.

References

Balakrishnan, N. and V. B. Nevzorov, 2003. A Primer on Statistical Distributions. Wiley-Interscience, Hoboken, New Jersey. isbn: 0-471-42798-5. doi: 10.1002/ 0471722227.

Baybutt, P., Sept. 2017. Issues for security risk assessment in the process industries. In: Journal of Loss Prevention in the Process Industries 49, pp. 509–518. issn: 0950-4230. doi: 10.1016/j.jlp.2017.05.023.

Directive (EU) 2022/2557, Dec. 14, 2022. Directive on the resilience of critical entities and repealing Council Directive 2008/114/EC. European Parliament and Council of the European Union.

Garcia, M. L., 2008. The Design and Evaluation of Physical Protection Systems. 2nd ed. Butterworth-Heinemann, Amsterdam et al. 370 pp. isbn: 978-0-7506-8352-4. doi: 10.1016/C2009-0-25612-1.

Gordon, T. J., 1994. Cross-Impact Method. In: Millennium Project. Futures Research Methodology.

International Atomic Energy Agency (IAEA), 2021. National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. Implementing Guide 10-G (Rev. 1). issn: 1816–9317. isbn: 978-92-0-131120-7.

Mahesh, S. and H. Moskowitz, Sept. 1990. An Information-Maximizing Interactive Procedure for Scenario Probability Elicitation. In: Decision Sciences 21.3, pp. 533–550. issn: 1540-5915. doi: 10.1111/j.1540-5915.1990.tb00332.x.

McGill, W. L., B. M. Ayyub, and M. Kaminskiy, Oct. 1, 2007. Risk Analysis for Critical Asset Protection. In: Risk Analysis: An International Journal 27.5, pp. 1265–1281. issn: 0272-4332. doi: 10.1111/j.1539-6924.2007.00955.x.

O'Hagan, A. et al., 2006. Uncertain Judgements. Eliciting Experts' Probabilities. Statistics in Practice. John Wiley & Sons. doi: 10.1002/0470033312.

Sarin, R. K., Feb. 1978. A sequential approach to cross-impact analysis. In: Futures 10.1, pp. 53–62. issn: 0016-3287. doi: 10.1016/0016-3287(78)90143-X.

Siu, N. O. and D. L. Kelly, Oct. 1998. Bayesian parameter estimation in probabilistic risk assessment. In: Reliability Engineering & System Safety 62.1–2, pp. 89–116. issn: 0951-8320. doi: 10.1016/s0951-8320(97)00159-2.

Witte, D., D. Lichte, and K.-D. Wolf, 2020. Threat Analysis: Scenarios and Their Likelihoods. In: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (Venice, Italy, Nov. 1–6, 2020). Ed. by P. Baraldi, F. Di Maio, and E. Zio, pp. 4589–4595. isbn: 978-981-14-8593-0. doi: 10.3850/978-981-14-8593-0_4283-cd.

Witte, D., D. Lichte, and K.-D. Wolf, 2023. On the Impact of Epistemic Uncertainty in Scenario Likelihood on Security Risk Analysis. In: Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023) (Southampton, United Kingdom, Sept. 3–7, 2023). Ed. by M. P. Brito et al. Research Publishing, Singapore. isbn: 978-981-18-8071-1. doi: 10.3850/978-981-18-8071-1_P603-cd.

Zapata-Vázquez, R. E., A. O'Hagan, and L. Soares Bastos, Sept. 2, 2014. Eliciting expert judgements about a set of proportions. In: Journal of Applied Statistics 41.9, pp. 1919–1933. issn: 0266-4763. doi: 10.1080/02664763.2014.898131.