Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P011-cd

Risk Adjusting of Scoring-based Metrics in Physical Security Assessment

Thomas Termin
Institute for Security Systems, University of Wuppertal, Germany. E-mail: thomas.termin@uni-wuppertal.de

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

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

Scoring-based systems are used worldwide to assess safety and security risks. Due to their ease of use, qualitative and semi-quantitative metrics are very popular. However, there may be the possibility that these scores do not accurately reflect the real risk, as was e.g. shown by Braband (2008) or Krisper (2021). In the worst case, this can lead to a misguided investment in measures. To avoid this, an adjustment of the scoring to a quantitative metric is required. The examples of the semi-quantitative Harnser metric and the quantitative vulnerability metric of Lichte et al. (2016) from physical security – in this work called intervention capability metric (ICM) – are used to show in this paper how to transfer a well-defined performance mechanism for quantitatively calculating physical vulnerability into consistent scores. To enable the transfer, this paper performs a metrical analysis. The results of the Harnser metric are extended by estimated probability intervals and compared to the results of the ICM. Different types of scales are used. Subsequently, we analyze measures to align the results of these two metrics, such as modifying the assignment of scores to scale categories or adjusting the probability intervals behind the scores. As an output, the metrical analysis generates rating scales for the Harnser scoring system that can be used to replicate quantitative vulnerability values. The results contribute to making more risk-appropriate decisions. Finally, we critically evaluate possibilities and limitations of metrical adaptability and summarize results.

Keywords: Metrical Analysis, Physical Security, Vulnerability Analysis, Decision-Making.

1. Introduction

Scorings are simple tools to assess risks in a quick way. Scoring systems that use descriptors such as "likely" or "unlikely" are useful when evaluating complicated issues (Newsome, 2013). Simplicity is an important prerequisite for making better decisions (Gigerenzer, 2014). This assumes that what is generated by scorings is also appropriate for risk (Braband, 2008). In the worst case, this can lead to a misguided investment in measures. To avoid this, an adjustment of the scoring to a quantitative metric is required (Krisper, 2021).

On the example of the semi-quantitative Harnser metric and the quantitative vulnerability metric of Lichte et al. (2016) from physical security – in this work called intervention capability metric (ICM), it is shown in this paper how to transfer a performance mechanism for quantitatively calculating physical vulnerability into consistent scores so that both assessments result in comparable vulnerability ratings.

For enabling the transfer, this paper performs a metrical analysis. The results of the Harnser metric are extended by estimated probability intervals and compared to the results of the ICM. Different types of score linkage and scales are used. Subsequently, measures to align the results of these two metrics are analyzed, such as modifying the assignment of scores to scale categories or adjusting the probability intervals behind the scores. As an output, the metrical analysis generates rating scales for the Harnser scoring system that can be used to replicate quantitative vulnerability values.

The remainder of this paper is structured as follows: Section 2 presents challenges using scoring-based metrics in comparison to quantitative metrics. As examples for scorings, the Harnser metric and the Failure Mode and Effect Analysis (FMEA) are described. Section 3 includes our approach proposed to align results of the Harnser scoring to real vulnerability levels. It is divided into the definition of the reference model setup under investigation and conducting the actual metric analysis. For demonstration purposes, we show how to align different Harnser scoring scales to vulnerability values based on a

quantitative analysis. This paper makes a valuable contribution to making more risk-appropriate decisions. Finally, possibilities and limitations of metrical adaptability are critically evaluated and results are summarized.

2. Background

Physical security risk is classically assessed based on threat, vulnerability and impact (Lichte et al., 2017). The focus in physical security risk assessment is placed on vulnerability and impact because:

- threats are epistemic and therefore difficult to quantify.
- vulnerability can be reduced by a defender investing in security measures. Quantitative metrics are available.
- it is assumed that a defender can quantify the extent of physical damage.

In the quantitative ICM, the interplay between the intrusion time of an attacker and the reaction time of a defender is assessed via the interaction of protection, observation and intervention. In order to take uncertainties about the performance of security functions into account, probabilistic density functions are assigned to the assessment parameters.

