Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

Cost Benefit Analysis For Critical Infrastructure Protection: Effectively Balancing Security And Resilience

Daniel Lichte[a], Tobias Demmer[a], Dustin Witte[b], Lukas Halekotte[a]

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

Keywords: critical infrastructure protection, security, resilience, cost benefit analysis, decision making, uncertainty

The protection of infrastructures is becoming increasingly important at an international level in the context of dynamic changes to the security situation. For example, the European Commission has drafted a directive on this topic (European Council, 2022), which has led to legislative measures throughout Europe, such as the "KRITIS-Dachgesetz" in Germany. Its implementation will foreseeably lead to major regulatory and operator-related costs, meaning that the selection of measures with the best possible effectiveness and economic appropriateness will be of paramount importance. This leads to a number of unresolved issues, which relate in particular to a sensible balance between securing critical entities and introducing measures to increase their resilience under existing uncertainties.

Measures to protect infrastructures against deliberate attacks can be roughly divided into two areas: (1) The prevention of successful attacks through security. (2) The reduction of the impact of such attacks by resilience enhancing measures to increase the ability to deal with disruptions caused by attacks on the infrastructure (Mentges et al., 2023). However, the measures from both areas hardly overlap and are usually associated with large investments, so that an efficient compromise must be made due to cost restrictions. At the same time, due to a lack of evidence, there is a high level of uncertainty regarding future thread scenarios and the related effectiveness of measures from both areas, which makes selection even more difficult.

In security in particular, there are some approaches that deal with cost-effectiveness analyses (Lichte and Wolf, 2018; Villa et al., 2017). However, these are hardly widespread in the field of resilience, and a consideration of both areas from a cost-benefit perspective is still missing.

Figure 1 outlines our approach, which we implement as an exemplary model. It is fundamentally based on the security risk model, which consists of the components threat, vulnerability and consequences (McGill, 2007).

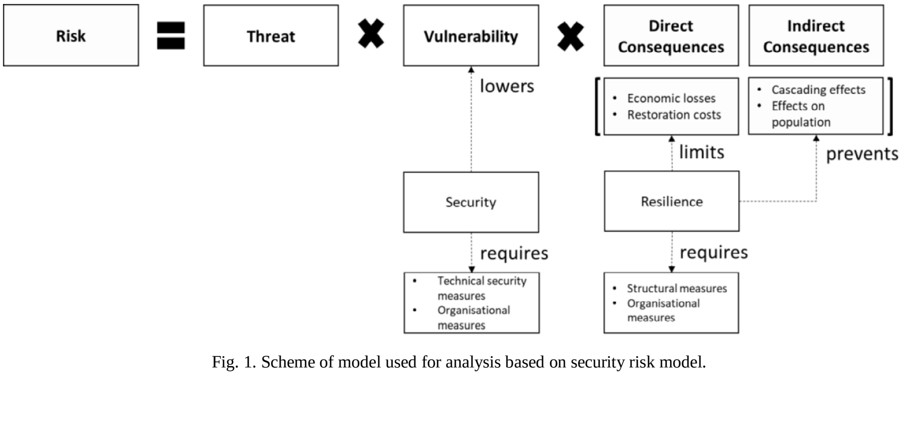

Fig. 1. Scheme of model used for analysis based on security risk model.

We link the assessment of security and resilience by incorporating the effectivity of measures of both sub-areas into the risk function. The effectivity is assessed in two different models. In the context of vulnerability, we use the "Estimate of Adversary Sequence Interruption" approach (EASI), e.g. described in Garcia, M. (2001), to analyse the ability of security measures to thwart an attack. Here, vulnerability is parametrised by the probability of detection and intervention based on a time comparison between the time to overcome protective measures and the time needed to interrupt the attacker. Exemplarily, we vary these parameters to describe the effectiveness of measures.

The impact of attacks that are successful despite security measures can be mitigated by additional measures to enhance resilience. Thus, we integrate the description of the resilience of the critical entity under consideration into the consequences as part of the risk function. On the one hand, direct effects, e.g. costs for the operator, are addressed here. On the other hand, we consider indirect effects, which are a consequence of the disruption, e.g. failures in the supply to the population, which may cascade through other entities. For this purpose, we use an abstract model based on a double-logistic function that depicts the performance of the critical entity in the form of a curve in the event of disruptions (Demmer et al., 2022):

$$Q(t) = P + \frac{L_1}{\left(1+e^{-k_1*(t-t_1)}\right)} + \frac{L_2}{\left(1+e^{-k_2*(t-t_2)}\right)}. \tag{1}$$

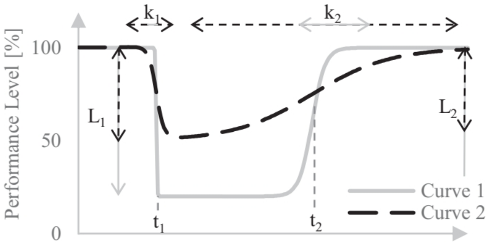

Fig. 2. Explanation of parameters in double-logistic function.

The parameters L_1, L_2, k_1, k_2, t_1 and t_2 in (1) characterise the shape of the performance curve (Figure 2). Our approach is to vary these parameters to manipulate the performance function in order to integrate the effectiveness of measures. Using this curve, we can then estimate the loss of performance in the event of a successful attack. For the sake of simplicity, we assume that the level of performance loss correlates with the indirect effects (see Figure 1). Exemplarily, we define a small number of potential attack scenarios for the threat, each of which is assigned an individual frequency of occurrence for a defined period of time.

The costs of the measures from both areas are defined in simplified form for a limited number of possible measures in order to enable a cost-benefit analysis. All parameters are assumed to be randomly distributed variables in order to consider the uncertainty regarding the possible scenarios and the effectiveness of the measures, as well as the possible effects and costs. Using a Monte Carlo simulation, we calculate the resulting risk of the assumed threats and the risk reduction achieved by the risk measures for all possible configurations. In addition, we determine the associated costs of the configurations. With the help of these results, we show how the proposed approach enables balancing of security- and resilience-enhancing measures by analysing costs of security and resilience measures and their respective contribution to risk reduction. Finally, we discuss the possibilities of the proposed approach and in-depth research approaches.

References

Demmer, T., Kahlen, J., Lichte, D., Wolf, K.-D. 2022. Towards the Prediction of Resilience: An Equation-based Resilience Representation. 32nd European Safety and Reliability Conference (ESREL 2022). Research Publishing, Singapore.

Council of the European Union. 2022. Directive (EU) 2022/2557 OF THE EUROPEAN PALIAMENT AND OF THE COUNCIL of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union. 27.12.2022, L 333/164-L 333/198.

Garcia, M. 2001. The design and evaluation of physical protection systems. Elsevier Science, Burlington.

McGill, W. L., Ayyub, B. M., Kaminskiy, M. 2007. Risk Analysis for Critical Asset Protection. Risk Analysis 27, 1265-1281.

Mentges, A., Halekotte, L., Schneider, M., Demmer, T., Lichte, D. 2023. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. International Journal of Disaster Risk Reduction 96, 103893.

Lichte, D., Wolf, K.-D. 2018. Approach to a Bayesian Descision Model for Cost-Benefit Analysis in Security Risk Management. European Safety and Reliability Conference (ESREL 2018).

Villa, V., Renier, G., Paltrinieri, N., Cozzani, V. 2017. Development of an economic model for counter terrorism measures in the process-industry. Journal of Loss Prevention in the Process Industries 49, 437-460.