Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26292-cd

On Benchmarking Modified Metrics in Security Risk Assessment

Thomas Termin

Institute for Security Systems, University of Wuppertal, Germany. E-mail: thomas.termin@witte-automotive.de

Dustin Witte

Institute for Security Systems, University of Wuppertal, Germany. E-mail: witte@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

Risk assessment often requires balancing accuracy and usability. While quantitative metrics promise objectivity, they are typically costly to apply, leading practitioners to rely on qualitative, semi-quantitative, or simplified quantitative metrics. However, this entails modifications to quantitative metrics that may introduce discrepancies and reduce validity. This paper aims to contribute to the assessment of the quality of such metrics by conceptualizing metric modification as a structured design space defined by key degrees of freedom, including scaling, dimensionality reduction, and scenario clustering. Rather than proposing another metric, the paper focuses on the conditions under which modified metrics can be considered methodologically defensible with respect to a quantitative reference. Criteria for qualifying deviations from benchmark metrics are discussed, covering objectivity, reliability, scale resolution, contextual fit, and challenges related to aleatoric and epistemic uncertainty. Based on these criteria, the paper derives explicit assumptions and alignment strategies that allow systematic identification, explanation, and limitation of distortions introduced by metric simplification. The approach deliberately abstracts from adaptive attacker behavior; changes in attacker capabilities, tools, or strategies are treated as defining distinct scenarios rather than as dynamic modifications within a fixed scenario. Using physical security as an illustrative domain, the paper examines the assumptions required for metric alignment and contributes guidance for the practical use of simplified metrics aligned with quantitative risk assessment. The results provide actionable guidance for metric designers and practitioners on when simplified metrics are suitable for decision support and where their use becomes methodologically unjustifiable.

Keywords: Modified Metrics, Risk Analysis, Uncertainty, Benchmarks.

1. Introduction

Risk assessment is a core element of physical security planning. It supports the identification and mitigation of vulnerabilities before threats materialize (Harnser, 2010). While quantitative methods ideally provide objective and reproducible results (Lichte et al., 2016), their application in practice is often limited by data availability and expert knowledge.

As a result, practitioners rely on modified metrics, including qualitative, semi-quantitative, and simplified quantitative approaches. These methods improve usability through scoring, ordinal scales, or scenario clustering, but reduce resolution and may introduce systematic distortions if they are not explicitly aligned with an underlying quantitative reference (Braband, 2003; Krisper, 2021).

This paper develops a benchmark-oriented methodological approach for assessing when modified security metrics remain defensible relative to a quantitative reference. Rather than proposing a new metric, it formalizes the design space of metric modification, defines a structured alignment procedure, and specifies the assumptions under which deviations from

benchmark metrics can be justified. The paper introduces three elements:

(i) a structured alignment procedure based on mapping, parameter alignment, and iterative validation.
(ii) design dimensions that govern metric comparability, including scoring logic, scaling, and aggregation.
(iii) criteria for benchmark selection, including objectivity, resolution, contextual relevance, and the treatment of epistemic and aleatoric uncertainty.

The approach supports the integration of modified metrics into risk assessment processes by reducing incompatibilities with benchmark-based assessments, while explicitly excluding the correction of metric-inherent limitations, such as the use of ordinal values. Although illustrated for physical security, the principles apply to other security and safety domains.

2. Background and Related Work

Safety and security metrics are used to assess the effectiveness of protective measures in technical systems. In security assessment, they typically estimate the likelihood and consequences of successful attacks on critical assets (Garcia, 2008), often under assumptions of rational attacker behavior and defined environmental constraints. Existing metrics differ widely in complexity, data requirements, and methodological foundations, including approaches such as the Common Vulnerability Scoring System (CVSS), attack potential-based methods, or attack vector-based approaches (ISO/SAE, 2021).

A commonly used taxonomy distinguishes quantitative, semi-quantitative, and qualitative metrics (Newsome, 2013). Quantitative metrics rely on probabilistic models and empirical data to produce continuous values but often require detailed input data that are scarce in security contexts characterized by epistemic uncertainty in attacker behavior. Semi-quantitative metrics reduce this complexity by discretizing continuous parameters into ordinal categories and aggregating them through weighted scoring, trading resolution for usability. Qualitative metrics rely entirely on descriptive assessments and expert judgment and are therefore widely applied due to their intuitive nature and low data requirements.

