BERGISCHE
UNIVERSITÄT
WUPPERTAL

Holistic Cyber-Physical Risk Assessment of Automotive Mobile Access Systems

Dissertation
for the Award of a Doctoral Degree
(Dr.-Ing.)

in the
Faculty of Mechanical Engineering and Safety Engineering

of the
University of Wuppertal

submitted by
Thomas Termin
from Wuppertal

First reviewer:	Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf
Second reviewer:	Univ.-Prof. Dr.-Ing. Tibor Jager
Date of submission:	12.04.2023
Day of the oral examination:	11.10.2023

Wuppertal 2023

Notice:

This work is a computer-assisted translation of the German doctoral thesis entitled "Ganzheitliche generische Risikobewertung von automobile Mobile-Access-Systemen".

Try to make sense of the things you see and question what the universe is made of. As hard as life may seem sometimes, there is always something to do and to be good at. It is important that you simply never give up. Remember to look at the stars - and not at your feet.

Stephen Hawking

Foreword by the First Reviewer

Nowadays, it is almost impossible to imagine technical systems without communication and data exchange with the environment. From configuration and control via the Bluetooth interface of a smartphone, which makes the complex implementation of user interfaces on the device superfluous, to quasi-permanent integration into platforms and networks via the internet and mobile radio or WLAN interfaces, as found in smart home devices, for example, IT-based communication is an essential part of the functionality of modern technology. However, in addition to all the advantages that IT-based communication offers, it also harbors vulnerabilities that arise, for example, from the availability of internet and mobile phone connections and, in particular, the vulnerability of IT components through networking. When we talk about security today, we usually mean "cybersecurity", i.e. the security of IT-based systems against attacks from "cyberspace", usually from the internet. The connection to the internet brings attackers from all over the world right to your doorstep, or better still, right into your home or vehicle. Protecting against such attacks is therefore a task that all modern and networked technical systems must fulfill. Recent technical guidelines and standards, such as ISO/SAE 21434: "Road Vehicles - Cybersecurity engineering", take this fact into account.

As ubiquitous IT connectivity involves more and more technical systems, concepts of "cyber-physical systems" are increasingly being discussed and developed. These systems are characterized by significant interaction with the physical world. For example, a car that gets out of control in an urban area due to a hacker attack can cause considerable damage to people and property. Security-related systems are particularly important in this context, as they have been developed to protect against physical dangers. In systems designed to ensure functional safety, which conceptually always include sensors and IT components, the focus therefore shifts to the appropriate design of IT security measures. While the IEC 61508 series of standards, for example, specifies quantitative criteria for the design of the availability (in the sense of the failure of components or subsystems) of functional safety systems in detail, there are no such specifications with regard to IT security.

This is a major current challenge for the people who design or assess such systems and are confronted with the question: How extensively must cybersecurity measures be designed to meet the security requirements in the physical world in terms of the underlying risks? The ISO/SAE 21434 mentioned above also does not contain any quantitative criteria for the design of cybersecurity systems. Accordingly, it is difficult to design physical security systems in the automotive sector, such as the automotive mobile access systems addressed in this dissertation, in a way that is appropriate in terms of the required level of security and thus risk-compliant. The reason for the still existing dichotomy in the assessment of the security of cyber-physical systems lies in the respective metrics. Quantitative security metrics, which would be necessary for a comprehensive consolidation of the two cyber-physical domains, are not commonly used in IT security.

In addition, interdependencies, such as those that can be established by statistically describable component failures or overcoming times of barriers in the physical world, are generally not mapped in IT security. This makes it difficult to compare physical and IT security levels. It is also difficult to assess the appropriate cross-domain design of security measures for cyber-physical systems in relation to a risk level. How and to what extent can the two cyber-physical domains be brought together in the security assessment by cleverly adapting the metrics, or how can a risk-appropriate design of the security measures in both domains, which may also be affected by interactions, be assessed? This dissertation is dedicated to this not entirely simple question.

Velbert, October 2023

Univ.-Prof. Dr.-Ing. K.-D. Wolf

Acknowledgments

"Management of security risk [...] is more an art than a science" (Wang et al., 2017, p. 53).

This research paper entitled "Holistic cyber-physical risk assessment of automotive mobile access systems" was written as part of the doctoral program between the WITTE Automotive Group and the Institute for Security Systems (ISS) at the University of Wuppertal (BUW) at the Chair of Mechatronics in the Faculty of Mechanical and Safety Engineering. The path to gaining knowledge is a special time for personal development and is associated with great challenges and efforts - both for the doctoral student and for the people who accompany him or her in the preparation of the dissertation. For this reason, I would first of all like to thank my supervisor, Univ.-Prof. Dr. Kai-Dietrich Wolf, who supervised this doctoral project and was always available for a constructive exchange of ideas. I would also like to thank Univ.-Prof. Dr.-Ing. Tibor Jager for his second opinion and valuable input during the preparation of my doctoral thesis.

I would also like to thank the WITTE Digital team for their stimulating advice and discussions, especially Paul Meier, Christian Goldschmidt and Michael Tworek for their support. Special thanks go to Mr. Rainer Gölz, Managing Director of WITTE Automotive, who made my doctoral project financially possible, so that I was able to conduct the dissertation in equal parts at the Institute for Security Systems and at WITTE Digital. I was given the opportunity to organize my time resources variably at the Institute and at WITTE. I would also like to thank my colleagues at WITTE and my companions in the industry, including Claudia Heussen-Mestor, Mario Schwarz, Thomas Angerer, Bernhard Huber, Heiko Huber, Christoph Bolsinger, Philip Marienfeld, Alfred Fuhr, Elka Sloan, Hannes Bauer, Robin Bauer, Olaf-Gerd Gemein and Daniel Hommen. They have always motivated me and helped me with my tasks.

I would also like to thank my university colleagues, Dustin Witte, Max vom Stein, Christian Marré, Max Hoppe, Manfred Dillenberg and Benjamin Dymel, as well as the assistant to the university professor, Sabine Kranz, who always supported me in my lecture supervision and scientific research and encouraged me in my plans. Furthermore, I would like to thank Mr. Roman Kochanek, Mr. Helge Schroda, Mr. Christoph Wegener and Mr. Dejan Djordevic for the lively exchange on security metrics and compliance. Many thanks to Enrico Zio, Dean of the Graduate School of the University Politecnico Milano in Italy, for the inspiring exchange on the topic of decision-making under uncertainty. Finally, a big thank you to my parents, who have always supported me emotionally and financially. My siblings, Kamil Termin and Kerstin Termin, were also always there for me in difficult times - thank you for your great patience and the trust you placed in me. I would never have got this far without your help.

Wuppertal, October 2023 Thomas Termin

Abstract

The growing global threat situation has far-reaching consequences for the standardization of product development processes in the automotive industry. As automotive products are increasingly security-relevant and there are business models behind the products, companies need to conduct a threat analysis and risk assessment. Due to the connection of physical security functions to information technology, two different domains have to be considered in threat analyses and risk assessments of automotive products: physical security and IT security. However, the assessment of physical security and the assessment of IT security do not fit together, as significantly different assessments in both domains correspond to unequal vulnerability levels: In physical security, vulnerability can be analyzed by interplay of time between the intrusion time of an attacker and the reaction time of a defender. The quantitative basis for assessment is the interplay between protection, observation and intervention. In the field of IT security, vulnerability is assessed by the exploitability of system-inherent vulnerabilities and determined by scoring of threat scenario-describing parameters. A quantitative analysis of effectiveness is difficult to conduct in IT security because there is no objective mechanism for assessing the performance of security measures. A reproducible assessment is not possible.

Given the interfaces between hardware and software, successful IT scenarios can have an impact on safety functions and physical security mechanisms. From a product development perspective, this raises the question of a suitable metric for cross-domain risk assessment. In common standards and guidelines, such as ISO 26262, ISO/SAE 21434 or IEC 61508, the problem of merging safety metrics and IT security metrics in particular is described at an abstract level. However, solutions to enable a quantitative analysis are not presented. This paper deals with the possibilities and limitations of conducting a cross-domain risk assessment of physical threat scenarios and IT threat scenarios. A structured approach is developed, which is based on the methodological approach of threat analysis and risk assessment from ISO/SAE 21434. The focus lies on the alignment of metrics for vulnerability assessment, the determination of security levels for scenarios with cross-domain effects and the harmonization of the approach to threat analysis and risk assessment in both domains.

This paper demonstrates how a clearly defined mechanism to describe performance in a quantitative metric can be translated into consistent scores as part of a scoring metric. Lichte's vulnerability assessment, referred to in this paper as the Intervention Capability Metric (ICM), is used for the quantitative calculation of physical vulnerability. The Harnser metric is used for the scoring-based assessment. As part of a metric analysis, the Harnser metric is adapted in terms of the combination of assessment parameters and the rating scale so that the same vulnerability ratings can be generated as for the ICM. It is assumed that the ICM assessment corresponds to objective vulnerability levels. Examples are used to illustrate the degrees of freedom that exist in the alignment of the semi-quantitative Harnser metric and the quantitative ICM. This scientific work then examines the distortions that occur when using scoring-based assessments and how these can be mitigated. The Common Vulnerability Scoring System (CVSS) from the IT security domain is considered as an example. In particular, possibilities for reducing metrics-inherent distortions by means of log transformation are shown. In addition, the architectural and metric considerations of a barrier-based CVSS approach are discussed; options to reduce distortions within the barrier-based CVSS approach are presented.

Approaches to cross-domain risk assessment are here discussed. Ways and assumptions for harmonizing vulnerability and risk descriptions as well as vulnerability and risk assessments in both security domains are elaborated. The Harnser metric for assessing physical vulnerability and the CVSS base metric for assessing the exploitability of vulnerabilities are considered first and foremost. Both metrics are modified with the aim of achieving a comparable vulnerability classification despite different assessment bases. This harmonization is conducted in order to standardize the approach to vulnerability assessment as a building block of threat analysis and risk assessment in physical security and IT security. To this end, a normalization of the assessment parameters by a log transformation is proposed. In addition, the scale categories and the parameter values are adapted to each other. It is explained how the assessment scale of physical impacts and IT impacts can be normalized. The normalization of the impact scale aims to take into account the different scalability of impacts caused by physical attacks and impacts caused by IT attacks in one scale range.

Because an objective mechanism to describe performance is difficult to find in IT security, the CVSS metric cannot be adapted in such a way that the resulting vulnerability classifications correspond to objective vulnerability levels. For this reason, a security assessment of a Physical Impact on IT Vulnerability is not performed. In contrast to the CVSS metrics, the Harnser metric can be backed up with an objective performance mechanism and adapted to objective vulnerability levels. As a result, it is argued that a quantitative assessment of the impact of IT scenarios on physical scenarios is possible. To assess this cross-domain interaction, the IT Impact on Physical Vulnerability parameter is newly introduced. Experts estimate the impairment of physical security mechanisms by IT attacks. The impairment is accompanied by an increase in physical vulnerability. The increased physical vulnerability is then compared with the physical vulnerability without the influence of an IT scenario. Finally, the degree of this compromise is assessed using a rating scale. It is shown that vulnerability does not have to be made comparable in both domains in order to enable a cross-domain security assessment.

It is then examined how security levels for physical security and IT security can be determined. First, differences in the determination of an Automotive Safety Integrity Level (ASIL) according to ISO 26262 and in the determination of a Cybersecurity Assurance Level (CAL) according to ISO/SAE 21434 are worked out. Since threats in security are epistemic and there is hardly any evidence, it is argued that it is difficult to transfer the matrix for ASIL classification to physical security classification and IT security classification. Instead, it is explained how Physical Assurance Levels (PAL) and CAL can be determined in the same way by mapping the impact of an event against controllability after a successful threat scenario. The next step is to develop how the IT Impact on Physical Vulnerability can be taken into account to align PAL and CAL in the event of an interaction.

