Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P0437-cd

On Pareto Optimality of Physical Security Concepts Balancing Multiple Protection Objectives

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

Eva-Louisa Hefler
German Aerospace Center (DLR), Institute for the Protection of Terrestrial Infrastructures, Germany. E-mail: eva.hefler@dlr.de

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

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

Operators of critical infrastructures are confronted with safeguarding their assets against a wide range of potential threats. Conventional risk analysis include the assessment of scenario likelihoods, but for security risks, these are difficult to estimate. This poses a significant challenge for decision making. In order to configure a physical security system, an approach for decision making considering these uncertainties must be found. As a solution, we propose to specify multiple protection objectives and base the formulation of the decision problem on the fulfillment of these protection objectives as well as security system cost. In our approach, we initially develop relevant scenarios via morphological analysis. Based on these scenarios, we define site-specific protection objectives including minimum requirements and analyze their fulfillment by qualitative or quantitative models, depending on the level of available information. With these models, we search for Pareto-optimal security system configurations regarding protection objectives and costs. We demonstrate our approach using a notional case study on a generic critical infrastructure site. There, the conducted optimization yields a manageable number of optimal configurations. Additionally, the resulting optimal configurations show varying trade-offs between protection objectives, as well as costs. Out of this Pareto-optimal set, a selection may be narrowed by the operator's assessment of appropriateness. In this way, the proposed approach enables operators to identify an optimal security system configuration that is tailored to their specific requirements, thus supporting decision making.

Keywords: Cost-Benefit Analysis, Physical Security, Vulnerability, Critical Infrastructure Protection, Pareto Optimality, Multi-Criteria Decision-Making.

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 such as the CER Directive (2022) requires operators to take appropriate physical security and resilience measures, which makes the development of concepts for securing critical infrastructures against possible attacks necessary. Conventional risk analysis includes the estimation of the likelihood of threat scenarios. However, these likelihoods are difficult to estimate due to freedom of offenders' choice (Baybutt, 2017). Yet, the effectiveness of security measures can be based on protection objectives (Garcia, 2008). Generally, these protection objectives will be in conflict with the objective of minimizing costs, resulting in a multi-criteria decision problem.

To support decision making on appropriate security system designs, we therefore propose to relate costs to the fulfillment of protection objectives, basing the analysis on a comprehensive set of scenarios to ensure the coverage of relevant scenarios

by security measures.

We demonstrate the approach alongside a notional example of a generic site considering alternative measures of perimeter and building protection. In order to consider scenarios systematically, we apply a morphological scenario analysis. Then, we define site-specific protection objectives and analyze their fulfillment by qualitative or quantitative models, depending on the level of available information. Based on this fulfillment and the costs of security measures, we calculate Pareto-optimal security system configurations, out of which a selection may be narrowed by the operator's assessment of appropriateness.

2. Methods

We use the following methods, models and existing approaches as a basis.

2.1. *Morphological scenario analysis*

Morphological scenario analysis explores the space of possible scenarios (Ritchey, 2006; Johansen, 2018). The scenario space is divided into multiple dimensions of uncertainty. For each dimension, a set of possible instances is identified. Thus, a scenario describes a set of instances that specify each dimension.

The Cartesian product over all dimensions yields all possible combinations, i.e. scenarios. A subsequent consistency assessment filters consistent scenarios by judging the consistency of all pairs of characteristics. Only scenarios that have no inconsistent pairs are consistent and are included in further analyses.

2.2. *Pareto optimality in security assessment*

The assessment of physical security measures is based on scenario-specific protection objectives (Garcia, 2008). The fulfillment of each protection objective represents a decision criterion of a multi-criteria decision problem, whereas the degree of fulfillment can be represented by an objective function f. For examples see Hester and Mahadevan (2010); Bandlow et al. (2017).