Each metric type reflects a trade-off between accuracy, transparency, and usability. In this paper, the term modified metric denotes any assessment approach that deviates from an idealized reference description (Termin et al., 2023). This reference, termed a benchmark metric, represents an idealized quantitative metric assumed to approximate true risk levels (Termin et al., 2025).

Despite their practical relevance, modified metrics face well-known challenges (Braband, 2003; Braband, 2012; Krisper, 2021), including information loss due to reduced resolution or dimensionality, mapping inconsistencies caused by missing transformation rules, missing benchmark alignment, and opaque aggregation based on weakly justified weighting schemes.

These challenges are closely linked to uncertainty. Safety metrics are often dominated by aleatoric uncertainty, which can be addressed probabilistically and enables objective comparison of design alternatives. Security metrics, by contrast, are primarily affected by epistemic uncertainty, as attacker intent and behavior cannot be reliably represented by probability distributions (Kiureghian and Ditlevsen, 2009). Consequently, decisions rely on human judgment regarding scenario selection (Witte et al., 2020), and methods developed for aleatoric uncertainty cannot be directly transferred to security contexts.

Integrating safety and security metrics therefore requires bridging fundamentally different logics: one grounded in statistical modeling, the other in judgment, assumptions, and incomplete knowledge (Abdo, 2017). Although epistemic uncertainty is sometimes approximated using pseudo-probabilities, such representations risk conveying a false sense of certainty rather than resolving the underlying lack of information.

Recent work emphasizes benchmark-driven alignment as a means to improve the comparability and informativeness of simplified metrics (Braband, 2008; Krisper, 2021; Termin et al., 2023). However, systematic and generalizable alignment procedures across domains and system types remain difficult to find. This paper addresses this gap by proposing a structured alignment approach that clarifies how modified metrics can be assessed and validated without obscuring their inherent limitations, while highlighting key challenges associated with defining and applying benchmark metrics.

Compared with our prior ESREL contributions, this paper shifts the focus from specific metric designs to a general methodological problem. Earlier work addressed the alignment of scoring-based metrics in physical security assessment (Termin et al., 2023), vulnerability-aligned metrics in performance-based assessments (Termin et al., 2024), and the development of a hybrid security metric (Termin et al., 2025). The present paper abstracts beyond individual metric forms. It proposes a benchmark-oriented methodological framework that supports the comparison, alignment, and qualification of modified metrics relative to quantitative benchmark metrics.

3. Approach

This Chapter presents a structured procedure for aligning simplified security metrics with a quantitative benchmark metric. The purpose is not to introduce a new metric, but to define a systematic framework for assessing when modified metrics remain comparable and methodologically defensible with respect to a quantitative reference. The approach comprises four steps, summarized in Figure 1.

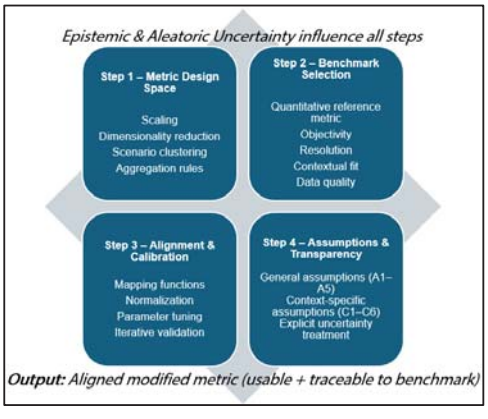

Figure 1. Four-Step Alignment Process for Modified Security Metrics.

The first step identifies the control variables that define a metric's structure, including inputs, outputs, and internal logic. Key degrees of freedom in metric modification are grouped into three categories: (1) scaling (e.g., continuous versus discretized values or linear versus logarithmic transformations), (2) dimensionality reduction through aggregation of multiple risk contributions, and (3) scenario clustering, where similar attack or hazard scenarios are combined into representative categories. These choices determine how closely a modified metric can approximate a benchmark and where systematic distortions may occur.

The second step selects an appropriate benchmark metric. The benchmark represents an idealized quantitative reference and must satisfy criteria such as objectivity, reproducibility, sufficient resolution, and contextual relevance. It does not represent ground truth but serves as a consistent reference against which deviations introduced by simplification can be identified.

The third step aligns modified and benchmark metrics through explicit mapping of ordinal categories to quantitative intervals, parameter tuning, and iterative validation using representative scenarios. The objective is not to eliminate differences, but to reduce systematic bias and preserve interpretability relative to the benchmark.