The approaches developed for vulnerability assessment and the metrics for determining security levels are then integrated into the procedure for threat analysis and risk assessment in accordance with ISO/SAE 21434. A probabilistically consistent linking of knowledge about the vulnerability to physical or IT attacks is conducted using Bayesian networks. In a further step, the threat analysis and risk assessment is extended by applying a methodology for the elicitation of expert knowledge in order to be able to take different expert statements into account. The proposed survey methodology combines elements from the Delphi method and Cooke's survey approach. Each expert states his or her subjective degree of conviction as to the extent to which a certain condition is correct for an assessment variable. In addition, their own confidence in the statement made is indicated between 0 % and 100 %. The subjective probabilities are weighted using the confidences. By integrating the survey and feeding in different expert statements, a possible spread of vulnerability results can be revealed. This can help to readjust the investment of resources in security measures until a defined level of risk acceptance is achieved.

This research work introduces a mixed-method or mixed-metric approach to the risk assessment of cyber-physical systems. The generic approach can be used for different use cases and applied repetitively in the sense of a continuous improvement process. It enables a quantitative analysis of physical scenarios that are influenced by IT scenarios. Overall, the proposed methods and metrics can be used in order to make better decisions regarding investment in security measures because the scoring-based vulnerability assessment in physical security is adapted to objective vulnerability levels using a quantitative metric. This results in the same vulnerability classifications from the assessments based on the Harnser metric and the ICM. Furthermore, it is shown how security metrics from the physical security and IT security domains can be merged using the log transformation. The findings may result in follow-up research to develop an IT security metric with an underlying, objective mechanism of describing performance. In addition, the approaches developed can be used to pursue the harmonization of the description and assessment of threats in the domains of physical security and IT security so that the metrics of all three risk contributions are structured in a risk-appropriate manner. In addition, the approaches and considerations presented in this work may serve to contribute to enabling the merging of metrics from functional safety and physical security or IT security.

Zusammenfassung

Die global wachsende Bedrohungslage hat weitreichende Folgen für die Standardisierung von Produktentwicklungsprozessen in der Automobilbranche. Da automobile Produkte zunehmend sicherheitsrelevant sind und hinter den Produkten Geschäftsmodelle stehen, ist in Unternehmen die Durchführung einer Bedrohungsanalyse und Risikobewertung erforderlich. Aufgrund der Anbindung von physischen Sicherheitsfunktionen an Informationstechnik sind in Bedrohungsanalysen und Risikobewertungen von automobilen Produkten zwei Domänen zu berücksichtigen, die physische Sicherheit und die IT-Sicherheit. Die Bewertung der physischen Sicherheit und die Bewertung der IT-Sicherheit passen aber nicht zusammen, da erheblich unterschiedliche Bewertungen in beiden Domänen zu ungleichen Vulnerabilitätsniveaus korrespondieren: In der physischen Sicherheit kann Vulnerabilität über das Zeitspiel zwischen der Eindringzeit eines Angreifers und der Reaktionszeit eines Verteidigers analysiert werden. Quantitative Bewertungsgrundlage ist das Zusammenspiel der Protektion, Observation und Intervention. In der IT-Sicherheit wird Vulnerabilität über die Ausbeutbarkeit von systeminhärenten Schwachstellen bewertet und über das Scoring von Bedrohungsszenario-beschreibenden Parametern bestimmt. Eine quantitative Analyse der Wirksamkeit ist in der IT-Sicherheit schwerlich durchführbar, weil ein objektiver Wirkmechanismus zur Bewertung der Effektivität von Sicherheitsmaßnahmen fehlt. Eine reproduzierbare Bewertung ist nicht möglich.

Erfolgreiche IT-Szenarien können angesichts der Schnittstellen zwischen Hardware und Software eine Auswirkung auf Safety-Funktionen und physische Sicherungsmechanismen haben. Deswegen wird aus der Sicht der Produktentwicklung die Frage nach einer geeigneten Metrik zur domänenübergreifenden Risikobewertung aufgeworfen. In gängigen Standards und Richtlinien, wie z. B. ISO 26262, ISO/SAE 21434 oder IEC 61508, wird das Problem bei der Zusammenführung von insbesondere Safety-Metriken und IT-Security-Metriken auf einer abstrakten Ebene beschrieben. Lösungsansätze zur Ermöglichung einer quantitativen Analyse werden dagegen nicht aufgezeigt. Die vorliegende Arbeit beschäftigt sich mit den Möglichkeiten und Grenzen in der Durchführung einer domänenübergreifenden Risikobewertung von physischen Bedrohungsszenarien und IT-Bedrohungsszenarien. Es wird eine strukturierte Vorgehensweise entwickelt, welche sich auf den methodischen Ansatz der Bedrohungsanalyse und Risikobewertung aus der ISO/SAE 21434 stützt. Im Fokus stehen die Angleichung von Metriken zur Vulnerabilitätsbewertung, die Bestimmung von Sicherheitslevels für Szenarien mit domänenübergreifenden Auswirkungen sowie die Harmonisierung der Vorgehensweise zur Bedrohungsanalyse und Risikobewertung in beiden Domänen.

In dieser Arbeit wird dargelegt, wie sich ein klar definierter Wirkmechanismus in einer quantitativen Metrik in konsistente Scores als Teil einer Scoring-Metrik überführen lässt. Die Lichte'sche Vulnerabilitätsbewertung, in dieser Arbeit als Intervention Capability Metric (ICM) bezeichnet, wird für die quantitative Berechnung der physischen Vulnerabilität verwendet. Für die Scoring-basierte Bewertung wird die Harnser-Metrik benutzt. Im Rahmen einer metrischen Analyse wird die Harnser-Metrik hinsichtlich der Kombination der Bewertungsparameter und der Bewertungsskala so angepasst, dass gleiche Vulnerabilitätseinstufungen wie bei der ICM erzeugt werden können. Es wird davon ausgegangen, dass die ICM-Bewertung objektiven Vulnerabilitätsniveaus entspricht. An Beispielen wird beleuchtet, welche Freiheitsgrade in der Angleichung der semi-quantitativen Harnser-Metrik und der quantitativen ICM bestehen.

Daraufhin wird untersucht, welche Verwerfungen bei der Anwendung Scoring-basierter Bewertungen auftreten und wie diese gemindert werden können. Beispielhaft wird das Common Vulnerability Scoring System (CVSS) aus der IT-Security-Domäne betrachtet. Insbesondere werden Möglichkeiten zur Reduktion von Metrik-inhärenten Verwerfungen mittels der log-Transformation aufgezeigt. Darüber hinaus werden die architekturellen und metrischen Überlegungen eines Barriere-basierten CVSS-Ansatzes diskutiert. In dieser Arbeit werden Optionen aufgezeigt, Verwerfungen innerhalb des Barriere-basierten CVSS-Ansatzes zu reduzieren.

Im Anschluss daran werden Lösungsansätze zur domänenübergreifenden Risikobewertung diskutiert. Wege und Annahmen zur Angleichung der Vulnerabilitäts- und Risikobeschreibungen sowie Vulnerabilitäts- und Risikobewertungen in beiden Security-Domänen werden herausgearbeitet. Die Harnser-Metrik zur Bewertung physischer Vulnerabilität und die CVSS-Basismetrik zur Bewertung der Ausbeutbarkeit von Schwachstellen werden hierbei vordergründig betrachtet. Beide Metriken werden mit dem Ziel verändert, trotz unterschiedlicher Bewertungsgrundlagen eine vergleichbare Einstufung der Vulnerabilität vorzunehmen. Diese Angleichung wird vorgenommen, um die Vorgehensweise zur Vulnerabilitätsbewertung als Baustein der Bedrohungsanalyse und Risikobewertung in der physischen Security und in der IT-Security zu vereinheitlichen. Zu diesem Zweck wird eine Normalisierung der Bewertungsparameter über eine log-Transformation vorgeschlagen. Darüber hinaus werden die Skalenkategorien und die Parameterausprägungen zueinander angepasst. Es wird erklärt, wie die Bewertungsskala der physischen Auswirkungen und der IT-Auswirkungen normalisiert werden kann. Die Normalisierung der Auswirkungsskala zielt darauf ab, die unterschiedliche Skalierbarkeit von Auswirkungen durch physische Angriffe und von Auswirkungen durch IT-Angriffe in einer Skala zu berücksichtigen.

Weil in der IT-Security ein objektiver Wirkmechanismus schwerlich zu finden ist, kann die CVSS-Metrik nicht in der Form angepasst werden, dass die resultierenden Vulnerabilitätseinstufungen objektiven Vulnerabilitätslevels entsprechen. Aus diesem Grund wird auf eine Sicherheitsbewertung eines Physical Impacts on IT Vulnerability verzichtet. Im Gegensatz zu den CVSS-Metriken kann die Harnser-Metrik mit einem objektiven Wirkmechanismus hinterlegt und an objektive Vulnerabilitätsniveaus angepasst werden. Demzufolge wird argumentiert, dass eine quantitative Bewertung der Auswirkungen von IT-Szenarien auf physische Szenarien möglich ist. Zur Bewertung dieser domänenübergreifenden Wechselwirkung wird die Größe IT Impact on Physical Vulnerability neu eingeführt. Experten schätzen hierbei die Beeinträchtigung physischer Sicherungsmechanismen durch IT-Angriffe ab. Mit der Beeinträchtigung geht eine Erhöhung der physischen Vulnerabilität einher. Die erhöhte physische Vulnerabilität wird daraufhin mit der physischen Vulnerabilität ohne Einfluss eines IT-Szenarios verglichen. Über eine Bewertungsskala wird abschließend der Grad dieser Kompromittierung bewertet. Es wird dargelegt, dass Vulnerabilität nicht in beiden Domänen vergleichbar gemacht werden muss, um eine domänenübergreifende Sicherheitsbewertung zu ermöglichen.

Daraufhin wird untersucht, wie Sicherheitslevels für die physische Sicherheit und für die IT-Sicherheit bestimmt werden können. Zunächst werden Unterschiede in der Bestimmung eines Automotive Safety Integrity Levels (ASIL) gem. ISO 26262 und in der Bestimmung eines Cybersecurity Assurance Levels (CAL) gem. ISO/SAE 21434 herausgearbeitet. Da Bedrohungen in der Security epistemisch sind und kaum Evidenz vorliegt, wird begründet, dass eine Übertragung der Matrix zur ASIL-Einstufung auf die physische Sicherheitseinstufung und IT-Sicherheitseinstufung schwierig umsetzbar ist. Stattdessen wird dargelegt, wie sich Physical Assurance Levels (PAL) und CAL in gleicher Weise über die Zuordnung der Auswirkungen eines Ereignisses gegen die Kontrollierbarkeit nach einem erfolgreichen Bedrohungsszenario ermitteln lassen können. Als nächstes wird entwickelt, wie der IT Impact on Physical Vulnerability berücksichtigt werden kann, um PAL und CAL im Falle einer Wechselwirkung aufeinander abzustimmen.

Die erarbeiteten Ansätze zur Vulnerabilitätsbewertung und die Metriken zur Bestimmung von Sicherheitslevels werden dann in die Vorgehensweise zur Bedrohungsanalyse und Risikobewertung nach ISO/SAE 21434 integriert. Eine probabilistisch konsistente Verknüpfung des Wissens über die Angreifbarkeit auf physischem oder IT-Wege wird über die Methode Bayes'scher Netze durchgeführt. Um unterschiedliche Expertenaussagen berücksichtigen zu können, wird in einem weiteren Schritt die Bedrohungsanalyse und Risikobewertung durch die Anwendung einer Methodik zur Erhebung von Expertenwissen erweitert. Die vorgeschlagene Erhebungsmethodik verknüpft Elemente aus der Delphi-Methode und dem Cooke'schen Erhebungsansatz. Jeder Experte gibt für eine Bewertungsgröße jeweils seinen subjektiven Grad der Überzeugung an, inwieweit ein bestimmter Zustand zutreffend ist. Zusätzlich wird das eigene Vertrauen in die gemachte Aussage (Konfidenz) zwischen 0 % und 100 % angegeben. Die subjektiven Wahrscheinlichkeiten werden über die Konfidenzen gewichtet. Durch die Integration der Erhebung und Einspeisung von unterschiedlichen Expertenaussagen kann eine mögliche Spreizung von Vulnerabilitätsergebnissen aufgedeckt werden. Das kann dazu beitragen, die Investition von Ressourcen in Sicherheitsmaßnahmen nachzujustieren, bis eine definierte Risikoakzeptanz erreicht wird.