In this context, solutions can be compared by their Pareto-order to find a set of Pareto-optimal solutions. A solution is Pareto-optimal if no improvement of an objective function is possible without worsening another objective function, i.e. it is not Pareto-dominated by another solution (Censor, 1977). Solution x_1 Pareto-dominates solution x_2 over all l objectives if:

$$\forall i \in \{1, \ldots, l\}: \quad f_i(x_1) \leq f_i(x_2) \tag{1}$$

$$\exists j \in \{1, \ldots, l\}: \quad f_j(x_1) < f_j(x_2) \tag{2}$$

2.3. *Assessment of security measures*

The performance of security measure is essential for the fulfillment of protection objectives. In the context of risk, McGill et al. (2007) describe the performance by the reduction of threat likelihood via deterrence, as well as reduction of vulnerability via prevention.

2.3.1. *Assessment of deterrence*

Security research has worked on quantifying the deterrent effect of critical infrastructures (Taquechel and Lewis, 2012). For instance, McGill et al. (2007) propose to assess deterrence based on the expected utility of the attack profile from the adversary perspective. This model includes four key factors that influence the adversary's decision:

- *Perceived probability of success:* the adversary's assessment of the likelihood that an attack will succeed.
- *Gain from success:* the potential benefit to the adversary if the attack is successful.
- *Loss from failure:* the potential negative consequences to the adversary if the attack fails.
- *Cost of the attack:* the resources and effort the adversary must invest to carry out the attack.

2.3.2. *Assessment of vulnerability*

The assessment of vulnerability is commonly based on the approach compiled by Garcia (2008) (McGill et al., 2007; Čakija et al., 2020). The Adversary Sequence Diagram (ASD) is one such a model of this approach where potential intrusion paths are described by a graph of barriers (Sandia National Laboratories, 1989). The supplementary EASI model describes the effectiveness of security measures along the barriers of an intrusion path by a probability of detection P_D and a time game of

delaying the intruder long enough to intervene in time with a given delay time t_{D} and response time t_{R} (Bennett, 1977).

Uncertainties regarding t_{D} and t_{R} are considered by describing these parameters as random variables with probability distributions, for instance normal distributions.

According to the EASI model, the probability of adversary sequence interruption for a path with n barriers is:

$$P_{\mathrm{I}} = P_{\mathrm{D},1}\, P(t_{\mathrm{R}} < t_{\mathrm{RD},1}) + \sum_{i=2}^{n} P_{\mathrm{D},i}\, P(t_{\mathrm{R}} < t_{\mathrm{RD},i}) \prod_{j=1}^{i-1} (1 - P_{\mathrm{D},j}) \quad (3)$$

where t_{RD} is the residual delay time, given by the sum of delay times of all remaining barriers along the path. The residual delay time at the i-th of n barriers is:

$$t_{\mathrm{RD},i} = \sum_{j=i}^{n} t_{\mathrm{D},j} \quad (4)$$

2.3.3. *Assessment of costs*

Cost models describe subcategories of costs associated with the implementation of security measures. Examples of such models can be found in the work of Villa et al. (2017), Chen et al. (2020) and Reniers and Sörensen (2013). These models allow for a detailed breakdown of the costs involved in protection means for physical security systems. In principle, these models sum up costs in cost categories (CC) and cost subcategories (CSC):

$$\mathrm{Cost} = \sum_{i} CC_i, \qquad CC_i = \sum_{j} CSC_j \quad (5)$$

Typical cost categories include initial costs, installation costs, operating costs, as well as maintenance, inspection and sustainability costs (see Villa et al., 2017).

3. Approach and Notional Case Study

In the following, we propose an approach to find Pareto-optimal security system configurations balancing multiple protection objectives considering costs. The approach incorporates the aforementioned methods of morphological scenario analysis and assessment of security measures.

Alongside the description of our approach, we demonstrate its application to a notional case study. In this example, we consider only ground based attacks for the sake of simplicity. Fig. 1 shows the structure of the system in the form of an ASD, which includes the considered barriers. The initial two columns in Table 5 and Table 6 provide an overview of alternative security measure options that are under review at each barrier.

