Advances in Reliability, Safety and Security, Part 7 – Kołowrocki, Magryta-Mut (eds.)
 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

Vulnerability Adjusted Metrics in Performance Based Physical Security Assessments

Thomas Termin[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, Germany*

Abstract

Critical infrastructure (CRITIS) protection requires the skillful integration of security measures to maintain integrity and functionality in the event of a potential attack. This involves the identification, categorization and assessment of elements requiring protection, followed by the astute allocation of security measures, all within the constraints of limited resources. The challenge is to make simple decisions about security-related investments. One solution is the use of risk-adjusted scorings. While risk-adjusted scoring scales are well established in functional safety (e.g. Braband, 2008), their application to physical vulnerability assessment remains a mostly unexplored area. This paper presents a versatile approach to performance-based physical vulnerability analysis using risk-adjusted scorings. Based on Harnser's (2010) framework, the presented method defines different barrier types and resistance classes. Each type is associated with a scale mapping probability intervals to vulnerability scores. By aligning with Termin et al.'s (2023) metric compatibility approach, these scores are locally adjusted to replicate quantitative vulnerability values derived from the application of Lichte et al.'s (2016) quantitative vulnerability metric. To illustrate the potential of the approach, a vulnerability analysis based on the risk-adjusted scoring framework is demonstrated. This approach can support CRITIS operators in making informed security investment decisions when using the presented toolkit. Finally, challenges and opportunities are discussed and the findings summarized.

Keywords: metrical analysis, physical security, vulnerability analysis, decision-making, generic approach

1. Introduction

In an increasingly interconnected and vulnerable world, the protection of critical infrastructures (CRITIS) has emerged as a paramount concern (Hurst et al., 2014). Ensuring their uninterrupted operation and resilience against deliberate threats has become a cross-industry and cross-national imperative (Farrell et al., 2004). As the security risk landscape continues to evolve, so does the need for sophisticated and adaptable methodologies to assess and improve physical security measures (Krisper, 2021). In the field of physical security, probabilistic approaches have become established over time, which can assist users in conducting cost-benefit analyses. However, the quantification often involves rather complex calculations, raising the question of whether simpler ways in the form of simple scoring systems could provide comparable results.

The paper by Termin et al. (2023) illustrates how the adjustment of the results of a vulnerability scoring to the results of a quantitative vulnerability metric can be conducted. The present contribution builds upon these considerations and explores the applicability of risk-adjusted vulnerability metrics through concrete examples. In the context of the three-part risk formula of threat probability, vulnerability and impact, this paper focuses on the assessment of physical vulnerability, assuming that an attack occurs ($p = 1$). The assumption of disjointedness and strict independence between threats, vulnerabilities and impacts allows individual risk contributions to be analyzed and assessed separately. This facilitates risk assessment, as uncertain variables, especially those that are highly epistemic, can be excluded (Lichte et al., 2016). At the end of this paper, challenges in the application of adjusted scoring metrics are identified, using the example of cost-benefit analysis.

2. Background

In today's world, where the functioning of societies and economies relies heavily on interconnected critical infrastructures (CRITIS) and systems, ensuring their security and resilience has become a vital concern (Aradau, 2010). These infrastructures span various sectors such as energy, transport, communications and healthcare, each of which plays an essential role in maintaining the stability of our daily lives (De Felice et al., 2022). The prevailing threat landscape has evolved significantly in recent years, marked by a significant increase in deliberate attacks on CRITIS. Malicious actors, ranging from cybercriminals to state-sponsored entities, are constantly exploiting vulnerabilities to disrupt services, compromise data and potentially endanger lives. As a result, there is an urgent need for robust security measures (Kovacevic & Nikolic, 2015).