In dieser Forschungsarbeit wird insgesamt ein Mixed-Methods- bzw. ein Mixed-Metric-Ansatz zur Risikobewertung von cyberphysischen Systemen eingeführt. Der generische Ansatz kann für unterschiedliche Anwendungsfälle verwendet werden, im Sinne eines kontinuierlichen Verbesserungsprozesses repetitiv Anwendung finden und eine quantitative Analyse physischer Szenarien ermöglichen, die durch IT-Szenarien beeinflusst werden. Insgesamt können mit den vorgeschlagenen Methoden und Metriken bessere Entscheidungen bezüglich der Investition in Sicherheitsmaßnahmen getroffen werden, weil die Scoring-basierte Vulnerabilitätsbewertung in der physischen Sicherheit mittels einer quantitativen Metrik an objektive Vulnerabilitätsniveaus angepasst wird. Dadurch resultieren aus den Bewertungen auf Basis der Harnser-Metrik und der ICM gleiche Vulnerabilitätseinstufungen. Ferner wird aufgezeigt, wie mittels der log-Transformation Sicherheitsmetriken aus den Domänen Physical Security und IT-Security zusammengeführt werden können.

Die Ergebnisse dieser Arbeit können im Rahmen einer Anschlussforschung genutzt werden, um eine IT-Security-Metrik mit einem hinterlegten, objektiven Wirkmechanismus zu entwickeln. Darüber hinaus können die entwickelten Ansäte genutzt werden, um die Angleichung der Beschreibung und der Bewertung von Bedrohungen in den Domänen physische Sicherheit und IT-Sicherheit zu verfolgen, sodass die Metriken aller drei Risikobeiträge risikogerecht aufgebaut werden. Außerdem können die in dieser Arbeit vorgestellten Ansätze und Überlegungen verwendet werden, um einen Beitrag zur Ermöglichung einer Zusammenführung von Metriken aus der Functional Safety und Physical Security oder IT Security zu leisten.

Table of Contents

List of Abbreviations

Abbreviation in continuous text	Meaning
A	Availability
AADL	Architecture Analysis & Design Language
ABG	General building permit
AC	Attack Complexity
AC-S	AC Score
ADL	Architecture Description Languages
AG	Attack Graph
AGA	Attack Graph Analysis
ALKS	Automated Lane Keeping Systems
ASIL	Automotive Safety Integrity Level
ASSESS	Analytic System and Software for Assessing Safeguards and Security
ASVS	Application Security Verification Standard
AT	Attack Tree
ATA	Attack Tree Analysis
AV	Attack Vector
AV-S	AV Score
BAN	Body Area Networks
BPMN	Business Process Model and Notation
BSI	Federal Office for Information Security
C	Confidentiality
CAL	Cybersecurity Assurance Level
CC	Common Criteria
CCC	Car Connectivity Consortium
CCRA	Common Criteria Recognition Arrangements
CPS	Cyber-Physical System
CPTARA	Cyber-Physical Threat Analysis and Risk Assessment
CSMS	Cybersecurity management systems
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D	Detection
DES	Data Encryption Standard
DiD	Defense in Depth
DIN	German Institute for Standardization
DKS	Digital Key Standard
EAL	Assessment Assurance Levels
EFSA	European Food Safety Authority
EVITA	E-safety Vehicle Intrusion Protected Applications
FAIR	Factor Analysis of Information Risk
FESEM	Forcible Entry Safeguards Effectiveness Model
FMEA	Failure mode and effects analysis
FT	Fault Tree
FTA	Fault Tree Analysis
HARA	Hazard Analysis and Risk Assessment
I	Integrity; only in the context of asset valuation
I	Intervention
IAM	Identity & Access Management
ICM	Intervention Capability Metric
IDS	International Data Spaces
IEC	International Electrotechnical Commission
IoT	Internet of Things
I-S	Intervention score
ISEM	Insider Safeguard Effectiveness Model

ISO	International Organization for Standardization
IT	Information technology
ITIPV	IT Impact on Physical Vulnerability
ITU	International Telecommunication Union
K	Know-How
KBA	Federal Motor Transport Authority
KRITS	Critical infrastructures
L	Likely
LIM	Lower Interval Limit
LoE	Likelihood of Exploitability
LoEmod	Likelihood of Exploitability modified
Log	logarithmized
LoV	Likelihood of Vulnerability
MAS	Mobile Access System
MDS	Mobility Data Space
MI	Mean of Interval
MMT	Multi-Modeling Techniques
n.a./na	not applicable
NATO S&T	North Atlantic Treaty Organization Science and Technology
NIST	National Institute for Standardization
NVD	National Vulnerability Database
O	Observation
OEM	Original Equipment Manufacturer
OLU	Onboard Logic Unit
O-S	Observation Score
OSI	Open Systems Interconnection
OSS	Open Security Standards
OSSO	OSS Standard Offline
OWASP	Open Web Application Security Project
P	Protection
P2P	Peer to peer
PAL	Physical Security Assurance Level
PDDL	Planning Domain Definition Language
PiD	Protection in Depth
PIITV	Physical Impact on IT Vulnerability
PL	Privilege Level
PR	Privileges Required
PR*	Size composed of PR and UI
PR*-S	PR* Score
PRISM	Performance Risk-based Integrated Security Methodology
P-S	Protection Score
QM	Quality management/quality managed
R	Resources
RAND	Research and Development Corporation
RPN	Risk Priority Number
RSS	Radio Standard Specification
SAE	Society of Automotive Engineers
SAFE	Safeguards Automated Facility Assessment
SAHARA	Security-Aware Hazard and Risk Analysis Method
SAVI	System Analysis of Vulnerability to Intrusion
SC	System Check
SecL	Security level
SHELF	Sheffield Elicitation Framework
SM	Security Metric
SNAP	Safeguards Network Analysis Procedure
STRIDE	Acronym for: S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege

Sum	Summarized
SUMS	Software update management systems
T	Threat
TARA	Threat Analysis and Risk Assessment
TR	Technical Report
MOT	Technical Inspection Association
UI	User Interaction
UIM	Upper Interval Limit
UL	Unlikely
UML	Unified Modeling Language
UNECE	United Nations Economic Commission for Europe
V	Vulnerability
VL	Very Likely
VUL	Very Unlikely
VVUL	Very very unlikely
WP	Working Party

List of Figures

List of Tables

1 Introduction

Over the last ten years, the use of cyber-physical systems (CPS) has increased worldwide. According to the forecast in Lee et al. (2017), CPS will play an increasing role in industry and everyday life in the 21st century. According to a study commissioned by the Federal Ministry for Economic Affairs and Energy, which was conducted as part of the accompanying research for the AUTONOMIK technology program for Industry 4.0 in 2015, the use of CPS is accompanied by a change in entrepreneurial value creation and an increase in application potential (BMWi, 2015). Neugebauer (2018) argues that CPS even heralds a disruptive paradigm shift compared to purely physical systems, in which the "efficiency gain through flexibilization [...] and better use of resources through the self-optimizing automation of processes is in the foreground" (Neugebauer, 2018, p. 198). The increase in the number and applications of CPS can be observed worldwide. The mobility sector stands out in particular (Geisberger & Broy, 2012, pp. 32-43; Möller et al., 2019, pp. 171-172). This is partly due to the concentrated efforts of original equipment manufacturers (OEMs) and suppliers to successfully implement the structural change to digital business models and digital value creation driven by digitalization (Macher et al., 2020a; BSI Branchenlagebild Automotive, 2022).

Customer needs, individualization and networking opportunities are key drivers of digitalization (Bormann et al., 2018). The global coronavirus pandemic can also be seen as an accelerator of digital change (Puls et al., 2021). As part of the transformation process, companies are faced with the challenge of rethinking and realigning historically evolved business model structures. In addition, product development processes must be set up in accordance with new guidelines and standards. This is necessary in order to remain competitive and obtain approval for CPS on the automotive market (Möller et al., 2019, pp. 29, 34-37, 60; ISF Munich, 2021, pp. 7, 51). An important basis for the implementation of the digital transformation is the use of information technology and its technological possibilities for storing, processing and transmitting data (Hoffmeister, 2017, p. 41). The use of CPS plays a key role in this (Möller et al., 2019, pp. xii-xiii). The latest developments pursue the approach of extending the functionality of a conventional physical vehicle key by using a digital certificate in new use cases (Möller et al., 2019, pp. 439-440, 443-447). A digital certificate is a digital key that is linked to a digital user identity, a product, user rights and periods of use (Grimm, 2019, p. 22).

In addition to locking or unlocking a vehicle, e.g. via a mobile device, other (data-based) services can be offered, such as sharing, payment functions, navigation or delivery (Möller et al., 2019, pp. 220-233, 439). Mobile access systems (MAS) are a relatively new type of digitized access system. As CPS, they combine the physical domain and the IT domain, i.e. the mechanical locking system is extended by software and cloud components (Schwerdtfeger, 2018, pp. 29-34). The diverse application possibilities of CPS, the resulting potential for threats (Wurm, 2022, p. 32) and the globally increasing threat situation (Hubbard et al., 2016, pp. 8-11) are the motivation for conducting a risk assessment of MAS in specific use cases (see also: Möller et al., 2019, pp. 266, 271, 317, 339, 350). Operators are keen to protect their products against attacks, as they are increasingly relevant to security and the use cases are based on business models (Becker et al., 2019; Macher et al., 2020a). MAS must be designed as securely as possible using limited resources so that risks can be mitigated to a level that is acceptable to all stakeholders (Sowa, 2011, p. 23). In this context, ethical hackers and security researchers are working to uncover vulnerabilities in specific applications, see e.g. Samcurry.net (2023).

"In several academic attacks on vehicles, researchers have [already] demonstrated that remote control of various vehicle functions via radio interfaces is feasible" (Wurm, 2022, p. 35). On the one hand, cooperation between industry and security research helps to make product suppliers aware of security vulnerabilities at an early stage, before these vulnerabilities can be exploited by maliciously motivated attackers. On the other hand, security research supports product development by developing methods and metrics for security assessment and transferring these into practice to answer security questions (Sifo.de, 2023). A classification and delimitation of the risks on which this work focuses is shown in Figure 1. The gray ellipses in this figure mark the thematic focus of this research work. This thesis uses the terms IT security and cybersecurity synonymously. The terms refer to the state in which functions and goods worthy of protection are adequately protected against threat scenarios for road vehicles, their functions and (electronic) systems.