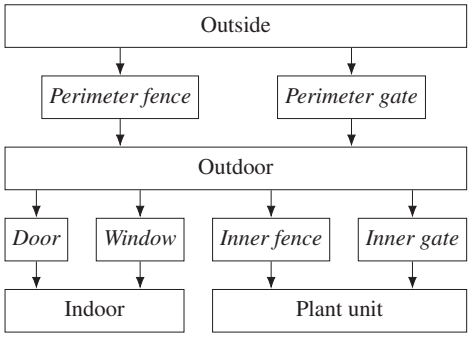

Fig. 1. Adversary Sequence Diagram of generic site.

3.1. *Development of a scenario space*

We explore and identify potential scenarios via a morphological scenario analysis. There, we include factors that are relevant for the subsequent analysis: On the one hand, the analysis needs to include factors that enable the specification of protection objectives, e.g. the *act* to be addressed. On the other hand the analysis needs to include factors that enable the analysis of the effectiveness of security measures, e.g. the attack *means* relevant for vulnerability or the type of *offender* relevant for deterrence.

For the notional case study, we assume the scenario characteristics and their pairwise consistency given by the cross consistency matrix in Table 1. A special feature of our cross consistency matrix is the pairwise assessment of different means. By doing so, we can derive sets of means that can be used by an offender in one scenario.

The result of the morphological scenario analysis is a list of consistent scenarios as shown in Table 2. The scenarios link the characteristics, which influence the optimization.

Table 1. Cross consistency matrix of scenario characteristics.

Category	Characteristic	Offender			Act			Target			Means			
		Activist	Burglar	Terrorist	Trespass	Theft	Sabotage	Outdoor	Indoor	Plant unit	Lightw. tools	Heavyw. tools	Light vehicle	Heavy vehicle
Offender	Activist	–	–	–	–	–	–	–	–	–	–	–	–	–
	Burglar	–	–	–	–	–	–	–	–	–	–	–	–	–
	Terrorist	–	–	–	–	–	–	–	–	–	–	–	–	–
Act	Trespass	0	1	1	–	–	–	–	–	–	–	–	–	–
	Theft	1	0	1	–	–	–	–	–	–	–	–	–	–
	Sabotage	1	1	0	–	–	–	–	–	–	–	–	–	–
Target	Outdoor	0	0	0	0	0	1	–	–	–	–	–	–	–
	Indoor	1	0	0	0	0	0	–	–	–	–	–	–	–
	Plant unit	0	0	0	0	0	0	–	–	–	–	–	–	–
Means	Lightweight tools	0	1	1	0	0	0	0	0	0	–	–	–	–
	Heavyweight tools	1	0	0	0	0	0	0	0	0	1	–	–	–
	Light vehicle	1	0	1	0	0	0	0	0	0	0	0	–	–
	Heavy vehicle	1	0	0	0	0	0	0	0	0	1	0	1	–

Legend: 0: consistent pair, 1: inconsistent pair.

Table 2. Scenario space of consistent scenarios with most extensive sets of means.

	Offender	Act	Target	Set of means
1	Activist	Tresp.	Outdoor	L. tools
2	Activist	Tresp.	Plant unit	L. tools
3	Burglar	Theft	Outdoor	H. veh. & H. tools
4	Burglar	Theft	Indoor	H. veh. & H. tools
5	Burglar	Theft	Plant unit	H. veh. & H. tools
6	Burglar	Theft	Outdoor	L. veh. & H. tools
7	Burglar	Theft	Indoor	L. veh. & H. tools
8	Burglar	Theft	Plant unit	L. veh. & H. tools
9	Terrorist	Sabot.	Indoor	H. veh. & H. tools
10	Terrorist	Sabot.	Plant unit	H. veh. & H. tools

Legend: H: Heavy/Heavyweight, L: Light/Lightweight.

3.2. *Specification of protection objectives*

We propose three protection objectives that security measures aim for:

- *Deter:* reduce the likelihood of attacks.
- *Monitor:* detect an intrusion.
- *Prevent:* detect and interrupt an intrusion.

We define lower bounds for the fulfillment of the protection objectives. This ensures a minimum level of protection in the optimization process while it allows to define the desired level of protection as a basis.

We relate the protection objectives to scenario factors established in the morphological scenario analysis. For the case study, we define protection objectives based on the *target* and the *act*, as we assume this determines the severity of the consequences essentially. Table 3 shows the protection objectives. Note that we define no lower bound for deterrence for demonstration purpose. Additionally, we set a low probability to prevent an act outside, as prevention may be difficult due to short attack paths.