Historically, security assessments for CRITIS have often been static and compliance-based, addressing specific known threats without the flexibility to adapt to emerging risks. Recognizing the limitations of traditional approaches, the concept of performance-based security assessment has emerged, particularly in the physical security domain. In the energy sector in particular, performance-based security assessments are based on scorings, e.g. according to Harnser (2010). The Harnser metric includes three variables to assess vulnerability: Protection, Observation (or Detection respectively) and Intervention. Each variable has five descriptive levels from one to five, with five being the strongest and one being the weakest. For example, level five is defined as "There is no ability to prevent this scenario from occurring and causing the worst consequences" (Harnser, 2010, p. 109). In this vulnerability metric, protection, observation and intervention are scored and summed based on expert judgement. The sum of these three variables serves as a measure of vulnerability, with the highest sum (“15”) indicating low vulnerability/high performance and the lowest sum (“3”) indicating high vulnerability/low performance. However, the Harnser metric poses challenges in its application (see also: Termin et al, 2021):

a) Harnser does not differentiate between individual barriers; b) the three assessment variables are considered equivalent, which does not reflect real-world situations (protection can theoretically be effective on its own, while observation and intervention cannot); c) he descriptive nature of the levels from one to five complicates the classification of security measures and the repeatability of assessments (different experts may provide very different assessments); d) sharp vulnerability criterion cannot be represented, as is possible with the quantitative Intervention Capability Metric (ICM) according to Lichte et al. (2016).

In the ICM, the temporal interplay between protection, observation and intervention is used as a measure of physical vulnerability. For the three assessment variables, not only discrete time values but also probabilistic density functions can be chosen to account for uncertainties. In Termin et al. (2023), a five-step approach is developed to reconcile the results of the Harnser scoring with the results based on the ICM. These five steps are:

1) Define time steps (probabilistic density functions) in the quantitative ICM for each Harnser score. A set of defined score density function pairs corresponds to an ICM variant.
2) Extend the Harnser vulnerability scale ("3" to "15") with assumed probability intervals.
3) Compute all score combinations from 1 x 1 x 1 to 5 x 5 x 5 once using the Harnser metric and once using the ICM.
4) Compare the results of the two metrics.
5) Adjust the probabilities behind the Harnser vulnerability scale scores to match the quantitative results.

This paper analyzes the applicability of the approach proposed in Termin et al. (2023) using fictional scenarios and infrastructures (asset-barrier constellations) as examples.

3. Approach

The methodology presented in this contribution is designed to bridge the gap between semi-quantitative assessments and quantitative assessments, providing a pragmatic framework to conduct a scoring-based assessment of physical vulnerability with the aim of achieving results comparable to those of a quantitative assessment regarding accuracy. The foundation of the approach presented is the risk-adjusted scoring scheme developed by Termin et al. (2023) combined with the vulnerability analysis approach suggested by Lichte et al. (2016). A risk-adjusted scoring scheme is derived for different barrier types, i.e. the adjustment takes place locally for each barrier. It is assumed that every barrier of an infrastructure can have different expansion stages, e.g. weak barrier, medium barrier and very strong barrier - or simply put, there can be a door made of wood, sheet metal or thick steel. It is also assumed that the protection, observation and intervention characteristics improve with each level of expansion. Put simply, a thick steel door will deter an attacker for longer than a wooden door. The third assumption is that every barrier and every expansion stage has all three properties mentioned, i.e. always protection, observation and intervention. The fourth assumption is a simplifying assumption; it states that each barrier has five expansion stages in total (corresponding to the Harnser scores “1”, “2”, “3”, “4” and “5”). The

fourth assumption leads to the conclusion that there are five possible protection, observation and intervention measures for each barrier. The fifth assumption is that each security measure is associated with a corresponding time, represented by a probabilistic density function. The last assumption is that the scorings are adjusted locally for each specific barrier under consideration, i.e. the residual protection along a path (multiple barriers in a row), as it is considered in the ICM for attack path assessments, is not given here because each barrier with its properties of protection, observation and intervention are considered “in isolation”.

In summary, this results in a scoring matrix for each barrier type, in which the Harnser scores from "1" to "5" are assigned to protection, observation and intervention times. The approach in Termin et al. (2023) is now applied to these scoring matrices. The result is vulnerability scales for each barrier type. Behind each vulnerability score of each vulnerability scale is therefore a probability or probability interval for physical vulnerability. In a first step, it is assumed that the same score number for each security measure corresponds to a resistance class, i.e. protection = "1", observation = "1" and intervention = "1" is, for example, resistance class A, etc. If there were a catalogue with predefined resistance classes or predefined risk-adjusted scorings for different barrier types in industrial practice, vulnerability could be quickly determined using the corresponding scoring scheme. In a second step, it is assumed that a CRITIS operator has a catalogue of security measures with corresponding times for protection, observation and intervention. The question here is how risk-adjusted scoring evaluation systems for the individual barriers of an infrastructure can be built from the existing "construction kit" of measures in order to evaluate physical vulnerability on a scoring basis. In a third step, challenges are discussed using the example of carrying out cost-benefit analyses using scorings.