The final step requires explicit documentation of all assumptions introduced during modification and alignment, including those arising from incomplete information such as scenario selection, parameter ranges, or boundary conditions. While these assumptions cannot resolve epistemic uncertainty, their explicit formulation improves transparency and clarifies the limits of simplified metrics.

Together, these steps provide a concise methodological basis for calibrating modified metrics against benchmark references and for distinguishing acceptable simplifications from methodologically unjustifiable ones.

3.1. Design Space for Metric Modification

In physical vulnerability assessment, metric modification is commonly used to translate complex barrier properties, such as resistance against specific attacker profiles, into more manageable representations. A typical approach is scoring, where attributes such as protection, observation, and intervention are clustered and assigned ordinal values, usually based on expert judgment (Harnser, 2010).

These simplifications inevitably entail information loss. Ordinal scores represent value ranges rather than precise quantitative measures and therefore introduce uncertainty relative to an ideal reference metric (Krisper, 2021; Termin et

al., 2023; Termin et al., 2024). The resulting degrees of freedom define a design space for metric modification, which can be structured along eight recurring dimensions:

(i) Scaling of results, where continuous outcomes are mapped to normalized or categorical ranges (e.g., [0,1] or low/medium/high), improving the comparability at the risk of oversimplification.
(ii) Scaling of influencing factors, adjusting input ranges to account for differing magnitudes, which requires careful calibration to avoid further information loss.
(iii) Selection of influencing factors, balancing completeness against explanatory focus, as overly narrow selections omit relevant aspects while overly broad ones dilute interpretability.
(iv) Aggregation of factors, defining how inputs are weighted and combined, enhancing usability but potentially introducing bias when interactions or weights are weakly justified.
(v) Treatment of uncertainty, ranging from implicit suppression to explicit representation through confidence intervals or probability distributions.
(vi) Integration of temporal dynamics, extending static metrics with time-dependent elements such as feedback from observed events or updated threat information.
(vii) Contextual adaptation, tailoring metrics to specific scenarios (e.g., site-specific correction factors), increasing accuracy at the cost of additional assumptions.
(viii) Dimensionality management, either expanding metrics to multiple impact dimensions (e.g., environmental, economic, reputational) or reducing complexity by clustering dimensions into composite criteria.

3.2. Metric Benchmarks

The accuracy of modified metrics can be assessed relative to a benchmark metric (Aigner and Khelil, 2020). Benchmarks support both absolute assessments, indicating how closely results approximate a theoretical optimum, and relative comparisons, such as ranking alternative metrics. A central challenge is determining which quantitative metrics are suitable benchmarks. To function as proxies for "true" risk values, benchmarks require systematic validation.

At a minimum, benchmark metrics must deliver objective, consistent, and reproducible results, such that identical inputs lead to identical outputs. They must also provide sufficient resolution and scale sensitivity to capture meaningful differences between modified metrics and remain relevant to the specific application context. Even methodologically rigorous metrics fail as benchmarks if they emphasize aspects that are irrelevant to the system under study.

Ideally, benchmarks are grounded in high-quality data and validated through scientific studies or recognized standards. From these requirements, five core criteria for benchmark selection can be derived: objectivity and reliability, contextual relevance, scalability and accuracy, data consistency, and acceptance within the expert community.

The principal difficulty in defining benchmark metrics lies in the treatment of uncertainty. In safety-related contexts, uncertainty is often predominantly aleatoric, such as random component failures, and can be addressed probabilistically. This enables objective comparisons and cost–benefit analyses and allows benchmark metrics to be derived from established statistical models with analytically tractable uncertainty.

Security metrics, by contrast, are largely shaped by epistemic uncertainty. Attacker intent, capabilities, and evolving tactics cannot be reliably represented by probability distributions (Kiureghian and Ditlevsen, 2009). Consequently, benchmark metrics in security cannot be purely analytical. Decisions instead rely on human judgment influenced by organizational risk appetite, stakeholder interests, cultural factors, and situational context (O'Hagan, 2019). While epistemic uncertainty is sometimes approximated using simplified probability distributions, such as triangular distributions, these representations risk conveying a false sense of certainty, as they reflect belief rather than knowledge.

Estimating attack frequencies for specific infrastructures often relies on expert elicitation or analogies to past events. Such estimates remain sensitive to expert selection and information

updates. Consequently, benchmark metrics in the security domain can serve as meaningful reference points only if their epistemic limitations are explicitly acknowledged. This requires transparent documentation of assumptions, clear differentiation between aleatoric and epistemic uncertainty where feasible, and mechanisms for iterative updating.