The quantitative calculation of vulnerability requires the confident use of mathematical statistics and probability theory. A simpler variant for calculating physical vulnerability is proposed in the semi-quantitative scoring system Performance Risk-based Integrated Security Methodology (PRISM) of the Harnser Group (Harnser, 2010). By using the PRISM, hereafter only referred to as the Harnser metric, the assessment parameters are scored between "1" (low) and "5" (high) and summed. This results in a total score range from "3" to "15": "15" indicates that vulnerability is very low and "3" indicates that vulnerability is very high.

As qualitatively described in Termin et al. (2022) and criticized in Termin et al. (2021), there are biases compared to the ICM: If protection and intervention are good, but observation is very poor, then the Harnser vulnerability score would be in the midrange. However, according to the ICM, the system would be highly vulnerable, because an intervention can only succeed if an attacker is detected in time - i.e. quickly enough. The Harnser metric does not differentiate between individual barriers as the ICM does. For another, protection, observation and intervention are interpreted as equal contributions. As explained before, however, this is not reasonable. A similar phenomenon of deviations is found in other semi-quantitative metrics, such as Failure Mode and Effects Analysis (FMEA) (Braband 2008).

A total of three parameters, occurrence, significance, and detection, are scored between "1" (low) and "10" (high) and multiplied together. The product is the so-called Risk Priority Number (RPN). The highest achievable value is (10x10x10 =) "1000" (maximum risk), while the next lowest value is "900" (10x10x9).

If we now look at the minimum score instead of the maximum score, we notice that the risk for small scores scales differently than for large scores. The smallest risk is (1x1x1 =) "1", the next highest (1x1x2 =) "2". The distance between these two scores is "1", for the two values of the maximum expression "100". Since this is a semi-quantitative approach with an ordinal scale, it lacks a reference point that allows for proportionality.

However, FMEA scoring suggests that risk behaves differently at high scores than at lower scores (Braband, 2003). Whether this actually corresponds to real conditions must be critically questioned (Krisper, 2021). In addition, the full "bandwidth" of possible results between "1" and "1000" cannot be achieved in FMEA, i.e., for example, "950" is never reached by the given parameter combinations. This is a general problem with scoring-based approaches, since they only allow a defined, computationally prescriptive space of outcomes. In Braband (2003), the systemic weaknesses of FMEA are summarized as follows:

- Occurrence, significance and detection are characteristics on an ordinal scale, which means that multiplication is not defined mathematically.
- Similar risks should be assigned the same RPN. In FMEA, this cannot be guaranteed.
- Risks with the same RPN are not accepted to the same extent.

In order to mitigate the systematic weaknesses, the following three requirements are therefore placed on a risk scale for determining the RPN:

- "**Rational scaling**. The scaling of the evaluation tables must be at least approximately rational, i.e., the bandwidths b of the classes should be approximately equal.
- **Monotonicity**. If the risk for scenario i is less than the risk for scenario j, the RPN for scenario i must be less than or equal to the RPN for scenario j.
- **Accuracy**. If the RPN for scenario i is equal to the RPN for scenario j, the risk for scenario i and the risk for scenario j should be approximately equal." (Braband, 2012).

Depending on the metric, there are different ways in which information is collected and processed. As highlighted in Krisper (2021), an analysis of the quality of metrics can be conducted by measuring the prediction strength of a metric. A further discussion of the advantages and disadvantages of using scores especially in the context of risk matrices is presented, for example, in Julian (2011). The goal of this paper is to be able to evaluate and optimize the quality of the Harnser metric used to calculate physical vulnerability compared the quantitative ICM.

3. Approach

A sharp vulnerability criterion, as can be objectively mapped in the Intervention Capability Metric (ICM), cannot be implemented with the Harnser metric. The problem with using semi-quantitative metrics is stated in Krisper (2021) as follows: "A problem here is that by transforming quantitative values into a domain and scale, which only supports ordering relations, we lose the ability to do reasonable arithmetic, estimate uncertainty, or do any sophisticated mathematical analysis."