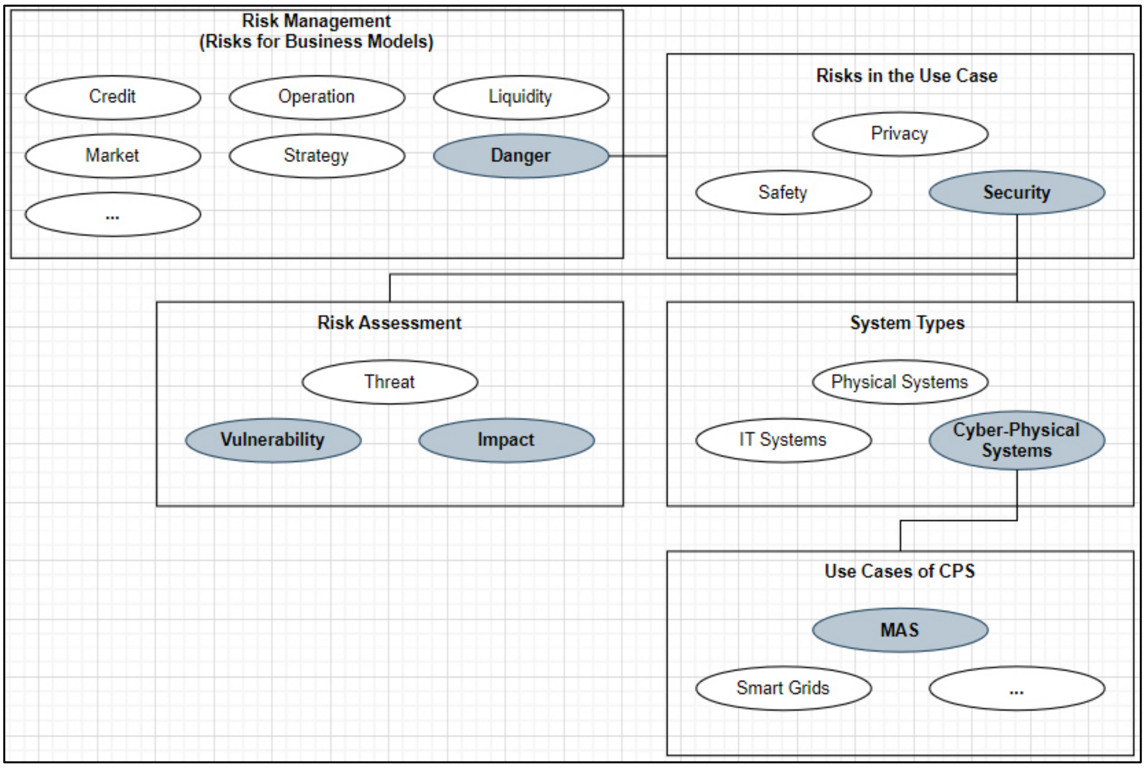


Figure 1: Contextual classification of the risk assessment of MAS.
Source: Own Figure based on Garcia (2005, p. 3).

1.1 Problem Definition

Product design processes generally run via functional specifications in which design requirements are defined. Guidelines help to concretize technical-functional, safety and security requirements and to make the complexity associated with the use of CPS manageable (Möller et al., 2019, p. 10) (Schwerdtfeger, 2018, p. 35; Macher et al., 2020a). They define what needs to be done by product development and quality management in order to meet certain requirements. On the one hand, this is necessary in order to obtain market approval. In the USA, this includes product testing in accordance with the requirement specifications listed in 47 CFR Part 15.247 (U.S. Government Publishing Office, 2010) and RSS 247 (Government of Canada, 2017). On the other hand, compliance with guidelines may be required by customers and stakeholders. Compliance is also a seal of quality for a provider and can create competitive advantages over the competition (BSI, 2016). Security is a quality feature that can be a unique selling point for providers (Wurm, 2022, p. 37).

Product developers can also use guidelines to take safety, security and quality criteria into account early on in the product design process. For example, the Tier 1 automotive supplier WITTE Automotive is certified in accordance with IATF 16949 (IATF, 2016) and ISO 9001 (DIN e.V., 2015b) for the development and manufacture of locking systems, with regular audits conducted to check compliance. The digital satellite of the WITTE Automotive Group, WITTE Digital, has developed a retrofit solution called flinkey for after-market vehicles to enable the flexible sharing of resources through the use of a digital key (Flinkey.de, 2021). Until now, the testing of the physical product has largely been based on safety guidelines, such as IEC 62368 (IEC, 2021). However, flinkey is a cyber-physical product that has firmware, software and cloud components in addition to hardware.

The development of cyber-physical products is accompanied by the challenge of bringing together functional safety features, physical security features and IT security features (Lyu et al., 2020; Möller et al., 2019, pp. 304-305). The features in the functional safety, physical safety and IT security domains are assessed differently, e.g. using various quantitative, semi-quantitative and qualitative criteria. The assessment criteria and procedures are therefore not compatible (Cert, 2022; Kriaa et al., 2015). The consideration of functional safety requirements, which are not considered in this research work, as well as security requirements and the balancing of conflicting requirements represent a major challenge for OEMs and suppliers in product development (Möller et al., 2019, pp. 269, 308). "Weighing up and sounding out how much security is just sufficient for the reliability of the product, but is still within the time and financial framework, is a balancing act", emphasizes Wurm (2022, p. 37).

The trade-off becomes more complicated when interactions between security functions can occur. "[The] stringent real-time requirements and the scarce memory sizes and bandwidths of embedded systems [are] often at odds with the resource requirements of security functions", explains Wurm (2022, p. 38). However, there is currently no formal security model for CPS that deals with security in a uniform framework that addresses hardware threats, network threats, physical threats and software threats (Möller et al., 2019, p. 318). Merging the domains of physical security and IT security requires new approaches to cross-domain (here: cyber-physical) assessment.[1] In order to be able to implement cyber-physical requirements in the development process, the question of a suitable metric for cross-domain security assessment arises (Macher et al., 2020a; see the classification in Figure 2).

[1] Initial approaches are being discussed in Technical Committee 512 "Safety and Security" of the Association of German Engineers (VDI), which is chaired by Prof. Dr. Kai-Dietrich Prof. Wolf with extensive industry participation from the disciplines of automotive, aviation security, maritime security, etc. (Sicherungssysteme, 2021).

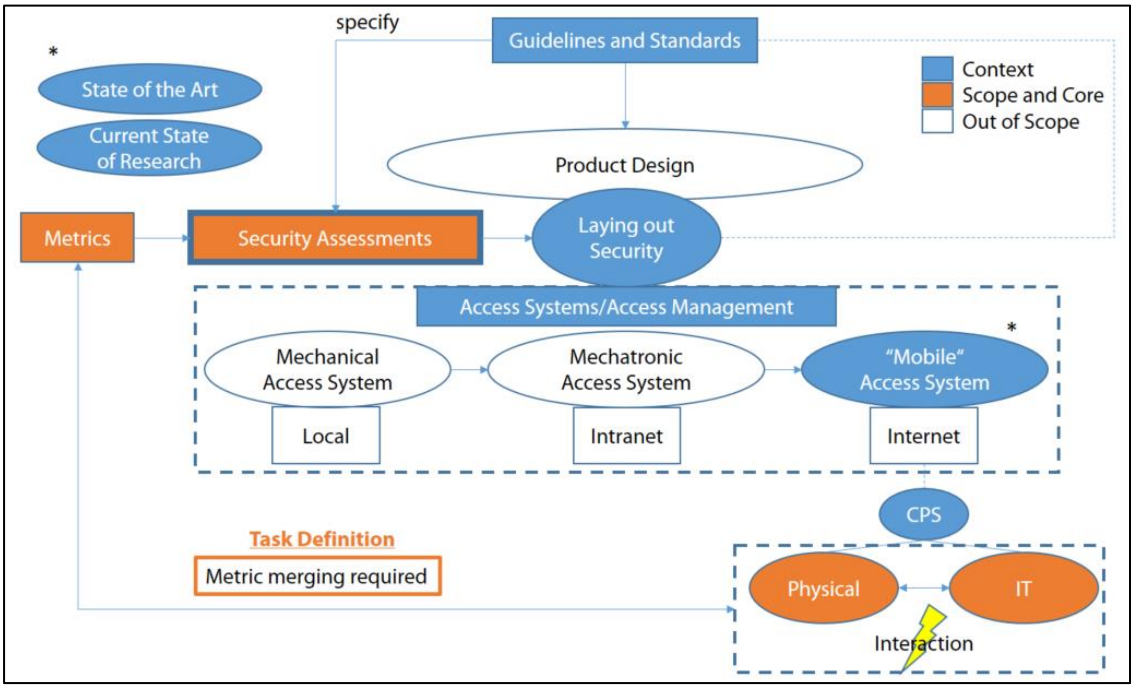


Figure 2: Classification of the research work.
Source: Own Figure.

In existing standards, such as IEC TR 63069 (IEC, 2019) or DIN ISO/TR 22100 (DIN e.V., 2014), the problem of metric alignment of quantitative and qualitative or semi-quantitative approaches is described in abstract terms. Neither IEC TR 63069 nor DIN ISO TR 22100 describe a solution for metric alignment or merging of safety and security metrics. This is a problem from the product developer's point of view because the necessary procedure for risk assessment, which is usually provided by specifications from guidelines and standards and implemented in product development processes, is insufficient for the cross-domain risk assessment in the present case (Macher et al., 2020a). In this context, specifications would help to set clear guidelines for product development.

1.2 Challenges

In the case of cyber-physical structures containing physical components and IT components, two paradigms come together, each of which has been incorporated into different, domain-specific approaches to risk assessment in the two domains (Macher et al., 2020a). In Macher et al. (2020a), the hurdles in product development taking into account security aspects from two domains are named as follows: "A significant barrier [for conducting cross-domain risk assessments] comes from fundamentally different safety and security viewpoints, engineering approaches, and nomenclatures" (Macher et al., 2020a). Quantitative metrics are used for risk assessment in both physical security and functional safety. In physical security, for example, Lichte et al. (2016) use the probability that an attacker reaches an asset[2] faster than the defender reaches the attacker as an assessment criterion for vulnerability. When analyzing the interplay between the intrusion time of an attacker and the reaction time of a defender, there is a clearly defined mechanism of performance consisting of protection, observation and intervention.

In functional safety, the assessment standard (especially for hardware) is the failure rate of a system component over a specific period of time (Lichte et al., 2017; Wurm, 2022, p. 70). The metrics underlying the disciplines of physical security and functional safety are based on a time-related probability that relates to physical processes and states (Macher et al., 2020a). In IT security, it is common to use scores for assessments, as there is no underlying time metric and no objective mechanism for assessing the performance of measures (Yee, 2013, p. 8; Jacobs et al., 2019; Pohlmann, 2015). Newsome (2013) justifies the use of scoring systems as follows: "[...] If [you] were not confident enough [and] when dealing with [...] complicated events, the threats are rarely identified with certainty, so [...] [it] Is likely to use words like possibly in this context" (Newsome, 2013, p. 102). Scoring offers users an advantage over complicated calculations if it is more intuitive and easier to assess risks. This assumes that real risks can also be mapped with scorings (Gigerenzer, 2014, p. 140).

Common IT security metrics are traditionally qualitative and semi-quantitative. They do not map the processes as in physical security or functional safety. The principles in IT security differ from those in physical security: in IT, both physical access points (e.g. hardware in server rooms) and digital access points (e.g. network nodes) can be used to gain access to a data asset (Wheeler, 2011, p. 18). An IT attacker can exploit known vulnerabilities. However, vulnerabilities that are unknown to an operator can also be exploited to achieve a compromise, so-called zero days (e.g. implementation errors) (BSI Glossary, 2022). In physical security, an attacker is guided along a known path, which is determined by the placement of barriers and their openings (Garcia, 2005, p. 39).

Furthermore, the use of probabilities in IT security is based on a different interpretation than in physical security or functional safety. In IT, probability means, for example, the possibility that a vulnerability in a system can be exploited (Braband, 2019), or that, for example, 90 % of all publicly known vulnerabilities can be identified and closed (Jones, 2007). In physical security, on the other hand, probability means that an attacker needs 30 seconds to overcome a barrier in 65 % of cases, for example (Lichte et al., 2019). In functional safety, probability refers to the failure of a component within a defined time window (Zio, 2007, p. 50). In all three cases, these are probabilities. However, these probabilities do not fit together correctly.

[2] According to ISO/SAE 21434, an asset is "[an] object that has value, or contributes to value" (ISO/SAE, 2021b, p. 1).

In physical security, the risk is described on the basis of the impact, threat and vulnerability, and assessed through the interaction of protection, observation and intervention (Lichte et al., 2016). Scenarios are considered that have not yet occurred or for which hardly any historical data is available (Lichte et al., 2017). The lack of historical data is due to the fact that worst-case scenarios, such as those considered in physical security, have rarely or never occurred in the past. For this reason, statistical estimates and therefore the specification of absolute probability values are not possible. Determining the probability of a threat is difficult, which is why threats are grouped into scenarios in the threat analysis in which certain combinations of knowledge, tools and attacker type are meaningful and consistent. Such scenarios must be isolated by a risk analyst so that they can be assigned probabilities of occurrence with the help of experts (Witte et al., 2020). The modeling of scenario probabilities and the assessment of threat contributions are not considered in detail in this research work.