3.3. *Quantification of protection objective fulfillment*

To quantify the extent to which the objectives are fulfilled, we apply the models described in the following sections.

Table 3. Protection objectives and used objective functions with minimum requirements.

Act	Target	Objective		
		Deter	Monitor	Prevent
Trespass	Outdoor	D	$P_{\mathrm{D}} \geq 0.5$	$P_{\mathrm{I}} \geq 0.1$
Trespass	Plant unit	D	$P_{\mathrm{D}} \geq 0.5$	$P_{\mathrm{I}} \geq 0.5$
Theft	Outdoor	D	$P_{\mathrm{D}} \geq 0.5$	—
Theft	Indoor	D	$P_{\mathrm{D}} \geq 0.5$	$P_{\mathrm{I}} \geq 0.5$
Theft	Plant unit	D	$P_{\mathrm{D}} \geq 0.5$	$P_{\mathrm{I}} \geq 0.5$
Sabotage	Indoor	D	$P_{\mathrm{D}} \geq 0.5$	—
Sabotage	Plant unit	D	$P_{\mathrm{D}} \geq 0.5$	$P_{\mathrm{I}} \geq 0.5$

3.3.1. *Deter Model*

We base our model of deterrence on the perception of the adversary to its expected utility, although we use a qualitative model as we assume to have few information about the deterring effect of the security measures. We rely on the visibility of deterrence measures as a measurement indicator in combination to the impact of the expected utility and relate it to the intention of the respective offender as seen in the scenario analysis. Table 4 is used to categorize the strength of deterrence D.

Table 4. Strength of deterrence.

D	Label	Description
–	No deterrence	Measures are not perceived or do not impact the expected utility.
+	Weak deterrence	Measures are perceived, but only slightly reduce the expected utility.
++	Strong deterrence	Measures are perceived and reduce the expected utility extensively.

We define the deterrence effect of the security system by the maximal deterrence effect of a single measure from all m taken measures:

$$D = \max(D_1, \ldots, D_m) \tag{6}$$

3.3.2. *Monitor model*

We assume the probability of detection along paths to be an indicator for the objective of monitoring. By removing intervention considerations from the EASI model, we obtained the probability of detection along a path with n barriers:

$$P_{\mathrm{D}} = 1 - \prod_{i=1}^{n} (1 - P_{\mathrm{D},i}) \tag{7}$$

3.3.3. *Prevent model*

We use the EASI model in conjunction with an ASD as a model of prevention and determine the probability of interruption along the weakest path.

In the case study, we assume a normally distributed response time with mean $\mu = 600\,\mathrm{s}$ and standard deviation $\sigma = 60\,\mathrm{s}$. Values of normally distributed delay time t_{D} and detection probability P_{D} are shown in Table 5 and Table 6, respectively.

3.3.4. *Cost model*

We define a simplified cost model in which we define a cost value for each measure C_{Measure} individually. Then, the system cost is the sum over all m implemented measures:

$$\mathrm{Cost} = \sum_{i=1}^{m} C_{\mathrm{Measure},i} \tag{8}$$

We consider the costs of the individual measures over a period of time. For simplicity, a single cost value is assumed for each measure, but in principle it can be derived from the cost categories and cost subcategories introduced in section 2.3.3. The used cost values are shown in Table 5 and Table 6.

3.4. *Optimization*

We use the aforementioned deter, monitor, prevent and cost models as objective functions that quantify the objectives like formulated in Table 3. The optimization problem is defined as follows:

$$\begin{aligned} \min_{x_i} (& -D_1, ..., -D_k, \; -P_{\mathrm{D},1}, ..., -P_{\mathrm{D},k}, \\ & -P_{\mathrm{I},1}, ..., -P_{\mathrm{I},k}, \; \mathrm{Cost}) \end{aligned} \tag{9}$$

Here, k is the number of the corresponding objective functions and x_i is a security system configuration formed by the alternative barrier and sensor options in Table 5 and Table 6. A configuration is a set of m taken options:

$$x_i = (M_1, ..., M_m) \tag{10}$$

where M_j is the measure option taken from the j-th alternative.