The Harnser scores do not have an underlying metric based on time, as is the case with ICM according to Lichte et al. (2016). For example, Harnser score "5" is defined as "There is no capability to prevent this scenario from occurring and causing worst-case consequences" (Harnser, 2010).

The background chapter already points out in qualitative form the deviations between the additive approach according to Harnser and the probabilistic approach according to Lichte et al. (2016). From a scientific perspective, questions arise as to how large the distortions between the two metrics actually are and what possibilities there may be to reduce them. In this chapter, a mathematical analysis is performed to answer this question.

The differences between the vulnerability scores of the two metrics are calculated using the Harnser metric and variation in means and standard deviations in the ICM. Measures to reduce the metric differences are then examined.

3.1. Reference Model Setup

For the metrical analysis, the following reference model setup is chosen: One barrier and one asset are considered. The barrier must be overcome by the attacker in order to reach the asset. The barrier has properties of protection, observation and intervention. The performance of the barrier functions is evaluated in case of an attack.

For the determination of vulnerability, quantitative counterparts are formulated for each Harnser score in the ICM, i.e. a protection score (P), an observation score (O) and an intervention score (I) are assigned to a mean and standard deviation of normal distributed parameters, as in this paper assumed (see Table 1). In actual practice, the defined levels can look quite different. In this context, experts can be consulted to define appropriate levels in the quantitative metrics that correspond to real-world conditions.

Table 1. Mapping of Scores to Performance Mechanisms

P	ICM 1	O	ICM 1	I	ICM 1
1	$\mu = 15$ $\sigma = 30$	1	$\mu = 135$ $\sigma = 30$	1	$\mu = 135$ $\sigma = 30$
2	$\mu = 45$ $\sigma = 30$	2	$\mu = 105$ $\sigma = 30$	2	$\mu = 105$ $\sigma = 30$
3	$\mu = 75$ $\sigma = 30$	3	$\mu = 75$ $\sigma = 30$	3	$\mu = 75$ $\sigma = 30$
4	$\mu = 105$ $\sigma = 30$	4	$\mu = 45$ $\sigma = 30$	4	$\mu = 45$ $\sigma = 30$
5	$\mu = 135$ $\sigma = 30$	5	$\mu = 15$ $\sigma = 30$	5	$\mu = 15$ $\sigma = 30$

The standard deviations are set to 30 (seconds) for all levels. The protection time increases as the score increases, whereas the observation time and intervention time each become shorter as the score increases. ICM 1 represents ICM variant number one. In the Harnser metric, all three parameters are always scored.

To enable a comparison between the scoring result and the quantitative result, presumed probability intervals are written behind the score totals (Newsome, 2013). Since it is not yet known a priori how the intervals are to be set in order to replicate the quantitative results as best as possible, an equal distribution is assumed: the 100 % (probability of vulnerability) is divided equally between the categories of the Harnser scale (compare Table 2).

Table 2. Harnser Scale

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

In total all possible (5x5x5 =) 125 permutations are considered. In the case of the ICM, 36 variants are calculated, whereby one variant considers the consideration of discrete values approximately. The configurations ICM 1 - ICM 35, on the other hand, were based on density functions. The standard deviations are defined in Table 3. The mean values of these variants are identical to those in Table 1.

Table 3. ICM Variants (with μ for each score from Table 1)

ICM	σ_P	σ_O	σ_I
Dis-crete	0.0000001	0.0000001	0.0000001
1	30	30	30
2	30	30	60
3	30	30	90
…	…	…	…
27	90	90	90
28	100	100	100
29	50	50	50
30	10	75	100
31	1	40	1
32	10	40	120
33	150	150	150
34	300	300	300
35	10	100	100

The higher the number of the variant up to No. 27, the higher the scatter used. Variants 28 to 36 represent configurations where further metric modifications are tested. The result of using the ICM is a quantitative vulnerability value between 0 (minimum) and 1 (maximum) for each permutation, which can be mapped to Harnser's vulnerability results based on the scale in Table 2. For the analysis runs, the following steps are generally performed:

- Plot of vulnerability results Harnser versus ICM according to permutation.
- Plot of the Harnser vulnerability results: The results are sorted according to the Harnser vulnerability mean, i.e. the ICM results are "taken along" and sorted to the sorted Harnser mean values. The result in each case is curve representing vulnerability values.
- Plot of the amount between the Harnser mean values and the ICM values.