The approach is aimed to build a basis for practical implementation in the operational context of scoring-based vulnerability assessments of CRITIS. It allows for adaptability in the selection of vulnerability scales based on infrastructure attributes and barriers in place. The following chapters explore the application and implications of this approach, highlighting its potential to simplify physical security assessments for critical infrastructures.

3.1. Reference Model Setup

In this paper, three barrier types are defined exemplarily, Barrier I, Barrier II and Barrier III. Each of the three barriers has five levels, hereinafter referred to as Resistance Class (RC) A, B, C, D, and E. Each RC corresponds to a score for protection (P), a score for observation (O) and a score for intervention (I) (see Table 1).

Table 1. Mapping of Resistance Classes to Harnser Scores.

RC	P	O	I
A	1	1	1
B	2	2	2
C	3	3	3
D	4	4	4
E	5	5	5

In the example in Table 1, the RC are assigned 1:1 to the scores for protection, observation and intervention. However, depending on the RC, P, O and I may have different "strengths" (see Table 2 as an example). What is fundamentally important here is the specific time behind the scores.

Table 2. Mapping of Resistance Classes to Harnser Scores (Variant 2).

RC	P	O	I
A	1	3	2
B	1	3	3
C	2	3	3
D	3	4	4
E	5	5	4

In a next step, expert knowledge is used to determine a protection time, an observation time and an intervention time for each RC of each barrier. The collection of expert knowledge is not shown further in this paper. It is assumed that for each score, a timely mean and a standard deviation can be estimated by experts. In the case of our paper, P, O and I are normally distributed variables. The following correlations are assumed for the aforementioned barriers (see Table 3 to Table 5):

Table 3. Barrier Type I Configuration: Mapping of Scores to Specific Time Values (in sec.).

RC	P	P time	O	O Time	I	I Time
A	1	μ = 15 σ = 30	1	μ = 135 σ = 30	1	μ = 135 σ = 30
B	2	μ = 45 σ = 30	2	μ = 105 σ = 30	2	μ = 105 σ = 30
C	3	μ = 75 σ = 30	3	μ = 75 σ = 30	3	μ = 75 σ = 30
D	4	μ = 105 σ = 30	4	μ = 45 σ = 30	4	μ = 45 σ = 30
E	5	μ = 135 σ = 30	5	μ = 15 σ = 30	5	μ = 15 σ = 30

Table 4. Barrier Type II Configuration: Mapping of Scores to Specific Time Values (in sec.).

RC	P	P time	O	O Time	I	I Time
A	1	μ = 15 σ = 30	1	μ = 135 σ = 30	1	μ = 135 σ = 60
B	2	μ = 45 σ = 30	2	μ = 105 σ = 30	2	μ = 105 σ = 60
C	3	μ = 75 σ = 30	3	μ = 75 σ = 30	3	μ = 75 σ = 60
D	4	μ = 105 σ = 30	4	μ = 45 σ = 30	4	μ = 45 σ = 60
E	5	μ = 135 σ = 30	5	μ = 15 σ = 30	5	μ = 15 σ = 60

Table 5. Barrier Type III Configuration: Mapping of Scores Classes to Specific Time Values (in sec.).

RC	P	P time	O	O Time	I	I Time
A	1	μ = 15 σ = 10	1	μ = 135 σ = 75	1	μ = 135 σ = 100
B	2	μ = 45 σ = 10	2	μ = 105 σ = 75	2	μ = 105 σ = 100
C	3	μ = 75 σ = 10	3	μ = 75 σ = 75	3	μ = 75 σ = 100
D	4	μ = 105 σ = 10	4	μ = 45 σ = 75	4	μ = 45 σ = 100
E	5	μ = 135 σ = 10	5	μ = 15 σ = 75	5	μ = 15 σ = 100

It should be noted here that the differences between each RC do not have to be linear in nature, i.e. there can also be correlations in which the mean and standard deviation of P, O and I are fundamentally different from RC to RC. In addition, the barriers do not always have to have five levels (see Barrier X configuration in Table 6).

Table 6. Barrier Type X Configuration: Mapping of Scores Classes to Specific Time Values (in sec.).