Table 5. Barrier alternatives and model parameters.

Alternative	Option	Costs (€)	D			t_D							
			Activist	Burglar	Terrorist	Light-weight tools		Heavy-weight tools		Light vehicle		Heavy vehicle	
						μ (s)	σ (s)	μ (s)	σ (s)	μ (s)	σ (s)	μ (s)	σ (s)
Perimeter fence	Fence SR2	29250	+	–	–	180	54	120	36	0	0	0	0
Inner fence	Fence SR2	5850	+	–	–	180	54	120	36	0	0	0	0
Perimeter fence	Fence SR3	49000	++	++	+	900	270	300	90	*inf*	0	*inf*	0
Inner fence	Fence SR3	9800	++	++	+	900	270	300	90	*inf*	0	*inf*	0
Perimeter fence	Fence SR4	94000	++	++	+	720	216	420	126	*inf*	0	*inf*	0
Inner fence	Fence SR4	18800	++	++	+	720	216	420	126	*inf*	0	*inf*	0
Perimeter gate	Gate SR2	10500	++	+	–	180	54	120	36	20	6	10	3
Inner gate	Gate SR2	10500	++	+	–	180	54	120	36	20	6	10	3
Perimeter gate	Gate SR3	13750	++	+	–	540	162	300	90	120	36	60	18
Inner gate	Gate SR3	13750	++	+	–	540	162	300	90	120	36	60	18
Perimeter gate	Gate SR4	20000	++	+	+	600	180	480	144	*inf*	0	*inf*	0
Inner gate	Gate SR4	20000	++	+	+	600	180	480	144	*inf*	0	*inf*	0
Door	Door RC 2	2450	+	–	–	300	90	160	48	*inf*	0	*inf*	0
Door	Door RC 3	3700	++	–	–	900	270	400	120	*inf*	0	*inf*	0
Door	Door RC 4	5000	++	+	–	1200	360	600	180	*inf*	0	*inf*	0
Window	Window RC 2	2150	+	–	–	300	90	180	54	*inf*	0	*inf*	0
Window	Window RC 3	2650	++	–	–	600	180	400	120	*inf*	0	*inf*	0
Window	Window RC 4	5100	++	+	–	1200	360	600	180	*inf*	0	*inf*	0

Legend: *inf* means an unlimited delay within the scope of the analysis.

Table 6. Sensor alternatives and model parameters.

Alternative	Option	Costs (€)	D			P_D			
			Activist	Burglar	Terrorist	Lightw. tools	Heavyw. tools	Light vehicle	Heavy vehicle
Perimeter sensors	Electric Fence, Microwave Detector (EF&MD)	20000	+	++	+	0.80	0.80	0.80	0.80
Inner sensors	Electric Fence, Microwave Detector (EF&MD)	10000	–	++	–	0.80	0.80	0.80	0.80
Perimeter sensors	Taut Wire Fence, Video Analytics (TWF&VA)	60000	+	++	+	0.90	0.90	0.90	0.90
Inner sensors	Taut Wire Fence, Video Analytics (TWF&VA)	20000	–	++	–	0.90	0.90	0.90	0.90
Perimeter sensors	Fence-Mounted Point Detector, Ground Based Radar (FM&GBR)	28000	+	++	–	0.95	0.95	0.95	0.95
Inner sensors	Fence-Mounted Point Detector, Ground Based Radar (FM&GBR)	14000	–	++	–	0.95	0.95	0.95	0.95
Building sensors	Fibre Optic Cable (FOC)	7750	–	–	–	1.00	1.00	1.00	1.00
Building sensors	Break-Glass Sensors, Balanced Magnetic Switch (BGS&BMS)	600	–	+	–	0.80	0.80	0.80	0.80
Building sensors	Active Infrared Beams (AIB)	1000	–	+	–	0.95	0.95	0.95	0.95

Additionally, we use the minimum requirements formulated in Table 3 as constraints of the optimization.