The following analyses are performed:

- Calculating vulnerability over the sum of the scores, using a 13-tier scale.
- Calculating vulnerability score over the sum of the scores, using a three-tier scale.

3.2. Calculating vulnerability over the sum of the scores

A first object of investigation is to calculate how vulnerability changes when the following setup is defined: Two performance mechanisms are emphasized, while the third performance mechanism is expected to increase. Three variants are calculated. First, observation and intervention are held constant high while the protection is varied. Following the same principle, in variant two the observation is varied and in variant three the intervention is varied, while the other two performance mechanisms remain particularly pronounced. The ICM results in Figure 1 reveal that the third variant achieves the best vulnerability reduction. Variant one and two are identical in terms of vulnerability reduction and lower than variant one.

It follows from this analysis that the Harnser metric does not distinguish between different resource distributions. For the ICM 1, the effect of a redistribution of resources can be demonstrated quantitatively. It should be noted, however, that this effect applies to ICM 1, taking into account the assumptions made. Depending on the properties of a barrier, the result for vulnerability may be different.

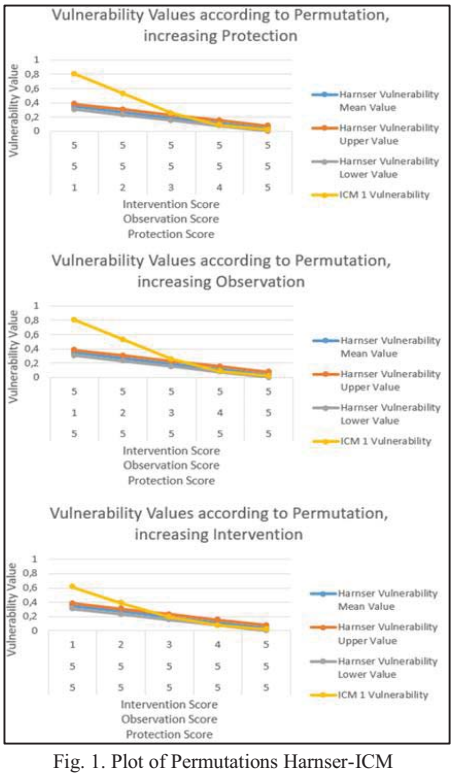

Fig. 1. Plot of Permutations Harnser-ICM

In a next step, the estimated probability intervals, which can be determined with the scale from Table 2 for each of the (5x5x5 =) 125 score combinations, are mapped to the quantitatively calculated results of the ICM. Then, the Harnser metric results and the ICM results are sorted by the magnitude of the Harnser scores (see Figure 2).

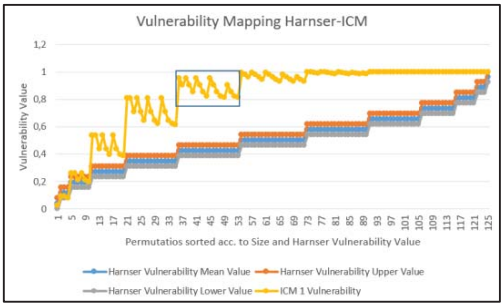

Fig. 2. Results of the Calculated Permutations Harnser-ICM

This mapping of results in a curve. While the Harnser results form a continuous curve of cubic progression with plateaus of probability intervals, the vulnerability results, which are ordered by Harnser values, jump. The ICM results form a discontinuous curve of limited growth. Two questions can be asked when examining Figure 2: Why do we have probability plateaus and why do the values of the ICM vulnerability values jump?

To answer the first question, attention must be paid to the permuted scores: Protection, Observation, and Intervention are varied between "1" and "5" in every possible manifold, i.e., there may be, for example, once P = "2", O = "3", I = "5" or P = "5", O = "3", I = "2". The score sum and thus the assumed probability interval are the same in both cases. Figure 2 shows that score sums of the same value occur more often in the "middle field". To answer the second question about the jumping of the ICM values, a series of permutations, marked by a blue rectangle in Figure 2, is picked out as an example and examined more closely.