Under these conditions, benchmark metrics can support the calibration of modified metrics while making explicit that certain uncertainties, such as the completeness of relevant threat scenarios, cannot be resolved by metrics and calculation alone.

3.3. Options for Metric Alignment

Ensuring comparability between benchmark metrics and modified metrics is a central methodological challenge, particularly when outputs differ in format (continuous versus categorical) or rely on heterogeneous input data. The following alignment strategies address this issue:

(i) Mapping of results. Ordinal categories are explicitly linked to quantitative intervals, for example by associating qualitative levels such as low, medium, and high with predefined probability ranges, thereby establishing a transparent relationship between simplified outputs and benchmark values (Termin et al., 2023).
(ii) Coherence of input data. Meaningful comparison requires congruent input data wherever possible; if different data sources are used, transformation or standardization is necessary to avoid structural bias.
(iii) Normalization of scales. Standardizing outputs to a common interval (e.g., [0–1]) enables direct comparison across metrics and reduces distortions caused by differing value ranges.
(iv) Alignment of dimensions. Modified metrics should address dimensions comparable to those of the benchmark, such as threat, vulnerability, and impact; where discrepancies exist, dimensional adjustments or weighting schemes are required.
(v) Assessment of information loss. Discretization reduces granularity relative to continuous benchmarks; this loss can be quantified by comparing categorized outputs with benchmark values, for example using sensitivity or specificity analyses or simulation studies to assess effects on decision quality.
(vi) Qualitative validation. Beyond quantitative alignment, expert judgment is required to assess plausibility and consistency, particularly in contexts dominated by epistemic uncertainty where numerical calibration alone may conceal assumption-driven effects.

These strategies allow simplified metrics to approach the expressiveness and comparability of idealized benchmark metrics. However, alignment remains context dependent and may affect usability. Domain-specific factors, including regulatory constraints, system architecture, and attacker models, ultimately determine both the feasible degree of modification and the effectiveness of alignment, as summarized in Table 1.

Table 1. Typical Modifications, Induced Distortions, and Alignment Measures.

Degree of Freedom	Typical Effect	Potential Distort-ion	Alignment Measure
Scaling (continu-ous to ordinal)	Higher usability (e.g., probabilities mapped to low/medium/high)	Loss of resolution	Category–interval mapping
Aggre-gation of factors	Single score for inputs (e.g. protection + detection + response)	Hidden weighting bias	Parameter tuning, sensitivity analysis
Scenario cluster-ing	Fewer representative cases (e.g., “insider” vs. “external threat”)	Scenario omission bias	Benchmark-based scenario selection
Dimen-sionality reduction	One overall risk score instead of separate values	Masked trade-offs	Dimen-sional alignment
Abstrac-tion of Uncer-tainty	Clear decisions without ranges (e.g., point estimates only)	False certainty	Explicit uncertainty documen-tation

3.4. Assumptions for Metric Alignment

Aligning simplified security metrics with benchmark-based assessments requires explicit assumptions. These assumptions ensure

methodological consistency and transparency while defining the conditions under which alignment between modified and benchmark metrics remains meaningful.

This Chapter distinguishes between general scientific assumptions (GA), which establish a cross-domain methodological baseline, and context-specific assumptions (CA), which adapt the alignment framework to a particular infrastructure, system, or threat environment. General assumptions apply independently of the use case and form the foundation for benchmark-based alignment:

GA1: Availability of a High-Quality Data Basis.
Both benchmark and modified metrics must be supported by empirical, simulated, or expert-derived data; without such a data basis, calibration cannot be meaningfully interpreted.

GA2: Conceptual Compatibility of Metrics.
Modified and benchmark metrics must be structurally compatible with respect to core input variables and assessment logic. Full identity is not required, but key constructs (e.g., vulnerability dimensions) must overlap or be mappable.

GA3: Existence of Mapping Mechanisms.
Systematic transformation mechanisms, such as normalization, categorization, or probability assignment, must exist to relate outputs across differing scales or formats.

GA4: Explicit Treatment of Uncertainty.
Uncertainty introduced by simplification must be addressed explicitly, for example through confidence intervals, sensitivity ranges, or probabilistic estimates, to ensure transparency and allow potential error to be assessed.