RC	P	P time	O	O Time	I	I Time
A	1	μ = 15 σ = 30	1	μ = 135 σ = 40	1	μ = 200 σ = 100
B	2	μ = 60 σ = 27	2	μ = 60 σ = 30	2	μ = 180 σ = 80
C	3	μ = 95 σ = 21	3	μ = 30 σ = 28	3	μ = 75 σ = 70

From the user's point of view, it must be asked whether there can also be barriers for which P, O and I can be unoccupied for certain RC, i.e. for RC A at a fictitious barrier Y, for example, there are properties of protection and properties of observation, but (as yet) no properties of intervention (see Table 7). Such a configuration is permissible in principle because there may not yet be any intervention features at RC A, but it must be borne in mind that in such a case the physical vulnerability is at a maximum because an attacker is never stopped in this particular case.

Table 7. Barrier Type Y Configuration: Mapping of Scores to Specific Time Values (in sec.).

RC	P	P time	O	O Time	I	I Time
A	1	μ = 15 σ = 100	1	μ = 135 σ = 100	1	/
B	2	μ = 45 σ = 100	2	μ = 105 σ = 100	2	μ = 105 σ = 100

C	3	μ = 75 σ = 100	3	μ = 75 σ = 100	3	μ = 75 σ = 100
D	4	μ = 105 σ = 10	4	μ = 35 σ = 100	4	μ = 45 σ = 100

The next step is to develop vulnerability scales for the outlined three barrier types that conform to the vulnerability results of a quantitative assessment metric. For the scoring-based assessment, the Harnser metric is used (Harnser, 2010). The scores of protection, observation and intervention are added together. This results in a score range from "3" to "15", where a high vulnerability score means low vulnerability. In order to be able to compare the Harnser results with the results of a quantitative metric, the vulnerability scores are expanded by presumed probability intervals, see Table 8 as an example.

Table 8. Harnser Scale (Source: Termin et al., 2023).

Vulnerability Score	3	4	…	13	14	15
Lower Value	0.924	0.847	…	0.154	0.77	0
Upper Value	1	0.924	…	0.231	0.154	0.77
Mean Value	0.962	0.8855	…	0.1925	0.462	0.385

For the "time-based" assessment, the quantitative vulnerability metric according to Lichte et al. (2016) is used, in this paper named intervention capability metric (ICM). Each P, O and I score therefore corresponds to a time in the ICM. To make the results of both vulnerability assessments compatible, the compatibility approach according to Termin et al. (2023) is applied. For Tables 3 to 5, this results in the following vulnerability-adjusted rating scales (see Table 9 to Table 11):

Table 9. Vulnerability Scale Barrier Type I.

Vulnerability Score	3	4	4	…	14	15
Lower Value	1	1	1	…	0.077	0.024
Upper Value	1	1	1	…	0.09	0.024
Mean Value	1	1	1	…	0.084	0.024

Table 10. Vulnerability Scale Barrier Type II.

Vulnerability Score	3	4	5	…	14	15
Lower Value	0.99	0.99	0.99	…	0.156	0.079
Upper Value	0.99	0.99	0.99	…	0.168	0.079
Mean Value	0.99	0.99	0.99	…	0.162	0.079

Table 11. Vulnerability Scale Barrier Type III.

Vulnerability Score	3	4	5	…	14	15
Lower Value	0.999	0.996	0.987	…	0.316	0.246
Upper Value	0.999	0.998	0.993	…	0.36	0.246
Mean Value	0.999	0.997	0.99	…	0.338	0.246

In a fictitious reference model, our infrastructure consists of one asset to be protected and twelve barriers. Each of the twelve barriers can be assigned to one of the previously defined three barrier types. Within the scope of an attack path analysis, the following paths to reach the asset could be outlined (see Figure 1):

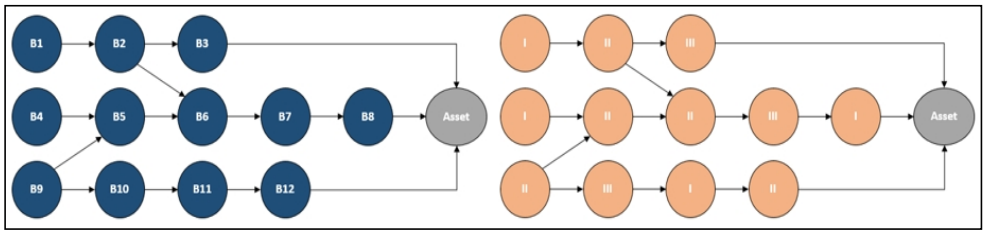

Fig. 1. Attack Paths of a Fictitious CRITIS (Left: Barrier Designation B1 – B12; Right: Barrier Type Categorization I - III).