The calculation results of the permuted variants are listed in Table 4 as an excerpt from the blue marked area shown in Figure 2. High values (red), medium values (orange) and low values (yellow) are marked as examples. The attributes high, medium and low refer to the considered range at the quantitative results considered here.

Table 4. Excerpt of Calculated Permutations

P	O	I	Sum	Low.	Up.	Mean	ICM 1 Vulnerab.
1	4	5	10	0.385	0.462	0.4235	0.95367115
1	5	4	10	0.385	0.462	0.4235	0.90338094
3	4	3	10	0.385	0.462	0.4235	0.85309073
3	5	2	10	0.385	0.462	0.4235	0.82195999
4	1	5	10	0.385	0.462	0.4235	0.95367115
4	2	4	10	0.385	0.462	0.4235	0.90338094
4	3	3	10	0.385	0.462	0.4235	0.85309073

The probability intervals, which are assumed behind the score sums of the Harnser metric, are sub-optimally chosen. The example of the comparison of Harnser vulnerability values and ICM 1-Vulnerability values can be used to illustrate that there are large distortions in certain parts.

From the user's point of view, it would be beneficial to have a scale classification in the scoring system that ideally corresponds to the quantitatively calculated vulnerability values of the respective ICM variant. For this purpose, the progressions of both vulnerability curves are first analyzed qualitatively (see Figure 3):

The jumps of the ICM vulnerability values are differently pronounced depending on the assigned Harnser plateau. While the fluctuations of the ICM vulnerability values at the beginning and at the end of the curve, which is composed of the Harnser plateaus associated with the score sums "3" to "15", are small, they are significantly larger in the middle field.

Consequently, in order to be able to describe as far as possible all ICM vulnerability values by a presumed probability interval from the Harnser scoring, the choice of different bandwidths of presumed probability intervals written behind a score sum is necessary. Another insight is that the presumed probability intervals can have a common intersection, for example score "10": 0.98 - 1.00 and score "15": 0.99 - 1.00.

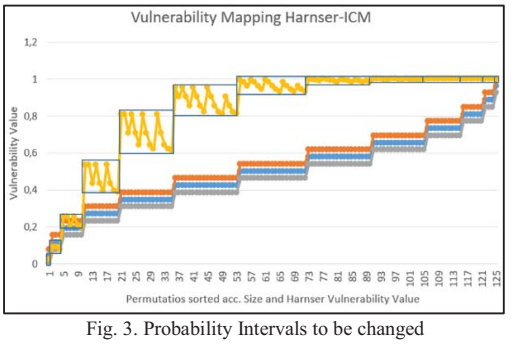

Fig. 3. Probability Intervals to be changed

In order to enable this scale fitting, an analysis of the vulnerability values of the sorted permutations is required. The smallest ICM vulnerability value within the length of a Harnser plateau is to be selected as the new lower interval limit of the corresponding score sum, the largest ICM vulnerability value accordingly as the new upper interval limit. The results can be seen in Table 5.

Table 5. Redefined Harnser Scale for ICM 1

V Score	3	4	5	6	7	8	9	10	11	12	13	14	15
Lower Value	1	1	1	1	0.998	0.984	0.931	0.81	0.614	0.388	0.195	0.077	0.024
Upper Value	1	1	1	1	1	1	0.994	0.954	0.807	0.534	0.257	0.09	0.024
Mean Value	1	1	1	1	0.999	0.992	0.963	0.882	0.7105	0.461	0.226	0.084	0.024

The plot of vulnerability scores for all 125 permutations by size and Harnser mean in Figure 4 shows successful alignment of the Harnser scoring system with ICM Variant 1.

