Advances in Reliability, Safety and Security

ESREL 2024
Collection of Extended Abstracts

On Pareto Optimality In Cost Effectiveness Analysis Of Physical Security Concepts

Dustin Witte, Daniel Lichte, Kai-Dietrich Wolf

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

Keywords: Cost-Benefit Analysis, physical security, vulnerability, critical infrastructure protection, Pareto Optimality, decision-making

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. In doing so, two overriding conflicting criteria must be taken into account when designing security systems: their vulnerability against attacks and their expenses in terms of capital and operational costs. Cost-effectiveness models have been developed, e.g. by Hicks et al. (1999) and Villa et al. (2017), but the in principle unbounded number of possible attack scenarios poses challenges as Baybutt (2017) points out. On the one hand, the effectiveness of security measures in terms of vulnerability for each scenario is cumbersome to evaluate; on the other hand, the relevance of individual scenarios is very uncertain due to a lack of evidence. It is therefore difficult to estimate the probability of occurrence of various scenarios. Additionally, there is no precise definition of appropriateness with regard to scenarios to consider. However, cost-efficiency of security measures depends on the effectiveness against attack scenarios relevant to the operators of the critical infrastructures and related expenses and is very likely to be one decision criterion together with a suitable definition of appropriateness.

To support decision making on appropriate security system designs, we therefore propose to compare expenses and effectiveness of design alternatives based on a precise definition of relevant scenarios. We suggest determining relevant scenarios by defining scenario-related protection objectives that a security concept should fulfill. We suggest basing the objectives on the criticality in the sense of impact of loss of the threatened assets. This way, decision makers can choose the aimed protection without knowing the actual probability of occurrence of scenarios. We then can relate the fulfilment of these protection objectives to the costs of alternative security system configurations. On this basis, we can identify Pareto-optimal security system configurations, out of which a selection may be narrowed by the operator's assessment of appropriateness.

We illustrate the approach with a notional example. To show the impact of asset criticality on cost-effectiveness analysis, we assume that several sites of a critical infrastructure need to be protected. For the sake of simplicity, we further assume that the security systems to be designed should follow the same design layout for all sites. Figure 1 depicts the layout consisting of one asset and two layers of physical protection: perimeter and building protection. In a first step, we develop potential scenarios in which the assets are threatened. Then we classify the assets of each site into different levels of criticality and define protection objectives for each criticality level. Table 1 shows an example. Here, we limit the analysis to the likelihood of a successful attack in three simplified scenarios. We assume a number of options for the security measures with different effectiveness and costs and analyze their ability in preventing an attack success via a vulnerability model as described in Witte et al. (2023). We then visualize the maximal vulnerability calculated for the relevant scenarios as a function of security system cost in a cost-vulnerability diagram (Figure 2). This diagram can support decision making by using

the ratio between cost increase and vulnerability reduction of Pareto-optimal configurations as an indicator for an appropriate security system design.

Table 1. Protection objectives.

Scenario	Objective depending on asset criticality level		
	Level 1	Level 2	Level 3
Trespass	Prevent	Prevent	Prevent
Theft	–	Prevent	Prevent
Sabotage	–	–	Prevent

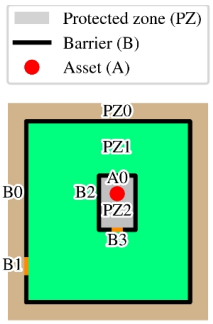

Fig. 1. Security system layout.

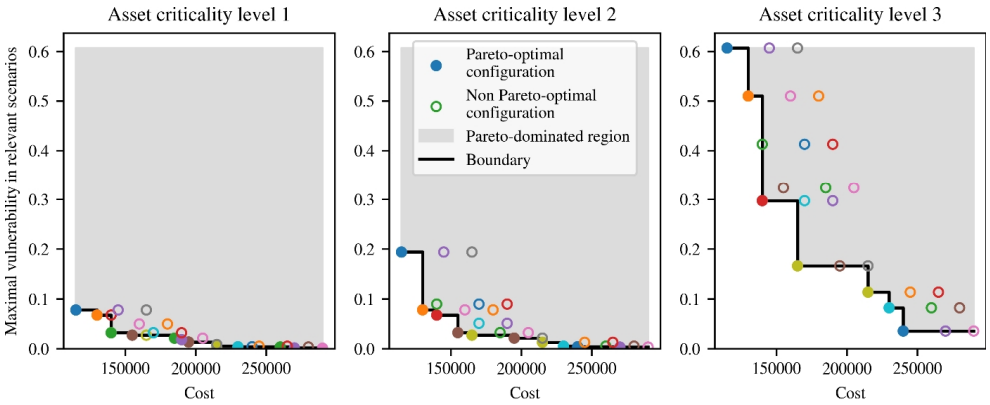

Fig. 2. Cost-vulnerability diagrams of security system configurations.

References

Baybutt, P., Sept. 2017. Issues for security risk assessment in the process industries. In: Journal of Loss Prevention in the Process Industries 49, 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.

Hicks, M. et al., Apr. 1999. Physical Protection Systems – Cost and Performance Analysis: A Case Study. In: IEEE Aerospace and Electronic Systems Magazine 14.4, 9–13. issn: 1557-959X. doi: 10.1109/62.756078.

Villa, V. et al., Sept. 2017. Development of an economic model for counter terrorism measures in the process-industry. In: Journal of Loss Prevention in the Process Industries 49, 437–460. issn: 0950-4230. doi: 10.1016/j.jlp.2017.06.001.

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.