3.2 Performance-based Assessment Using Local, Risk-Adjusted Scorings

In total, the following five attack paths can be realized:

1) B1-B2-B3-Asset
2) B4-B5-B6-B7-B8-Asset
3) B9-B10-B11-B12-Asset
4) B1-B2-B6-B7-B8-Asset
5) B9-B5-B6-B7-B8-Asst

In a next step, experts are asked, for example, to specify the RC for each barrier. The following is an example on the first path "B1-B2-B3-Asset": Barrier 1 is to be assigned to barrier type I, or B1.I for short. Barrier 2 is to be assigned to barrier type II (B2.II) and barrier 3 to barrier type III (B3.III). The following classification was determined within the framework of an expert survey: The first barrier has the properties of RC A, the second barrier the inherent shadows of RC D and the third barrier the property RC E. This attack path can consequently be written as the following code: B1.I.RCA - B2.II.RCD - B3.III.RCE – Asset. As there are scores for protection, observation and intervention behind each RC, these can be added up according to the Harnser metric and sorted into the respective vulnerability scale of the barrier type in question, i.e. e.g. for "B1.I.RCA", P = 1, O = 1 and I = 1 results in a vulnerability score V = 3. According to Table 9, this corresponds in this example to a presumed probability of vulnerability of 100 % (Lower, Upper and Mean). Based on this principle, the probability values for physical vulnerability can be determined for the other barriers along the path considered (see Table 12).

Table 12. Vulnerability Values Path I.

Vulnerability Score	B1.I.RCA	B2.II.RCD	B3.III.RCE
Lower Value	1	0.42	0.246
Upper Value	1	0.56	0.246
Mean Value	1	0.49	0.246

Using the vulnerability-adjusted Harnser scoring metric, a range of probability values for the physical vulnerability at a given barrier configuration can be determined. In contrast to the ICM, not all results determined in Table 12 have the same discrete value. From the user's point of view, there is a problem if not the individual vulnerability is determined, but the total vulnerability along the considered path. If the events at barrier 1 to n are disjoint from each other and strictly independent of each other (Lichte et al., 2016), then the individual vulnerabilities at the barriers can be multiplied with each other to obtain the total vulnerability.

The question when applying this scoring-based assessment method is which vulnerability values (Lower, Upper, Mean) should be multiplied together. One possible approach can be to distinguish between different views of risk affinity. For example, a general recommendation could be to take the pessimistic (worst case) perspective from a defender's point of view (Harnser, 2010). In this case, the determined upper values are multiplied by each other. Another possibility can, of course, be an optimistic stance. In such a case, the lower values are multiplied together along the path. A third variant would be "indifferent". In this case, the mean values would be used as the evaluation measure. It should be noted at this point that the choice of probability values for determining the overall volatility depends strongly on the use case. Thus, a plausible approach can also be to carry out two calculations, once only with the lower values and once only with the upper values, in order to reveal the spread in the total vulnerability "The total vulnerability goes from x to y". To demonstrate the principle described, all four variants shown are calculated using the example of attack path one (see Table 13 to Table 16).

The delta in vulnerability from Lower to Upper is quite small in this example, but it can be much larger in concrete use cases. Furthermore, working with the RC is not compulsory. Experts can also score P, O and I per barrier and classify the result in the vulnerability scale of the respective barrier type.

Table 13. Total Vulnerability Value Path I, Optimistic View (Lower Values).

B1.I.RCA	B2.II.RCD	B3.III.RCE	V total
1	0.42	0.246	0.1

Table 14. Total Vulnerability Value Path I, Pessimistic View (Upper Values).

B1.I.RCA	B2.II.RCD	B3.III.RCE	V total
1	0.56	0.246	0.14

Table 15. Total Vulnerability Value Path I, Indifferent View (Mean Values).

B1.I.RCA	B2.II.RCD	B3.III.RCE	V total
1	0.49	0.246	0.12

Table 16. Total Vulnerability Value Path I, Spread of Results (Lower and Upper).