To find also nearly Pareto-optimal configurations, we relax the strict definition of Pareto-dominance in Eq. (1) and Eq. (2). For this we introduce a tolerance T for each objective function. Configuration x_1 dominates configuration x_2 if:

$$\forall i \in \{1,\dots,l\}: \quad f_i(x_1) + T_i \leq f_i(x_2) \quad (11)$$

$$\exists j \in \{1,\dots,l\}: \quad f_j(x_1) - T_j < f_j(x_2) \quad (12)$$

For the notional example, we use:

$$T_{\text{Cost}} = 1000 \quad (13)$$

$$T_{P_\text{I}} = T_{P_\text{D}} = 0.01 \quad (14)$$

4. Results

Table 7 shows the resulting Pareto-optimal configuration for the notional case study, sorted by increasing cost. The optimization yields 16 optimal configuration out of a total of $3^9 = 19\,683$ possible configurations. The optimal measures variate, but all optimal configurations include strong barriers (SR3/SR4 and RC3/RC4). It can therefore be said that the specified protection objectives and minimum requirements necessitate a long delay time. For instance, a long delay at the perimeter is required to prevent trespassing outdoor. This is underlined by Fig. 2, that shows the objective functions of configurations 2 and 4 selected for illustration purpose. Here, a relative low P_I can be identified for that protection objective of preventing trespassing outdoor. This is in line with the EASI model, as only one barrier has to be overcome.

Furthermore, Fig. 2 shows an increased overall effectiveness for configuration 4 at higher cost compared to configuration 2, except for preventing theft indoor, where P_I is lower. This reveals that there is a trade-off between protection objectives.

It is evident from Fig. 2, that the optimal configurations are influenced solely by prevention and monitoring, with no variation of deterrence. In our case study, this applies to all configurations. This may be due to the fact that we only consider measures that are effective for both prevention and deterrence.

Table 7. Resulting optimal configurations.

	Barrier						Sensor		
Configuration	Perim. fence SR	Inner fence SR	Perim. gate SR	Inner gate SR	Door RC	Window RC	Perimeter	Inner	Building
1	3	4	4	4	3	3	EF&MD	EF&MD	AIB
2	3	4	4	4	4	4	EF&MD	EF&MD	AIB
3	3	4	4	4	3	3	EF&MD	FM&GBR	AIB
4	3	4	4	4	3	3	FM&GBR	EF&MD	BGS&BMS
5	3	4	4	4	4	4	EF&MD	FM&GBR	AIB
6	3	4	4	4	3	3	FM&GBR	EF&MD	AIB
7	3	4	4	4	4	4	FM&GBR	EF&MD	BGS&BMS
8	3	4	4	4	4	4	FM&GBR	EF&MD	AIB
9	4	3	4	4	4	4	FM&GBR	EF&MD	BGS&BMS
10	4	3	4	4	4	4	FM&GBR	EF&MD	AIB
11	4	4	4	4	3	3	EF&MD	FM&GBR	AIB
12	4	4	4	4	3	3	FM&GBR	EF&MD	BGS&BMS
13	4	4	4	4	4	4	EF&MD	FM&GBR	AIB
14	4	4	4	4	3	3	FM&GBR	EF&MD	AIB
15	4	4	4	4	4	4	FM&GBR	EF&MD	BGS&BMS
16	4	4	4	4	4	4	FM&GBR	EF&MD	AIB

Note: See Table 5 and Table 6 for full names of measure options.

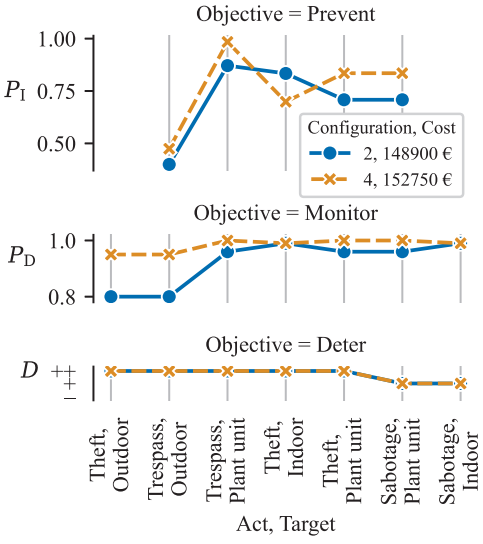

Fig. 2. Objective functions of two selected optimal configurations in a parallel coordinates plot.