The quantitative assessment of security functions in the event of an attack (the system is exposed to a threat) enables cost-benefit optimization with regard to the use of security measures against specific threat scenarios (Lichte et al., 2019). This assumption can be justified by the argumentation of Krisper (2021):

> One big problem regarding the measurement of performance is that there could be years until some risk eventually occurs - hence there is no immediate feedback, which could be measured easily. [...] Immediate feedback is an absolute must for being able to improve. (Krisper, 2021).

A prerequisite for modeling and assessing a security system in the event of an attack is the assumption that threat components are disjoint from vulnerability components and impact components. In reality, this idealization is not given, as threat components can also contain vulnerability components and impact components (Harnser, 2010, B5, p. 57). The attractiveness of a goal, for example, can depend on the potential impact. However, vulnerability also has threat components because it depends on threat scenarios. In this ideal case, strict independence is assumed between the events of threat, vulnerability and impact.

Physical vulnerability can be assessed at a very specific, impact-related level (Harnser, 2010, B4, p. 47). On the one hand, a quantitative assessment of physical vulnerability is possible, e.g. by using the vulnerability metric according to Lichte et al. (2016). For the quantitative vulnerability assessment according to Lichte et al. (2016), the term Intervention Capability Metric (ICM) is introduced in this paper based on Garcia (2005). Regarding the choice of suitable security technologies, Garcia (2005) explains: "Selection of the appropriate technologies depends on threat capability and motivation" (Garcia, 2005, p. 152). And further: "For an immediate response, neutralization capability and the probability of communication are key performance measures" (Garcia, 2005, p. 250). The ICM is used to assess whether an attacker needs more time to overcome the barriers to the asset than a defender needs to successfully intervene. Uncertainties about the security functions of a physical system can be taken into account in the form of density functions for protection, observation and intervention (Lichte et al., 2021). The interaction of the components of the physical mechanism of performance is typically set up for a single threat. However, the mean values and standard deviations of a density function based on a normal distribution, for example, can also refer to a set of several threats. In this context, the weakest path of the security system determines the physical vulnerability of the system under consideration, because it is assumed that the path of an attacker is uncertain (Lichte et al., 2016).

On the other hand, there are also scoring systems in physical security. One example of this is the Harnser metric from the Performance Risk-based Integrated Security Methodology

(PRISM) according to Harnser (2010). In the Harnser metric, the parameters of protection, detection and intervention are rated by experts with values between "1" (low) and "5" (high). The designation of the assessment parameters in Harnser (2010) is different from that in Lichte et al. (2016). In the Harnser metric, the term "detection" is used for the second assessment parameter. In Lichte et al. (2016), the term "observation" is used. According to the ICM by Lichte et al. (2016), detection is an assessment parameter that is made up of observation and protection components, i.e. it is a composite event (Lichte et al., 2016). Consequently, protection would be included twice in the vulnerability assessment according to Harnser: Once via the assessment of protection and once via assessment of detection. In principle, it must be questioned whether experts are in a position to directly assess assessment variables that are made up of several parameters. Vulnerability, for example, can hardly be assessed directly by experts without a vulnerability metric. Instead, it is necessary to assess the vulnerability components according to the vulnerability metric used, so that a vulnerability value results as the output of the vulnerability metric. It therefore makes more sense to rename the assessment parameter "Detection" to "Observation".

The scores for protection, detection and intervention are then added together in the Harnser metric to create a vulnerability score. This leads to deviations compared to the ICM: for example, if the protection is "3" (moderate design), the detection is "1" (minimum design) and the intervention is "5" (maximum design), then the vulnerability assessment according to Harnser (2010) is in the medium range (value "9"). According to the ICM, the system is highly vulnerable under these conditions if the following assumptions are made (Lichte et al., 2016)[3] :

- The combination of protection and observation at barriers is necessary because an attacker is always able to break through a barrier if he has an infinite amount of time without being detected.
- The detection of an attack is only possible if the protection is sufficient to prevent a breakthrough until detection.
- After detection, an attack can only be stopped if the remaining protection along the remaining attack path lasts long enough to prevent the attacker from reaching the asset until the intervention is completed.

The Harnser metric does not say how detection score "1" relates to detection score "5" (is score "5" five times as good as score "1"?). The metric does not provide any information about this because the scores are only ordinal values, i.e. values without absolute reference to size. Vulnerability score values for Harnser below "3" or intermediate values are undefined, e.g. scores between "4" and "5". A similar phenomenon can also be seen with other semi-quantitative metrics. One example of this is the Failure Mode and Effects Analysis (FMEA) (Braband, 2003; Braband, 2004): The three parameters occurrence, significance and detection are scored between "1" (low) and "10" (high). The scores are then multiplied together. The product of occurrence, significance and detection is the so-called Risk Priority Number (RPN). The highest achievable value is (10 x 10 x 10 =) "1000" (maximum risk), while the next lowest value is "900" (10 x 10 x 9). If the minimum score is considered instead of the maximum score, it is noticeable that the risk scales differently for small scores than for large scores. The lowest risk here is (1 x 1 x 1 =) "1", the next highest (1 x 1 x 2 =) "2".

The distance between these two scores appears to be "1", whereas the distance between the two highest scores is "100". However, as this is a semi-quantitative approach with an ordinal scale, there is no reference point that would allow proportionality. FMEA scoring suggests that the risk scales differently for high scores than for lower scores (Braband, 2004). Whether this

[3] Taking into account the three aforementioned assumptions for ICM, a certain interplay of protection, observation and intervention is always required in order to achieve a protective effect.

actually corresponds to real conditions must be critically questioned (Krisper, 2021). In addition, the FMEA cannot achieve the full range of possible result values between "1" and "1000". The result space is restricted by the given parameter combinations and the underlying calculation rule. Braband (2003) summarizes the systemic weaknesses of FMEA as follows:

- Occurrence, meaning and discovery are characteristics on an ordinal scale, which is why multiplication is not mathematically defined.
- Similar risks should be assigned the same RPN. This cannot be guaranteed with the FMEA.
- Risks with the same RPN are not accepted to the same extent.

Braband (2012) makes the following three demands on a risk scale for determining the RPN:

> Rational scaling: The scaling of the assessment 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 lower than the risk for scenario j, the RPN for scenario i must be smaller 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, pp. 216-217).

On the one hand, the Harnser metric does not differentiate between individual barriers, as the ICM does. Secondly, protection, detection (or now observation) and intervention are interpreted as equivalent. This is not the case, as the following explanations show: Assume that protection is ideally 100 % and that there is no observation and no intervention[4] . This would mean that every attacker can be stopped. In this case, the system under consideration is 0 % vulnerable according to the ICM. 100 % protection corresponds to an ideal barrier that does not require any observation or intervention. With only a Harnser protection score of "5" (maximum protection)[5] , it would be assumed that the vulnerability is in the mid-range. If there is no protection and no intervention[6] , but only 100 % observation, then this constellation will lead to maximum vulnerability according to the ICM, because every attacker is recognized but not stopped. In such a case, the Harnser score sum (0 + 5 + 0 =) "5" attests to a level of security that does not exist. A 100 % intervention without protection and without observation is nonsensical, as all attackers can theoretically be stopped. However, they are not recognized as such beforehand.

The best possible protection can stand alone to theoretically achieve 0 % vulnerability. Observation and intervention, on the other hand, cannot. If there is no protection but, for example, 100 % observation and 100 % intervention in combination, then the system is 0 % vulnerable, as in the case of "only 100 % protection". Observation and intervention together could therefore be effective without protection components. However, the Harnser score of "10" (0 + 5 + 5) is again in the middle of the range. Further problems with the use of semi-quantitative approaches compared to quantitative approaches are highlighted, for example, in Krisper (2021), Braband (2004), Braband (2008), Braband (2009), Braband (2016), Termin et al. (2021), Ahmed (2019) and Hubbard et al. (2016, pp. 85-95). Krisper (2021) discusses a total of 24 problems with the use of semi-quantitative metrics compared to quantitative approaches, including "ordinal scales, semi-quantitative arithmetics, range compression, risk inversion, ambiguity, and neglection of uncertainty" (see Figure 3).

[4] Such an extreme case is rather unrealistic because zero observation means that any (heavy, loud, conspicuous) means of attack are possible. The examples given are intended to show that protection, observation and intervention are not equivalent.

[5] Mentally, observation and intervention would each have a score of "0".

[6] In this case, protection and intervention would have a score of "0".

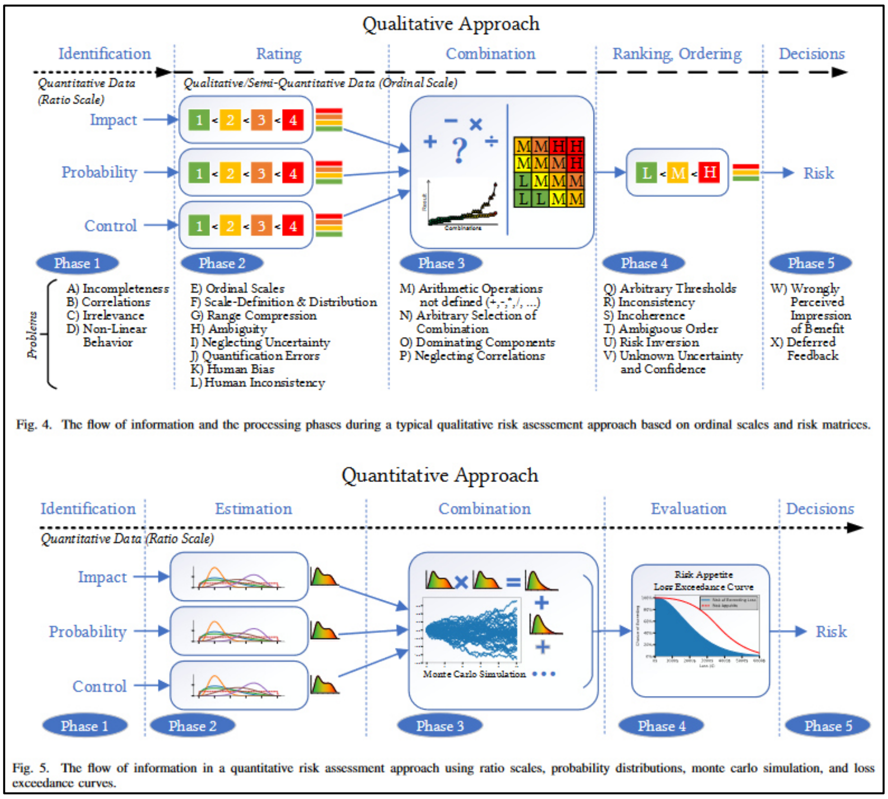


Figure 3: Phases of the semi-quantitative and quantitative assessment.
Source: Krisper (2021).

In IT security, there is no objective mechanism for assessing the security capability of a system (Jacobs et al., 2019). Without a quantitative metric with an objectively assessable mechanism of performance, a scoring system cannot be adapted to result in real risk classifications (Krisper, 2021). One internationally used metric in IT security is the Common Vulnerability Scoring System (CVSS) in version 3.1, v3.1 for short (First.org, 2022). Vulnerability is assessed in the CVSS via the degree of exploitability of a system-inherent vulnerability. An exploitability score is calculated using the scenario-describing parameters Attack Vector (AC), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI): Numerical values are assigned to the values of each parameter, for example "AV - Physical - 0.2", "AC - High - 0.44", etc., and linked to each other via a multiplicative relationship that forms the basis of the exploitability assessment according to CVSS. The numerical value of each assessment parameter is between 0 and 1 and represents an exploitability contribution. The higher this number, the assumption is, the more exploitable the system under consideration is. The exploitability score can be assigned to an attack feasibility category according to ISO/SAE 21434 (ISO/SAE, 2021b, p. 47) or a likelihood of exploitability category (LoE) according to Braband (2019).