B1.I.RCA	B2.II.RCD	B3.III.RCE	V total
1	0.56	0.246	0.14
1	0.42	0.246	0.1
Delta in Vulnerability			0.04

3.3 Practical Example of Using the Local, Risk-Adjusted Approach

The target under evaluation consists of two barriers (B1 and B2), one asset (A) and one attack path (B1-B2-A) (see Figure 2).

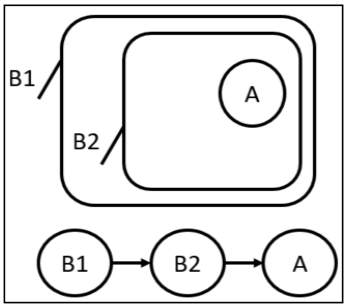

Fig. 2. System Architecture of a Fictitious CRITIS.

The provider of the CRITIS has a measure toolbox that describes the scope the defender capabilities in general. There exist three types of measures: protection measures (PM), observation measures (OM), intervention measures (IM). The toolbox consists of five possible measures that can be chosen and assigned to each barrier. There are 5 x 5 x 5 = 125 feasible configurations for each barrier in total. To each measure, a normal probability distribution is assumed (estimated by experts); there are no discrete time values (see Table 17).

Table 17. List of Measures.

Protection Measure (PM)	Protection Time in Sec.
PM 1	$\mu = 15; \sigma = 10$
PM 2	$\mu = 105; \sigma = 10$
PM 3	$\mu = 75; \sigma = 10$
PM 4	$\mu = 45; \sigma = 10$
PM 5	$\mu = 135; \sigma = 10$

Observation Measure (OM)	Observation Time in Sec.
OM 1	$\mu = 15; \sigma = 75$
OM 2	$\mu = 105; \sigma = 75$
OM 3	$\mu = 45; \sigma = 75$
OM 4	$\mu = 75; \sigma = 75$
OM 5	$\mu = 135; \sigma = 75$
Intervention Measure (IM)	Intervention Time in Sec.
IM 1	$\mu = 75; \sigma = 100$
IM 2	$\mu = 105; \sigma = 100$
IM 3	$\mu = 135; \sigma = 100$
IM 4	$\mu = 15; \sigma = 100$
IM 5	$\mu = 45; \sigma = 100$

The following rules apply for assessing physical vulnerability of the target under evaluation: 1. If not a full triplet of measures (PM, OM, IM) is assigned to a barrier, then the barrier vulnerability is equal to 1. 2. If a measure is already chosen e.g. for barrier 1, it can also be assigned to barrier 2. As a perquisite for the vulnerability assessment, the measures are sorted according to size of the assigned time, using the Harnser scoring as a frame: PM: upward rising time sorted; OM: upward falling time sorted and IM: upward falling time sorted. To the lowest PM, highest OM and highest IM, the lowest score (and resistance class, RC) is assigned, and so on (see Table 18). The score-time pair values correspond to Table 5. With this, we can use Table 11 as a risk-adjusted Harnser metric vulnerability scale in this context.

Table 18. Sorted List of Measures in the Harnser Scoring Scheme.

RC	P	P time	O	O Time	I	I Time
A	1	PM 1	1	OM 5	1	IM 3
B	2	PM 4	2	OM 2	2	IM 2
C	3	PM 3	3	OM 4	3	IM 1
D	4	PM 2	4	OM 3	4	IM 5
E	5	PM 5	5	OM 1	5	IM 4
RC	P	P time	O	O Time	I	I Time
A	1	$\mu = 15$ $\sigma = 10$	1	$\mu = 135$ $\sigma = 75$	1	$\mu = 135$ $\sigma = 100$
B	2	$\mu = 45$ $\sigma = 10$	2	$\mu = 105$ $\sigma = 75$	2	$\mu = 105$ $\sigma = 100$
C	3	$\mu = 75$ $\sigma = 10$	3	$\mu = 75$ $\sigma = 75$	3	$\mu = 75$ $\sigma = 100$
D	4	$\mu = 105$ $\sigma = 10$	4	$\mu = 45$ $\sigma = 75$	4	$\mu = 45$ $\sigma = 100$
E	5	$\mu = 135$ $\sigma = 10$	5	$\mu = 15$ $\sigma = 75$	5	$\mu = 15$ $\sigma = 100$

The fictitious configurations of measures assigned to the barriers are as follows: B1: PM 5, OM 1 and IM 4; B2: PM 2, OM 1 and IM 4. By using Table 18, the following Harnser scores can be assigned to B1 and B2:

- B1: P = 5; O = 5; I = 5
- B2: P = 4; O = 5; I = 5

In a next step, the scores are summed. For B1, the vulnerability results in a score of 15 and for B2, the vulnerability results in a score of 14. By looking at Table 11, we see that the quantitative vulnerability values (V) are as follows (see Table 19):

Table 19. Estimating Physical Vulnerability Using the Adjusted Harnser Scale.