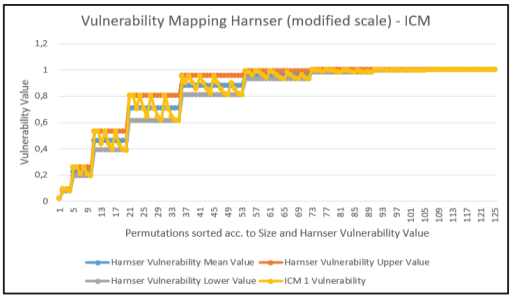

Fig. 4. Sorted Results of the Permutations Harnser (modified scale) – ICM

The quantitatively calculated vulnerability values can also be sorted by size within the plateaus as spanned by the presumed probability intervals. This shows that the ICM 1 values are approximately equally distributed within the plateaus in Figure 5.

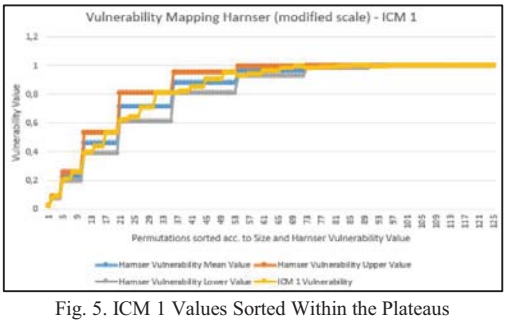

Fig. 5. ICM 1 Values Sorted Within the Plateaus

In specific use cases, however, it may be the case that the mean values and standard deviations of protection, observation, and intervention may be quite different from those in ICM 1. This can be seen when the vulnerability results of variant 30 are plotted to the results in Figure 6 (compare Figure 5).

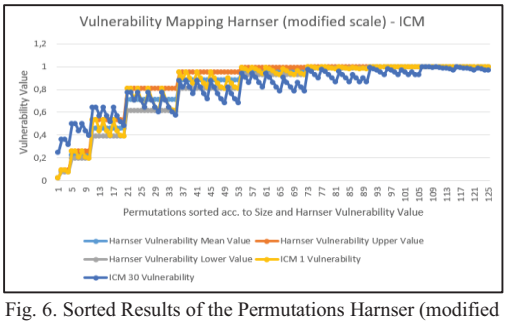

Fig. 6. Sorted Results of the Permutations Harnser (modified scale for ICM 1) – ICM 1 and ICM 30

For the variant ICM 30, a different Harnser scale is needed to map the quantitative results. The procedure to do this is identical to the one in the previous analysis: For each interval length of the Harnser plateaus, the respective largest and smallest ICM values are set as limits of the presumed probability intervals (see Table 6).

Table 6. Redefined Harnser Scales for ICM 30

V 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

As a result, the Harnser scale is now compatible with the vulnerability values of the ICM 30 (see Figure 7). The probability intervals based on the scoring now cover ICM 30 values, but no longer all values of ICM 1.

To be able to consider the vulnerability values of both variants in the Harnser scale, it is necessary to analyze the ICM values of both variants: For each plateau (Harnser), the minimum ICM value over both calculated ICM variants is selected for the lower interval limit. For the upper interval limit, the maximum ICM value is selected for both calculated ICM variants.

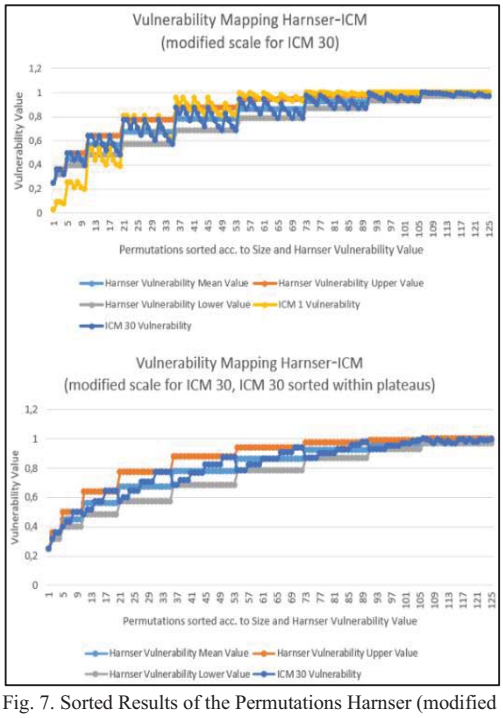

Fig. 7. Sorted Results of the Permutations Harnser (modified scale for ICM 30) – ICM 1 and ICM 30

The Harnser scale can be setup as defined in Table 7. As can be seen in Figure 8, the Harnser scale is compatible to both ICM variants.