GA5: Iterative Refinement of Alignment.
Alignment is treated as an iterative process in which deviations between benchmark and modified metrics are used to refine parameters, weights, or aggregation rules.

Context-specific assumptions define the scope and applicability of alignment for a given use case:

CA1: Defined Baseline Infrastructure Unit.
Alignment starts from a simplified reference configuration (e.g., a single asset and barrier) that serves as a calibration anchor.

CA2: Representative Threat Scenarios.
A defined set of relevant and operationalized threat scenarios structures parameterization and determines metric relevance.

CA3: Parameter Alignment Using a Benchmark.
Scores, weights, or rules are calibrated through systematic comparison of modified outputs with benchmark results in controlled scenarios.

CA4: Scalability to Complex Topologies.
Aligned metrics are expected to remain consistent when applied to larger, interconnected systems with multiple assets or defense layers.

CA5: Recognition of Use-Case Priorities.
Application-specific priorities, such as usability, cost, or regulatory constraints, are reflected in metric design and aggregation.

CA6: Generalizability Across Similar Contexts.
Alignment patterns are assumed to be transferable within a defined scope, such as infrastructures of the same class or comparable threat environments.

The assumptions define both the scientific baseline (GA1–GA5) and the application-specific boundary conditions (CA1–CA6). While they enable a structured alignment process, they also define its limits. Increasing context specificity reduces the scope of valid generalization. This dual-layer structure balances standardization and flexibility while maintaining traceability to benchmark quality.

Explicit formulation of assumptions improves transparency by making simplification decisions traceable and alignment logic reproducible. It also provides a structured basis for sensitivity analyses. Beyond these technical aspects, clearly stated assumptions support informed dialogue between developers, domain experts, and decision-makers regarding the scope and limitations of modified metrics. Ultimately, benchmark-based alignment remains valid only within the boundaries defined by its assumptions; making these boundaries explicit preserves methodological soundness without overstating operational certainty.

3.5. Actionable Implications

Based on the alignment approach and assumptions discussed above, several practical implications for the design and application of modified security metrics can be derived. These implications do not prescribe specific metrics but

define conditions under which simplified metrics can be considered methodologically defensible.

First, modified metrics are defensible only if conceptual compatibility with the benchmark (GA2) and explicit treatment of uncertainty (GA4) are ensured. Without overlap in core constructs or transparent handling of uncertainty, alignment claims lose interpretability.

Second, the absence of comprehensive empirical data does not invalidate simplified metrics per se, but it limits the type of claims that can be made. In such cases, modified metrics can support internal consistency or comparative reasoning but cannot claim benchmark alignment.

Third, scenario clustering emerges as a dominant driver of distortion, often exceeding the impact of scaling or aggregation choices. Decisions on which scenarios are included or excluded therefore require scrutiny and explicit justification.

Fourth, ordinal scoring systems require explicit interval mapping if results are to be interpreted relative to quantitative references. Without such mapping, numerical aggregation may create an appearance of precision that is not epistemically justified.

Benchmark-based alignment is less a matter of mathematical refinement than of transparent design choices and clearly stated boundaries. Simplified metrics remain valuable tools for decision support, provided their assumptions, limitations, and intended use are made explicit rather than implicitly assumed.

3.6. Illustrative Mini-Case

To illustrate the alignment process, consider a simplified assessment of intrusion risk for a facility entrance protected by a physical barrier and an alarm system. A benchmark metric estimates the probability of successful intrusion based on quantitative parameters such as detection probability, delay time, and response time. For a given configuration, the benchmark model may estimate a probability of successful intrusion of 0.18.

In practice, a modified metric may represent vulnerability using an ordinal score ranging from 1 to 5 derived from expert assessment of protection strength, detection capability, and response readiness. Alignment requires mapping these ordinal categories to quantitative benchmark intervals. For example, a vulnerability score of 1 may correspond to intrusion probabilities below 0.05, while a score of 5 represents probabilities above 0.40.

Parameter alignment ensures that changes in system characteristics influence both metrics consistently. For instance, increasing detection probability or reducing response time must reduce both the benchmark intrusion probability and the vulnerability score.

Iterative validation then compares results across several representative scenarios. If the modified metric preserves the ranking of protection configurations and reflects major performance differences identified by the benchmark model, the simplified metric can be considered aligned for the intended decision context.