Exploitability refers to the likelihood that a maliciously motivated attacker can take advantage of a system vulnerability to either perform an undesired action or attack an asset (First.org, 2022). High exploitability means that a vulnerability is easier to exploit than a vulnerability with low exploitability. Attack Feasibility assesses the likelihood that an attacker can conduct a successful attack on a system. It can now be argued that a system can be successfully attacked if there is at least one vulnerability that can be exploited. ISO/SAE 21434 (ISO/SAE, 2021b, p. 47) suggests using one of the three following approaches as a method for the attack feasibility rating:

1) Attack potential-based approach (assessment parameters: elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, equipment).

2) CVSS-based approach (assessment parameters: attack vector, attack complexity, privileges required, user interaction).
3) Attack vector-based approach (assessment parameters: predominant attack context; e.g. physical, local, adjacent, network).

Using the CVSS-based approach is one way of assessing exploitability. The assessment of the exploitability contributions with the CVSS results in an exploitability score, which is assigned to an attack feasibility category in ISO/SAE 21434 (ISO/SAE, 2021b, p. 69). In Braband (2019), for example, an exploitability score is assigned to a likelihood of exploitability (LoE) category. Based on the previous explanations, LoE or exploitability and attack feasibility can be equated. In the CVSS, in addition to exploitability, the impacts, consisting of the breach of the protection goals of confidentiality, availability and integrity, are also used to determine a vulnerability score. In a narrower sense, the CVSS does not generate a vulnerability score as a result because vulnerability components and impact components are linked together. If the CVSS were to include a metric for assessing threats in addition to the assessment of vulnerability and impact, the result of the CVSS could be interpreted as a risk score.

Braband (2019) proposes to logarithmize the CVSS score values. This is done to convert the CVSS metric for assessing exploitability into a semi-quantitative scoring approach. The logarithmization of values is a standard method in statistics (Gneiting & Raftery, 2004; Field, 2003, p. 203). Only formulas that do not mix the order of the data points may be used in the transformation. This is necessary in order to maintain the relative differences between the values of a variable. Data can also be transformed, for example, using a (square) root function, by adding a constant, by forming the reciprocal value (reciprocal transformation) or by reverse scoring. In the latter approach, each score value is subtracted from the maximum (Field, 2013, pp. 201-210).

When transforming data, a general distinction is made between linear transformation and non-linear transformation (Lehn et al., 2000). In a linear transformation, a linear function is applied to each numerical value of the data set, e.g. using the general formula "y = a·x + b". The "y" is the transformed value, the "a" describes the scaling factor, "x" is the original value and "b" describes the shift factor. Types of linear transformations are, for example, scaling (multiplication of the values of the data set by a number) or translation (addition of the values of the data set by a number). A common linear transformation in statistics is the z-transformation, also known as standardization. Here, data is normalized in such a way that it is converted into a standard normal distribution with a mean value of 0 and a standard deviation of 1 (Tachtsoglou et al., 2017, pp. 111-125).

An extension of the z-transformation is the robust scaler method, which is robust against data outliers (Brownlee, 2020; Eddie, 2021). The new, normalized values are determined using "X_new = (X - Q2) / (Q3 - Q1)". "X" describes the original value, "Q1" to "Q3" denote the quartiles of the data sets: "Q1" divides a data set into the lowest 25 %, "Q2" (median) into the middle 50 % and "Q3" into the top 25 % of the data. With non-linear transformation, a data set is transferred to a different scale. The function that is applied to the data set is correspondingly non-linear, i.e. the "output" is not proportional to the "input". Examples of non-linear transformations are the Box-Cox transformation (data is transformed to a normal distribution, see Box & Cox (1964)), and the log transformation (data is transformed to a logarithmic scale, see Keene (1995)). The log transformation is classically used when it is assumed that a growth process with a skewed or non-linear structure is present. With logarithmization, a multiplicative relationship can be transformed into an additive relationship (Gneiting & Raftery, 2004). This means that a non-linear growth function can be converted into linear growth stages. With logarithmization, an artificial zero point can be set arbitrarily, whereby the base to which the logarithmization is performed defines the dimensioning. When determining the exploitability (E) according to CVSS, a multiplicative relationship is assumed ($E = 8.22 \cdot AV \cdot AC \cdot PR \cdot UI$) (First.org, 2022).[7]

In addition, a barrier-based approach is applied to the CVSS, which postulates a defense-in-depth (DiD) effect (Braband, 2019). DiD assumes that each barrier has implementation errors and that each additional barrier reduces the probability of a successful attack (Schnieder et al., 2018, pp. 24-25). However, IT security lacks an objective mechanism of performance to assess the considerations of the proposed scoring system. For this reason, Termin et al. (2022) propose emulating the considerations from the IT security assessments in the physical security assessment. However, the emulation does not produce any clear results as to whether taking the number of barriers into account in the physical vulnerability assessment brings improvements. The questions arise from the previous explanation:

- To what extent can a cross-domain security assessment of physical security and IT security work?
- How can incompatibilities[8] between the semi-quantitative Harnser metric and the quantitative ICM from physical security be objectively proven? Under which boundary conditions can these incompatibilities be reduced? What requirements should be made to enable harmonization?
- How can distortions[9] be reduced within the Harnser metric and within the CVSS metric?
- How can the Harnser metric from physical security and the CVSS metric from IT security be aligned?
- How can security levels in the domains of physical security and IT security be coordinated with each other (also taking into account interactions)?

The questions raised encourage consideration of how two metrics from the domains of physical security and IT security can be harmonized, freed from distortions and merged into a cross-domain risk assessment that is not based on the same physical process, describes different influencing variables and where there may be interactions between the two domains. The interactions must be mapped on the basis of expert statements and linked selectively at individual points. At the same time, these links must be consistent in the overall context and it must also be possible to assign a certain probability to them so that vulnerability can ideally be calculated quantitatively. Due to the challenges mentioned, the risk assessment of automotive products must be carefully thought through in order to provide users with a toolbox of methods that can be used to support the risk-appropriate allocation of scarce resources in security measures.

[7] AV := Attack Vector, AC := Attack Complexity, PR := Privileges Required, UI := User Interaction.

[8] Incompatibility means that two metrics or the results based on the metrics do not match. Incompatibilities between two security metrics can occur, for example, if different objective risk amounts are assigned to the respective risk levels of the metrics. Examples of incompatibilities also include different definitions and interpretations of metrics, different scales, different measurement methods, measurement times and different units (Kan, 2002, pp. 219-226).

[9] Distortions include metric-inherent problems and inconsistencies. They only occur within a metric and not between metrics. Distortions are, for example, the non-consideration of relevant factors in relation to the facts under investigation, incorrect data or subjective or non-replicable assessments (Kan, 2002, pp. 63-69).

1.3 Goal Setting

The aim of this research work is to develop a framework for conducting a cross-domain threat analysis and risk assessment, which is based on common automotive standards. Based on the developed approach, users from industrial practice should be enabled to conduct both domain-specific security risk assessments and cross-domain security risk assessments of MAS applications. The basis for this should be the focus on the vulnerability of security technologies used in MAS. For the description of physical properties, it should be possible to determine probabilities for vulnerability on the basis of attacker properties. For the description of IT properties, it should also be possible to determine probabilities of exploitability based on attacker properties.[10] There should also be a procedure for feeding expert knowledge into the metric on which the assessment scheme from physical security or IT security is based. The favored solution for the probabilistically consistent merging of the physical security assessment and the IT security assessment is the transfer of the security assessments into Bayesian networks.

In order to achieve the goal of the research work, a cyber-physical threat analysis and risk assessment is proposed that builds on known standards and approaches for physical vulnerability and IT exploitability assessment and is partly based on methods of mathematical statistics and probability theory. First of all, a metric analysis using the example of metrics from physical security assessment is used to show how a scoring system can be calibrated or made quantitatively compliant with the aid of a quantitative metric with an objective mechanism of performance, so that the same vulnerability classifications can be achieved despite the different metrics. The requirements and boundary conditions for aligning scoring-based metrics with a quantitative metric are defined and how the quality of scoring-based assessment schemes can be assessed. In addition, requirements for enabling the harmonization of metrics from the domains of physical security and IT security are to be defined so that comparable risk classifications can be achieved despite different assessments. Building on the previous sub-goals, an approach is to be developed to assess cross-domain interactions between IT scenarios and physical scenarios.

To create a cross-domain security metric that is compatible with industry standards, the scenario analysis method is used for threat analysis and risk assessment. The approach provides a basis for collecting data for conducting a cross-domain security risk assessment (Cheng et al., 2014, p. 5). Overall, the threat analysis and risk assessment is essentially divided into three parts: the description of the mathematical relationships of an assessment metric of physical vulnerability, IT vulnerability and cyber-physical vulnerability. In the third part, the effects of IT security threats on physical security considerations are included. This work presents a holistic approach to consider expert knowledge, use-case specific threat scenarios and technological artifacts as well as impacts in case of a successful attack in the context of a cyber-physical threat analysis and risk assessment. To feed expert knowledge into the threat analysis and risk assessment, a procedure based on the Delphi and Cooke's survey method is presented, which can be used to bring together the probability statements of individual experts. The metric on which the proposed approach is based has the following overall properties:

1. It is modular, i.e. any MAS configurations and technological artifacts can be assessed.
2. It is structured consistently for both domains at process level.
3. It is designed in such a way that the protective effect of measures to reduce vulnerability can be mapped.
4. Expert knowledge can be elicited and transferred to the assessment system.

[10] The assessment variables in IT scoring systems cannot be traced back to an objective mechanism of performance because there is no quantitative metric. This is why "presumed" probability is written.

5. It can allow a comparison of MAS with conventional physical access systems, as the approach developed also enables a domain-specific assessment.

The metric contributes to risk assessment and can serve as a building block of corporate risk management so that risks of specific MAS use cases can be assessed at system level. The results of the dissertation can also contribute to the development of a guideline for the design of CPS and support the project's sponsor, WITTE Automotive, in designing cyber-physical products that deliver added value from data more securely.

1.4 Structure of the Work

Basic chapter 2 describes the state of the art in science and technology. It examines the scientific debate on cyber-physical security. The terms security and risk are then defined and types of metrics for assessing risks are presented. This is followed by a presentation of established assessment approaches in physical security assessment and IT security assessment. Common methods, models and metrics are described. The advantages and disadvantages of the approaches explained are named. In chapter 3 the genesis of an approach to the security assessment of physical security and IT security is presented. In the chapters 3.1 and 3.2 a structural analysis of the Harnser metric and the Common Vulnerability Scoring System (CVSS) metrics is conducted: On the one hand, in chapter 3.1, the semi-quantitative Harnser metric is compared with the quantitative Intervention Capability Metric. Using a barrier and an asset, the security capabilities of a fictitious system under consideration are assessed and compared for different configurations, once with one metric and once with the other metric.

The results then show a vulnerability assessment for both cases depending on the selected backup configuration. At the same time, the problem of incompatibility of metrics is examined in more detail and challenges, metric boundary conditions and requirements for harmonizing both metrics are worked out in detail. The aim is to generate the same vulnerability classifications despite different assessment metrics. On the other hand, in chapter 3.2, the classic CVSS and the barrier-based CVSS approach introduced in Braband (2019) are analyzed, whereby distortions and possibilities for reducing distortions within CVSS are discussed and analytically examined. In chapter 3.3.1 the vulnerability description in physical security and the vulnerability description in IT security are compared. Similarities and differences in the description of vulnerability in both domains are identified. In Chapter 3.3.2 assumptions and possibilities for harmonizing the risk descriptions and risk assessments in both security domains are presented. Chapter 3.3.4 shows how security levels in physical security and IT security can be defined and, in the case of cross-domain interaction, how they can be harmonized. Building on the findings of the analyses, chapter 4 will then outline the extent to which alignment can be achieved despite significantly different assessment metrics in the two domains.