Optimistic View (Lower Values)		
V B1	V B2	V total
0.246	0.0.316	0.078
Pessimistic View (Upper Values)		
V B1	V B2	V total
0.246	0.36	0.089
Indifferent View (Mean Values)		
V B1	V B2	V total
0.246	0.338	0.083
As a Reference: Calculation using the ICM		
V B1	V B2	V total
0.246	0.33	0.081

As can be seen in Table 19, when comparing the ICM vulnerability values with the results of the adjusted Harnser scoring, the indifferent view gives the closest result. With the approach presented before, we can build a Common Physical Vulnerability Scoring System (CPVSS) in analogy to the Common Vulnerability Scoring System from IT Security (First.org, 2023) (see Figure 3). The sum of the individual scores of PM, OM and IM can be sorted into the adjusted vulnerability scale of Table 11. The vulnerability sum score corresponds to a CPVSS score here.

"Protection Metric"		
Measure	Category	Num. Score
PM 1	Very Low	1
PM 2	High	4
PM 3	Medium	3
PM 4	Low	2
PM 5	Very High	5

"Observation Metric"		
Measure	Category	Num. Score
OM 1	Very High	5
OM 2	Low	2
OM 3	High	4
OM 4	Medium	3
OM 5	Very Low	1

"Intervention Metric"		
Measure	Category	Num. Score
IM 1	Medium	3
IM 2	Low	2
IM 3	Very Low	1
IM 4	Very High	5
IM 5	High	4

Fig. 3. CPVSS for the Specific Context in Fig. 2 and Table 17.

3.4 Discussion of Scorings and Cost-Benefit Analyses

For conducting a cost-benefit analysis, taking into account the formulated assumptions, it can be assumed that the asset has a specific monetary value, e.g. x monetary units. The provider of the fictitious CRITIS in this paper has a budget of y monetary units. The optimization objective is to equip the two barriers with measures that minimize the total vulnerability of the path. To find the configuration that leads to the lowest path vulnerability in general, the total vulnerability can be calculated for all possible combinations of measures that lie within the defined budget. The first step is to calculate the cost of all 5 x 5 x 5 x 5 x 5 x 5 theoretically possible configurations. The provider's defined budget then acts as a filter to select those configurations for further analysis that are practically feasible in this use case. The physical vulnerability can then be estimated for all feasible variants using the adapted Harnser vulnerability metric. This approach can be used to identify the minimum path vulnerability.

In general, it is a challenge to make a good cost-benefit decision despite the adjusted vulnerability scoring metrics. This is because the scores are inherently uncertain, i.e. there is always a range of probabilities behind the vulnerability scores. Depending on the scale structure used (e.g. three, four, five, ten or n categories), the interval width of the assumed probability intervals can vary greatly. The interval width behind the vulnerability ratings is usually greater for a few scale levels than for many scale levels. This poses a problem for cost-benefit analysis users, because the expected monetary loss values cover a range that depends on the interval width of the probability values behind the vulnerability scores.

Therefore, a sharp decision criterion does not exist here, but one criterion with an "error" with respect to the quantitative ICM vulnerability values that consists of a lower level and an upper level. In principle, a user could choose a view (optimistic, pessimistic, and indifferent) but it would be advisable to take the pessimistic view as a worst-case scenario, just to be on the secure side.