5. Conclusion

In this work, an approach is presented for analyzing the relationship between the costs of security measures (barriers and sensors) and the achievement of defined protection objectives (deter, monitor, prevent). The primary aim was to find an optimal balance between fulfilling these protection objectives and minimizing costs. To this end, we perform a morphological scenario analysis, thereby creating consistent scenarios based on scenario characteristics (offender, act, target, means). Subsequent to establishing the fundamental models (deterrence, prevention, monitoring, costs), a Pareto optimization was conducted, including the protection objectives as well as the aggregated costs.

By specifying multiple protection objectives and quantifying these protection objectives, we make the decision problem accessible to optimization without knowing the actual likelihood of scenarios. Nevertheless, we can balance protection objectives by the specification of minimum requirements.

This methodological approach effectively illuminates the trade-offs between security effectiveness and associated costs, thereby providing decision-makers with a framework for optimally allocating resources while ensuring the desired level of security. In the notional case study, a manageable set of solutions can be provided to the decision-maker, from which he can select an appropriate solution by evaluating the fulfillment of the protection objectives. Still, the number of solutions may increase with increasing system complexity.

The results demonstrate the potential of combining scenario-based analysis with multi-criteria optimization to support the development and evaluation of appropriate security systems.

References

Bandlow, A., K. A. Jones, N. J. K. Brown, and L. K. Nozick (2017). The impact of false and nuisance alarms on the design optimization of physical security systems. In I. L. Nunes (Ed.), *Advances in Human Factors and System Interactions*, Volume 497 of *Advances in Intelligent Systems and Computing*, Cham, pp. 189–201. Springer.

Baybutt, P. (2017, September). Issues for security risk assessment in the process industries. *Journal of Loss Prevention in the Process Industries 49*, 509–518.

Bennett, H. A. (1977). Easi (estimate of adversary sequence interruption) - an evaluation method for physical security systems. *Nuclear Materials Management 6*, 371–379.

Censor, Y. (1977). Pareto optimality in multiobjective problems. *Applied Mathematics and Optimization 4*(1), 41–59.

CER Directive (2022, December). Directive on the resilience of critical entities and repealing council directive 2008/114/ec. Directive (EU) 2022/2557, European Parliament and Council of the European Union.

Chen, C., G. Reniers, and N. Khakzad (2020). Cost-benefit management of intentional domino effects in chemical industrial areas. *Process Safety and Environmental Protection 134*, 392–405.

Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems* (2 ed.). Butterworth-Heinemann.

Hester, P. and S. Mahadevan (2010). A multicriteria approach to critical facility security system design. In K. D. Lawrence and G. Kleinman (Eds.), *Applications in Multicriteria Decision Making, Data Envelopment Analysis, and Finance*, Volume 14 of *Applications of Management Science*, pp. 105–131. Leeds: Emerald Group Publishing Limited.

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

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

Reniers, G. L. L. and K. Sörensen (2013). An approach for optimal allocation of safety resources: Using the knapsack problem to take aggregated cost-efficient preventive measures. *Risk Analysis 33*(11), 2056–2067.

Ritchey, T. (2006, July). Problem structuring using computer-aided morphological analysis. *Journal of the Operational Research Society 57*(7), 792–801.

Sandia National Laboratories (1989, December). Savi: Systematic analysis of vulnerability to intrusion. volume 1 of 2. Sandia Report SAND89-0926/1.

Taquechel, E. and T. Lewis (2012, August). How to quantify deterrence and reduce critical infrastructure risk. *Homeland Security Affairs 8*. Article 12.

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

Villa, V., G. L. L. Reniers, N. Paltrinieri, and V. Cozzani (2017, September). Development of an economic model for counter terrorism measures in the process-industry. *Journal of Loss Prevention in the Process Industries 49*, 437–460.