The following chapters 4.1 to 4.5 describe the genesis of a prospective risk analysis for CPS, which is based on the requirements of ISO/SAE 21434. It describes how assets, threats, vulnerabilities and impacts can be assessed as part of a Cyber-Physical Threat Analysis and Risk Assessment (CPTARA). In a further step, the considerations for CPS risk analysis are described in chapters 4.6 to 4.8. They are transferred to Bayesian networks in order to make the metrics in both domains probabilistically consistent. Finally, a procedure based on the Delphi method and Cooke's survey approach is presented in order to collect expert knowledge and transfer it to the Bayesian network as input. In chapter 5 a discussion of the approach developed takes place. The results are then presented in chapter 6. An outlook highlights points of contact for possible follow-up research. In the appendix, chapter 8.1 discusses the problem in more detail. In chapter 8.2 in the appendix, paradigms in physical security and IT security are presented in detail. Chapter 8.3 in the appendix shows the problem of cross-domain merging using the example of the synthesis of theories in physics.

2 Basics

2.1 Guidelines and Standards

The use of CPS in vehicles has been increasing for over fifteen years (BSI Automotive Industry Situation Report, 2022). This makes it essential for operators to assess CPS from a physical security perspective and from an IT security perspective. "The automotive industry is heavily regulated by national and international regulations. [...] Technical specifications and test procedures are defined in over 150 individual regulations, above all for the road safety of the vehicle" (BSI Branchenlagebild Automotive, 2022). "At the same time, standards and norms do not yet cover all areas of vehicle development, so that numerous aspects are solved on an OEM or supplier-specific basis and can therefore lead to inhomogeneous solutions" (Wurm, 2022, p. 41). In the automotive sector, there are already industry standards for functional safety, in particular ISO 26262 (ISO, 2018) and DIN EN 61508[11] (DIN e.V., 2011), as well as metrics, e.g. Automotive Safety Integrity Level (ASIL) (see ISO 26262-3:2018, section 6.4.3, pp. 10, 19-26). These support suppliers in making vehicles and sub-systems functionally safe during product development. "The entry into force and further development of new standards and norms should make a decisive contribution to this," explains the Automotive 2022 sector situation report from the German Federal Office for Information Security (BSI) (BSI Branchenlagebild Automotive, 2022). In Germany, the general type approval (ABG) defines requirements for the approval of vehicles in road traffic (KBA, 2021).

The German Technical Inspection Association (TÜV for short) offers a "comprehensive portfolio of services in the areas of testing and certification, auditing and advice on all aspects of vehicles" (TÜV, 2021). It is an organization that conducts safety checks on vehicles. The checks are prescribed by laws and regulations in the Federal Republic of Germany. They confirm the conformity of a vehicle with specified safety requirements. Quality assurance in the automotive sector also includes crash test ratings, such as RCAR (RCAR, 2021) and Euro NCAP (Euro NCAP, 2021). Crash tests help to improve safety. Customers generally prefer vehicles rated as safe to those rated lower (VDA, 2022). Such tests do not yet exist for the security of CPS. However, tests for conformity with specified IT security requirements are in progress.

Traditional physical locking systems are highly standardized in Germany (Schwerdtfeger, 2018, pp. 3-5). Physical security has evolved historically. There are established approaches in the industry for measuring physical security. These have been anchored in standards and guidelines for years. Requirements for different use cases and misuse scenarios are specified in physical security standards. DIN EN 1627 (DIN e.V., 2021a), for example, defines resistance classes (RC) for doors, windows, curtain walls, grille elements and shutters. Behind an RC are resistance times against attackers with certain skills and tools (Harnser, 2010, C2, p. 10). The higher the RC, the higher the resistance time. DIN EN 1628 (DIN e.V., 2021b), for example, describes procedures for testing the effectiveness of physical protection properties.

Thatcham, a testing institution for vehicles from the UK, offers certifications and catalogs of measures relating to the physical security of vehicles and access systems (Thatcham, 2021). Locks and door handle units are tested in mechanical penetration tests for their resistance to attempts to overcome them and given security ratings. There are not yet any specifications for radio-based locking systems. In contrast to standards for physical security, standards for IT security are fairly new. There is, for example, the ISO 27,000 family (DIN e.V., 2018) or specifica-

[11] DIN EN 61508 is the German version of IEC 61508 (IEC, 2010), which is a basic standard of ISO 26262.

tions from the German Federal Office for Information Security (BSI), such as the BSI basic protection compendium (BSI, 2020). The BSI baseline protection compendium includes specifications for the design and operation of an information security management system (ISMS) (Furnell et al., 2013, p. 151). However, these are not use case-specific and not all best practices are part of the compendium.

The Digital Key Standard (DKS) of the Car Connectivity Consortium (CCC, 2021) defines requirements for the virtual vehicle key of a digital vehicle access system, such as the use of an embedded Secure Element (eSE) in mobile devices to store digital keys and support cryptographic operations. The Potsdam-based non-profit organization Open Security Standards (OSS) Association is working on the development of international standards for access control systems. It has already published the OSS Standard Offline (OSSSO) for mobile access via smart cards. With the help of the OSSSO, electronic locks should be able to "read authorizations of an access card independently of the manufacturer and interpret them in the same way" (OSS Association, 2021). In the automotive sector, functional safety has been at the top of the industry's priorities for the last ten years (Macher et al., 2020a; Möller et al., 2019, p. 302). The increasing growth of IT components is turning modern vehicles into data hubs. At the same time, data from vehicle-inherent systems are attractive targets for cyberattacks (BSI Branchenlagebild Automotive, 2022).[12] Due to the interoperability of system components within the vehicle, successful attacks can cause unwanted damage events that affect functional safety or physical security (Macher et al., 2020a; Möller et al., 2019, pp. 266, 271). In particular, the consideration of cybersecurity in product development processes is becoming increasingly important (Möller et al., 2019, p. 294; Schmittner et al., 2018).

To address the challenges posed by cyber threats, the UNECE R 155 Regulation (R 155 for short) for Cybersecurity Management Systems (CSMS) was introduced by the United Nations Economic Commission for Europe (UNECE) in January 2021 (UNECE, 2021). It is part of the UNECE Working Party 29 (WP.29). In addition to specifications for the implementation of a CSMS (R 155), it also establishes specifications for Software Update Management Systems (SUMS; R 156) and Automated Lane Keeping Systems (ALKS; R 157). R 155 addresses companies that bring vehicles onto the market, e.g. original equipment manufacturers (OEMs). As of April 2022, the handling of cybersecurity is not yet a formal regulatory requirement for the approval of new vehicles for the market (homologation). Conformity with R 155 will already be required from July 2022 for all new vehicle types that are placed on the UNECE-regulated market. This market includes the EU, South Korea and Japan. From July 2024, conformity with R 155 will be mandatory for all new vehicle registrations here.

One way of demonstrating this conformity is certification in accordance with ISO/SAE 21434 "Road Vehicles - Cybersecurity Engineering". Informative excerpts of the standard can be viewed publicly (ISO/SAE, 2021a). The full version is provided by the Society of Automotive Engineers (SAE) (ISO/SAE, 2021b). The standard is based on SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (SAE, 2021). SAE J3061 contains a practical guide for cybersecurity engineering in relation to products in the vehicle over the entire life cycle. SAE J3061 proposes the Threat and Operability Analysis (TOA), Attack Tree Analysis (ATA) and the HEAVENS Security Model (Autosec, 2016) for analyzing and assessing cybersecurity risks.

[12] The BSI and the Federal Motor Transport Authority (KBA) have been working more closely together since December 2020 to "further secure digitalization and create reliable framework conditions for investment and innovation" (BSI Branchenlagebild Automotive, 2022).

ISO/SAE 21434 defines the scope somewhat more broadly and describes general requirements for information security[13] , process quality[14] and product security[15] . In contrast to the risk-based approach of Threat Analysis and Risk Assessment (TARA) from ISO/SAE 21434, ISO 26262 conducts a HARA (Hazard Analysis and Risk Assessment). "These two processes [HARA and TARA] are different, but are related and require integrated communications in order to maintain consistency and completeness between [...] process outputs" (SAE, 2021, p. 6). According to Wurm (2022), the task of a TARA is to conduct "a complete and systematic investigation of all possible and probable attack vectors for a specific system" (Wurm, 2022, p. 35).

According to ISO 26262, safety risk is defined as the combination of the probability of occurrence of damage and the corresponding extent of damage. According to the HARA from ISO 26262, risk can also be defined as a function of the frequency of occurrence of a hazardous event (Frequency, F), the ability to prevent damage by timely reactions of the persons involved or by external measures if a hazardous condition has occurred (Controllability, C) and the potential severity of the resulting damage (Severity, S). The three risk parameters F, C and S are divided into four levels and combined within the HARA to determine the Automotive Safety Integrity Level (ASIL). The ASIL can be interpreted as a measure of the required risk reduction (Krisper, 2021).

The security risk according to ISO/SAE 21434, on the other hand, is defined as a combination of the probability of damage occurring (attack feasibility) and the corresponding extent of damage (impact): The risk parameter Impact is linked to the present attack vector, consisting of the descriptors "Physical", "Local", "Adjacent" and "Network", in order to determine the Cybersecurity Assurance Level (CAL) (ISO/SAE, 2021b, p. 59) (see also Chapter 3.3.4). The definition of the CAL is described in Macher et al. (2020b):

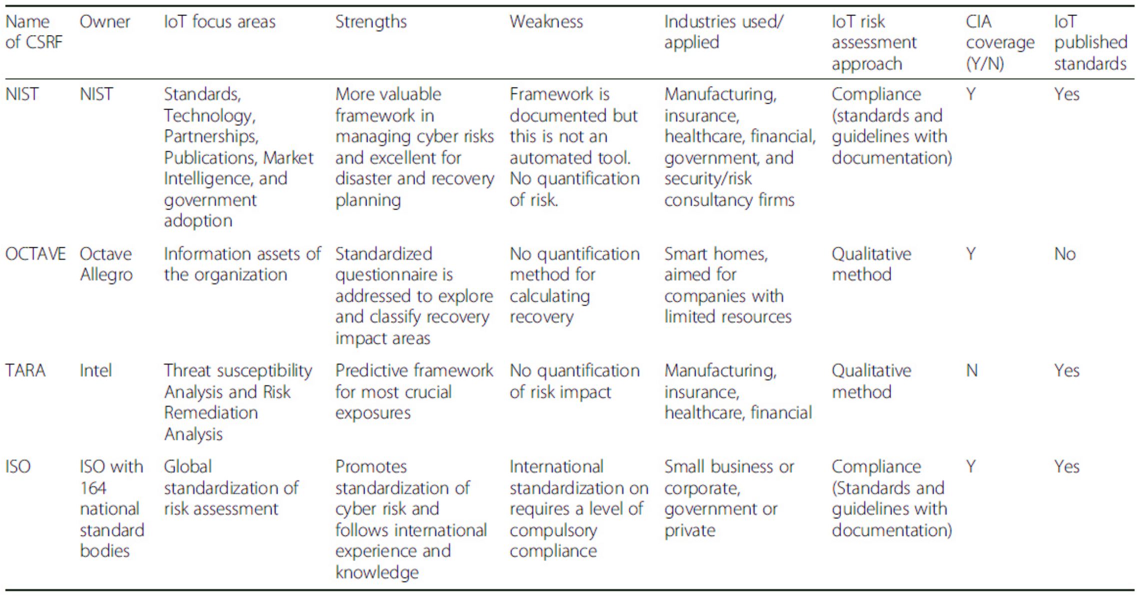
> The CAL should have been used to define rigorous and applicable methods, but since no consensus was found yet on how to determine and treat such a parameter, this part has also been moved to the Annex [E] only. Thus, a risk-oriented approach for prioritization of actions and methodical elicitation of cybersecurity measures is encouraged, but no further added value in terms of best practices or agreed approaches is given. (Macher et al., 2020b, p. 10).