Table 7. Redefined Harnser Scales for ICM 1 and 30

V Score	3	4	5	…	14	15
Lower Value	0.967	0.967	0.967	…	0.077	0.024
Upper Value	1	1	1	…	0.36	0.246
Mean Value	0.9835	0.9835	0.9835	…	0.2185	0.135

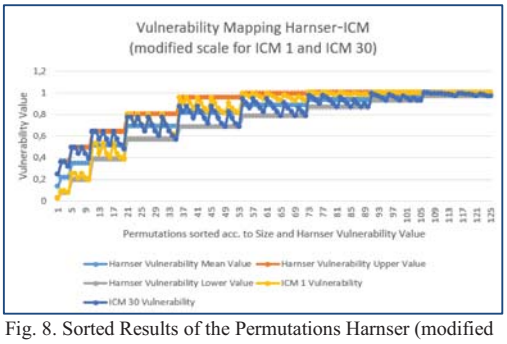

Fig. 8. Sorted Results of the Permutations Harnser (modified scale for ICM 1 and ICM 30) – ICM 1 and ICM 30

In today's standards, such as ISO/SAE 21434 (Cybersecurity) or ISO 26262 (Safety), vulnerabilities are not sorted on a thirteen-tier scale as is done in the previous analysis. Instead, it is common to use a three- to five-tier scale (ISO/SAE, 2022). The question to be asked is how well a Harnser scoring with a three-tier rating scale can mirror results from the ICM, e.g. ICM 1. For answering this question, the scale from Table 2 is redefined. Harnser score sums are now sorted on a scale with three categories; High, Medium, and Low (see Table 8).

Table 8. Three-Tier Harnser Scale

Categ.	High	Medium	Low
Sum	"3-6"	"7-10"	"11-15"
LIM	0.66	0.33	0
UIL	1	0.66	0.33
MI	0.83	0.495	0.165

An equal distribution of 13 possible score sums on three categories is not possible, therefore it is defined that the score sums "3" - "6", "7" - "10" and "11" - "15" each belong to one category. The assignment of suspected probabilities to scale categories follows the same principle as before: High score sums indicate low-suspected vulnerability, whereas low score sums indicate high suspected vulnerability. Behind the categories, the suspected probability intervals are initially divided equally, meaning "High = 0.66 - 1", "Medium = 0.33 - 0.66" and "Low = 0 - 0.33". All permutations are calculated and plotted again in Figure 9.

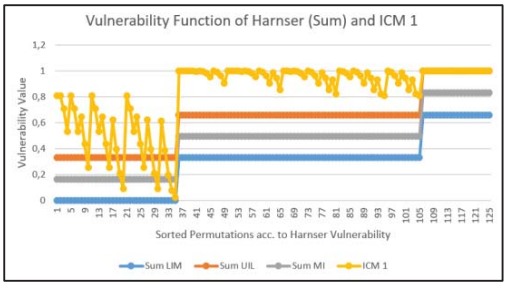

Fig. 9. Sorted Results of the Permutations Harnser (three-tier scale) – ICM 1

It can be examined how many ICM values actually lie in the presumed probability interval assigned to a plateau. For this purpose, in addition to the variant ICM 1, the configurations ICM 15 and ICM 27 from Table 3 are considered. It is defined: An ICM value lies within a plateau if it lies on or within the interval boundaries. The results are plotted in Figure 10. In the third interval (here: length of plateau two), all ICM values lie within the plateau for all ICM variants, but all ICM values in the second interval lie outside. In the first interval, an increase in the dispersion of the ICM causes distortions in the approximation of both metrics.