4. Summary

This research presents a pioneering approach in the field of performance-based physical security assessment, centered on the use of scoring metrics that are locally adjusted for different barrier types. A key advantage of risk-adjusted scoring in this case presented is its performance-based nature. By capturing the real-world probabilities for physical vulnerability for specific barriers, it provides a dynamic and adaptive framework. In particular, the scoring tables generated can serve as a comprehensive 'security catalogue', confirming with quantitatively calculated results using the ICM. This flexibility allows the selection of relevant vulnerability scales based on infrastructure attributes and deployed barriers, resulting in a versatile, adaptive and efficiency-oriented approach. A distinguishing feature of this approach is its ability to provide results comparable to those obtained from quantitative calculations (e.g. based on the ICM), thus underlining its reliability for local adjustments. In addition, it offers significant benefits to critical infrastructure operators. The use of a scoring system, a semi-quantitative metric, eliminates the use of complex mathematical formula. This not only streamlines decision-making, but also provides a pragmatic trade-off between accuracy and practicality.

In essence, risk-adjusted scoring is proving to be a transformative and inclusive methodology that skillfully bridges the gap between traditional security approaches and quantitative assessments. Its adaptability to specific use cases make it a useful tool for assessing the security posture of critical infrastructure with a simple scoring. While this paper lays a solid foundation for the integration of risk-adjusted scoring metrics into performance-based physical security assessments, several avenues for future research should be explored. First, developing an approach for “global” scoring adjustments, considering the residual protection times in different attack path combinations, could provide a more comprehensive and nuanced assessment of security measures across various scenarios and barrier combinations. In addition, conducting empirical studies to validate the effectiveness of the proposed approach in a range of real-world scenarios could strengthen its credibility and practical applicability.

Despite its first promising attributes, the integration of risk-adjusted scoring into physical security assessment also presents certain challenges. The development of comprehensive and accurate vulnerability metrics, as well as the determination of appropriate probability distributions, remains an ongoing endeavor. Balancing the need for simplicity in decision making with the desire for granularity in assessment is a delicate challenge. It should be noted additionally, that when using scores for cost-benefit analysis, a margin of security must be considered. This is due to the nature of scoring, which always reflects a range of vulnerability values. Furthermore, ensuring the seamless integration of risk-adjusted scoring into existing security frameworks and compliance requirements requires careful navigation. The potential for subjectivity in scoring underscores the importance of establishing consistent and transparent scoring criteria. As the field advances, overcoming these challenges through collaborative efforts, empirical validation and continuous refinement of methodologies will be essential to unlocking the full potential of risk-adjusted scoring in strengthening critical infrastructure security.

References

Aradau, C. 2010. Security that matters: Critical infrastructure and objects of protection. Security dialogue, 41(5), 491-514.

Braband, J. 2008. Beschänktes Risiko. QZ. Qualität und Zuverlässigkeit 53.2 (2008): 28-33.

De Felice, F. I. Baffo and A. Petrillo. 2022. Critical Infrastructures Overview: Past, Present and Future. Sustainability, 14(4), 2233.

First.org 2023. https://www.first.org/cvss/.

Farrell, A. E., H. Zerriffi and H. Dowlatabadi. 2004. Energy infrastructure and security. Annu. Rev. Environ. Resour., 29, 421-469.

Harnser Group. 2010. A Reference Security Management Plan for Energy Infrastructure. European Commission.

Hurst, W., M. Merabti and P. Fergus. 2014. A survey of critical infrastructure security. In Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference, ICCIP 2014, Arlington, VA, USA, March 17-19, 2014, Revised Selected Papers 8 (pp. 127-138). Springer Berlin Heidelberg.

Kovacevic, A., Nikolic D. 2015. Cyber attacks on critical infrastructure: Review and challenges. Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance, 1-18.

Krisper, M. 2021. Problems with Risk Matrices Using Ordinal Scales. arXiv preprint arXiv:2103.05440.

Lichte, D., S. Marchlewitz and K.-D. Wolf. 2016. A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

Termin, T., D. Lichte and K.-D. Wolf. 2021. Risk analysis for mobile access systems including uncertainty impact. In: Proceedings of the 31th European Safety and Reliability Conference and 16th Probabilistic Safety Assessment and Management Conference.

Termin, T., D. Lichte and K.-D. Wolf. 2022. Approach to generic multilevel risk assessment of automotive mobile access systems. In: Proceedings of the 31th European Safety and Reliability Conference and 17th Probabilistic Safety Assessment and Management Conference.

Termin, T., D. Lichte and K.-D. Wolf. 2023. Risk Adjusting of Scoring-based Metrics in Physical Security Assessment. In: Proceedings of the 32th European Safety and Reliability Conference and 18th Probabilistic Safety Assessment and Management Conference.