4. Discussion and Outlook

The methodology presented in Chapter 3 and conceptualized in Figure 2 demonstrates how simplified security metrics can be systematically aligned with benchmarks by balancing practical usability and methodological precision. The resulting actionable implications for metric design and use have been derived in Chapter 3.5 and are discussed here in a broader methodological context. From a broader ESREL perspective, the proposed approach relates to established practices in reliability engineering and probabilistic risk assessment, where benchmark models are used to assess simplified decision tools. In these fields, high-resolution probabilistic models often serve as reference systems for calibrating screening methods or scoring approaches. The approach proposed here follows the same principle while accounting for the stronger role of epistemic uncertainty in security risk assessment.

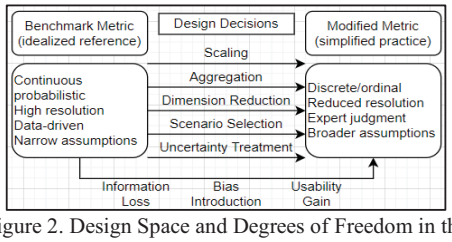

Figure 2. Design Space and Degrees of Freedom in the Modification of Security Risk Metrics.

Benchmarks provide reference points for assessing result quality and guiding metric design,

even though they rely on domain-specific assumptions and imperfect data. While they only approximate real-world risk, they help prevent simplified metrics from drifting away from empirical observations. Comparability between modified and benchmark metrics therefore requires explicit mapping, normalization, input harmonization, and sensitivity analysis to reveal information loss. Assumptions form the second structural pillar of the approach. General assumptions establish a methodological baseline, while context-specific assumptions define the scope of applicability. Together with design choices and benchmark alignment, they form an iterative refinement process that improves transparency while acknowledging epistemic limits.

Several limitations remain. Validated benchmarks are often unavailable, data and expert access may be limited, and assumptions can exert difficult-to-quantify influence. The proposed methodology improves traceability and robustness but cannot replace contextual expertise. Future work should focus on systematic documentation of assumptions, improved methods for uncertainty propagation, and dynamic alignment mechanisms using real-time data or adaptive learning. Where established benchmarks are difficult to find, hybrid reference approaches combining empirical evidence, expert judgment, and simulation may provide a practical path forward.

References

Abdo, H. (2017). Dealing with uncertainty in risk analysis: combining safety and security (Doctoral dissertation). Université Grenoble Alpes.

Aigner, A. and A. Khelil (2020, June). A benchmark of security metrics in cyber-physical systems. In IEEE International Conference on Sensing, Communication and Networking (SECON Workshops) 2020, pp. 1–6. IEEE.

Braband, J. (2003). Improving the risk priority number concept. Journal of System Safety 39, 21–23.

Braband, J. (2008). Beschränktes Risiko. QZ. Qualität und Zuverlässigkeit 53, 23–28.

Braband, J. (2012). A risk-based approach towards assessment of potential safety deficiencies. In Achieving Systems Safety, pp. 209–223. Springer, London.

Der Kiureghian, A. and O. Ditlevsen (2009). Aleatory or epistemic? Does it matter? Structural Safety 31, 105–112.

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

ISO/SAE (2021). ISO/SAE 21434:2021. Road vehicles – Cybersecurity engineering. SAE International.

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. international conference, Berlin, Germany.

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

O'Hagan, A. (2019). Expert knowledge elicitation: subjective but scientific. The American Statistician 73(sup1), 69–81.

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

Termin, T., D. Lichte, and K.-D. Wolf (2023). Risk aligning of scoring-based metrics in physical security assessment. In Proceedings of the 32nd European Safety and Reliability Conference and the 18th Probabilistic Safety Assessment and Management Conference.

Termin, T., D. Lichte, and K.-D. Wolf (2024). Vulnerability aligned metrics in performance-based physical security assessments. In Advances in Reliability, Safety and Security. ESREL 2024 Contributions, Part 7, pp. 179–188. Polish Safety and Reliability Association.

Termin, T., D. Lichte, and K.-D. Wolf (2025). Development of a hybrid metric for physical security assessment. In Proceedings of the 35th European Safety and Reliability Conference (ESREL 2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025), pp. 3314–3321. Research Publishing.

Witte, D., D. Lichte, and K.-D. Wolf (2020). Threat analysis: scenarios and their likelihoods. In Proceedings of the 30th European Safety and Reliability Conference (ESREL 2020) and the 15th Probabilistic Safety Assessment and Management Conference (PSAM15 2020), pp. 4589–4595.