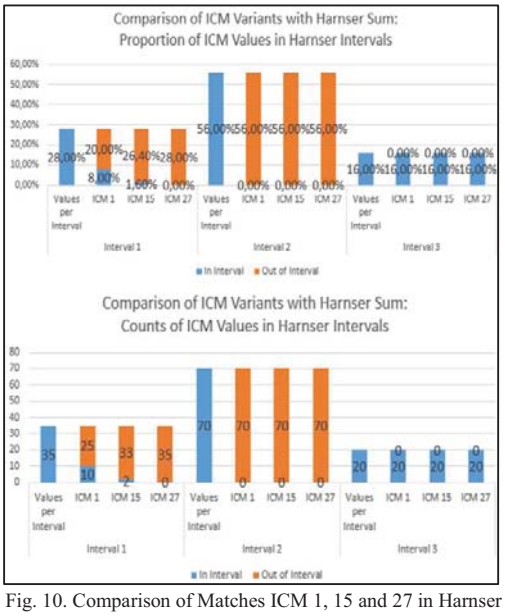

Fig. 10. Comparison of Matches ICM 1, 15 and 27 in Harnser

As in the case before, this Harnser scale can also be made compatible with specific ICM variants. The same approach is used as before. For each plateau, the largest and smallest ICM values are

searched for. These are then defined as the upper and lower interval limits of the plateau. This results in the new scale division to Table 9.

Table 9. Three-Tier Harnser Scale compatible with ICM 1

Categ.	High	Medium	Low
Sum	"3-6"	"7-10"	"11-15"
LIM	0.99	0.8	0.1
UIL	1	1	0.81
MI	0.995	0.9	0.445

What is striking in this context is that the width of the assumed probability intervals increases as far as the scale categories are reduced. With the 13-tier scale, the widths of the probability intervals were still moderate. In the case of the three-tier scale, however, the probability intervals behind the scale categories are quite large.

If the Harnser scoring is used and the result is, for example, a vulnerability score of "12", then a real vulnerability of about 0.1 to 0.81 is present. At this point, it must be critically questioned to what extent this scale classification helps users to allocate limited resources to security measures.

4. Summary

When using scores on an ordinal scale, mathematical operations are undefined, consequently they cannot be used for quantitative calculations. A quantitative metric however - here using ICM as an example - can be used to translate a performance mechanism into consistent Harnser score levels. By this transfer, it is possible to replicate quantitative results of a concrete ICM variant with the scoring.

This transfer has been performed once for the example of classical Harnser scoring with a thirteen-tier scale and once for Harnser scoring with a three-tier scale to show how metric alignment can succeed so that both assessments result in comparable vulnerability levels. Concluding, the approach proposed in this paper can reduce the incompatibility between the two metrics. In this paper, it is also demonstrated how the Harnser scale can be made compatible to several ICM variants.

It can be shown that the widths of the presumed probability intervals become larger when fewer scale categories are used, i.e. users have to be careful when interpreting the scorings. In future research, we want to investigate the extent to which ICM values can be replicated by Harnser scoring when there are conflicting requirements to consider, e.g., all ICM values should lie in the plateaus of the Harnser metric versus the estimated probability intervals must not overlap.

In addition, the approach described in this paper can help to adapt scoring systems in a wide variety of application areas in order to make decisions that are more appropriate to actual risk.

References

Braband, J. (2003). Improving the risk priority number concept. Journal of System Safety 39.3 (2003): 21-23.

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

Braband, J. (2012). A Risk-based Approach towards Assessment of Potential Safety Deficiencies. Achieving Systems Safety. Springer, London, 2012. 209-223.

Braband, J. (2019). A New Approach towards Likelihood Evaluation in Railway Cyber Security Assessment. In: Proceedings of the Third International Conference on Reliability, Safety, and Security of Railway Systems.

Gigerenzer, G. (2014). Risiko: Wie man die richtigen Entscheidungen trifft. C. Bertelsmann Verlag, 2014.

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

Julian, T. (2011). What's right with risk matrices. Management Policy.

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.

Newsome, B. (2013). A practical introduction to security and risk management. SAGE Publications, 2013.

ISO/SAE (2021). ISO/SAE 21434:2021. Road vehicles – Cybersecurity engineering. https://www.sae.org/standards/content/iso/sae21434.

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.