SAE J3061 contains a number of parallels to ISO 26262. In the Cybersecurity Process Overview (SAE J3061, Part 8), the phases of the development cycle are based on Parts 3-8 of ISO 26262 (SAE, 2021; Costantino et al., 2022). They include the concept phase, system development (hardware, software), production and supporting processes. It applies to components (electronic parts and software) of series-produced vehicles as well as spare parts and accessories. ISO/SAE 21434 covers the development, production, operation, maintenance and decommissioning phases in the life cycle of a vehicle. OEMs must therefore demonstrate compliance with the requirements of the standard across the entire supply chain (Macher et al., 2020b). Key points of ISO/SAE 21434 are the establishment and operation of a cybersecurity management system (CSMS) and threat analysis and risk assessment (TARA). According to Kandasamy et al. (2020), TARA is one of four common cybersecurity risk frameworks that can be used to assess networked devices (for the scope, advantages and disadvantages of the four frameworks, see Table 1).

[13] As an "umbrella", described in ISO 27001 (DIN e.V., 2018).

[14] As a "carrier", described in Automotive SPICE Supply Chain & Cybersecurity (SPICE, 2015).

[15] As a "foundation". The Threat Analysis and Risk Assessment (TARA) of ISO/SAE 21434 (ISO/SAE, 2021b, p. 41-49) is an important procedure for deriving cybersecurity requirements.



Name of CSRF	Owner	IoT focus areas	Strengths	Weakness	Industries used/ applied	IoT risk assessment approach	CIA coverage (Y/N)	IoT published standards
NIST	NIST	Standards, Technology, Partnerships, Publications, Market Intelligence, and government adoption	More valuable framework in managing cyber risks and excellent for disaster and recovery planning	Framework is documented but this is not an automated tool. No quantification of risk.	Manufacturing, insurance, healthcare, financial, government, and security/risk consultancy firms	Compliance (standards and guidelines with documentation)	Y	Yes
OCTAVE	Octave Allegro	Information assets of the organization	Standardized questionnaire is addressed to explore and classify recovery impact areas	No quantification method for calculating recovery	Smart homes, aimed for companies with limited resources	Qualitative method	Y	No
TARA	Intel	Threat susceptibility Analysis and Risk Remediation Analysis	Predictive framework for most crucial exposures	No quantification of risk impact	Manufacturing, insurance, healthcare, financial	Qualitative method	N	Yes
ISO	ISO with 164 national standard bodies	Global standardization of risk assessment	Promotes standardization of cyber risk and follows international experience and knowledge	International standardization on requires a level of compulsory compliance	Small business or corporate, government or private	Compliance (Standards and guidelines with documentation)	Y	Yes

Table 1: Cybersecurity risk frameworks.
Source: Kandasamy et al. (2020).

The steps for conducting a TARA are shown in Figure 4. The entries marked in light gray represent work packages. The TARA process is to be read from left to right. Inputs and outputs of the individual work packages are indicated by the respective arrow directions. The determination of the CAL is marked with a black frame because it is an optional work package. In Table 2 the associated methodological steps are listed. The steps in HARA and TARA are similar (Macher et al., 2020b). Assets are identified and damage scenarios are assessed: While HARA is concerned with the assessment of potential accidents, TARA is concerned with the assessment of malicious attackers (Ponsard et al., 2021). In both cases, security requirements and security measures are derived after the assessment of accident scenarios (ISO 26262) or attack scenarios (ISO/SAE 21434). "Both standards [however] pursue a common goal: the development of a reliable, error-free and safe (safe and secure) system by reducing the risks of hazards and threats as much as possible" (Wurm, 2022, p. 69).

However, ISO/SAE 21434 only describes a framework (Costantino et al., 2022; BSI Branchenlagebild Automotive, 2022) that focuses on defining minimum criteria for cybersecurity in the automotive industry (Macher et al., 2020a). The actual implementation is up to the user: "So far, published documents [of ISO/SAE 21434] indicate that the standard specifies neither cybersecurity technologies, solutions, nor remediation methods. Nor, that unique requirements for autonomous vehicles or road infrastructure are given" (Macher et al., 2020a, p. 3).

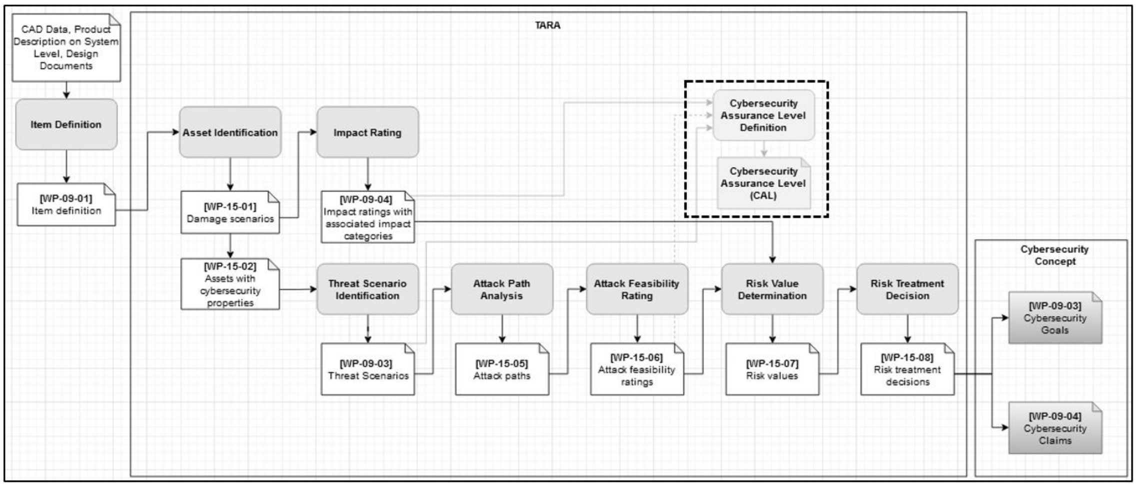

TARA
CAD Data, Product Description on System Level, Design Documents
Item Definition
[WP-09-01] Item definition
Asset Identification
[WP-15-01] Damage scenarios
[WP-15-02] Assets with cybersecurity properties
Impact Rating
[WP-09-04] Impact ratings with associated impact categories
Cybersecurity Assurance Level Definition
Cybersecurity Assurance Level (CAL)
Threat Scenario Identification
[WP-09-03] Threat Scenarios
Attack Path Analysis
[WP-15-05] Attack paths
Attack Feasibility Rating
[WP-15-06] Attack feasibility ratings
Risk Value Determination
[WP-15-07] Risk values
Risk Treatment Decision
[WP-15-08] Risk treatment decisions
Cybersecurity Concept
[WP-09-03] Cybersecurity Goals
[WP-09-04] Cybersecurity Claims

Figure 4: TARA according to ISO/SAE 21434
Source: ISO/SAE (2021b, pp. 73-78).[16]

Work Package	Input	Output	Methodical Steps
Item Definition (Precondition)	CAD Data, Product Description on System Level, Design Documents	**[WP-09-01]** Item definition	Items are defined, containing item boundary, item functions, the preliminary architecture and information about the operational environment
Asset Identification	**[WP-09-01]** Item definition	**[WP-15-01]** Damage scenarios	Damage scenarios are identified.
	[WP-09-01] Item definition **[WP-15-01]** Damage scenarios	**[WP-15-02]** Assets with cybersecurity properties	Assets with cybersecurity properties whose compromise leads to a damage scenario are identified.
Impact Rating	**[WP-15-01]** Damage scenarios	**[WP-15-04]** Impact ratings (with associated impact categories)	The damage scenarios are assessed against potential adverse consequences for road users in the impact categories of safety, financial, operational, and privacy (S, F, O, P) respectively. The impact rating of a damage scenario is determined for each impact category (severe, major, moderate or negligible). Safety related impact ratings are derived from ISO 26262-3:2018. If a damage scenario results in an impact rating and an argument can be made that every impact of another impact category is considered less critical, then further analysis for that other impact category is conducted.
Threat Scenario Identification	**[WP-15-02]** Assets with cybersecurity properties	**[WP-15-03]** Threat scenarios	Threat scenarios are identified and include targeted asset; compromised cybersecurity property of the asset; and cause of compromise of the cybersecurity property.
Attack Path Analysis	**[WP-15-03]** Threat scenarios	**[WP-15-05]** Attack paths	The threat scenarios are analyzed to identify attack paths. An attack path is associated with the threat scenarios that can be realized by the attack path.
Attack Feasibility Rating	**[WP-15-05]** Attack paths	**[WP-15-06]** Attack feasibility ratings	In case a CVSS-based approach is used, the attack feasibility rating should be determined based on the exploitability metrics, including: a) attack vector; b) attack complexity; c) privileges required; and d) user interaction.

[16] WP := Work Product. The first digit stands for the clause in ISO/SAE 21434. The second digit is a consecutive identification number.

Risk Determination	**[WP-15-04]** Impact ratings **[WP-15-06]** Attack feasibility ratings	**[WP-15-07]** Risk values	For each threat scenario the risk value is determined from the impact of the associated damage scenarios and the attack feasibility of the associated attack paths.
Risk Treatment Decision	**[WP-15-07]** Risk values	**[WP-15-08]** Risk treatment decisions	For each threat scenario, considering its risk values, one or more of the following risk treatment option(s) shall be determined: a) avoiding the risk; b) reducing the risk; c) sharing the risk; d) retaining the risk.
Cybersecurity Assurance Level Definition **(optional)**	**[WP-15-03]** Threat scenarios **[WP-15-04]** Impact ratings **CVSS' Attack Vector** **[WP-15-06]** Attack feasibility ratings	Cybersecurity Assurance Level (CAL)	For each threat scenario the CAL is determined from the impact of the associated damage scenarios and the attack vector of the associated attack paths.

Table 2: TARA process including method description.
Source: Own table based on ISO/SAE (2021b, p. 73-78).

As the OEMs have to provide evidence of the CSMS across the entire supply chain for the homologation of their products (vehicles) in accordance with UNECE R 155, they will require automotive suppliers to comply with the requirements for a CSMS and to prepare a TARA. Furthermore, evidence of cybersecurity test implementation and the test results will have to be provided as part of the CSMS across the supply chain. "Manufacturers must transfer certain requirements to their suppliers in order to implement a holistic security concept," says Wurm (2022, p. 36) in this context. In principle, homologation is the responsibility of the OEM. There are exceptions, e.g. in the case of passive safety systems. Here, the Tier 1 supplier can also homologate systems independently. With ISO/PAS 5112:2022 (ISO, 2022) "Road Vehicles - Guidelines for Auditing Cybersecurity Engineering", a standard has been published in which the auditing of a CSMS and the components of the CSMS auditor are defined. However, how OEMs require proof of ISO 21434 conformity from Tier 1 is a matter for the respective OEM. However, it is likely that a Tier 1 supplier will need to conduct a TARA. To help vehicle manufacturers prepare for the assessment, the German Association of the Automotive Industry (VDA) has published the document "Automotive Cyber Security Management System Audit" (VDA, 2020). It "defines the catalog of questions and the assessment scheme that can be used when auditing the CSMS of both OEMs and contractual partners" (VDA, 2020).

TARA is a scenario-based analysis in which the impact of an IT scenario on safety is classified qualitatively on a scale from "Negligible" (S0: No injuries) to "Severe" (S3: Life-threatening injuries) (ISO/SAE, 2021b, pp. 63-64). According to SAE J3061, functional safety is a subset of cybersecurity (see Figure 5 on the right). Safety architectures can therefore be extended by cybersecurity elements. Safety engineering and cybersecurity engineering also have overlaps in work steps (see Figure 5 left). Requirements from both domains can be part of a common specification. "Cybersecurity is a cross-cutting topic which, like functional safety, is linked to virtually all other disciplines. "Working in "silos" should therefore (also) be systematically avoided", says Wurm (2022, p. 60). For example, HARA can be conducted first. The results are introduced as input into the TARA, i.e. functional safety objectives can be formulated in the form of assets to be protected in the TARA (for the principle, see Figure 6Figure 5). A similar approach is proposed by the North Atlantic Treaty Organization Science and Technology (NATO S&T) (Piper, 2020).

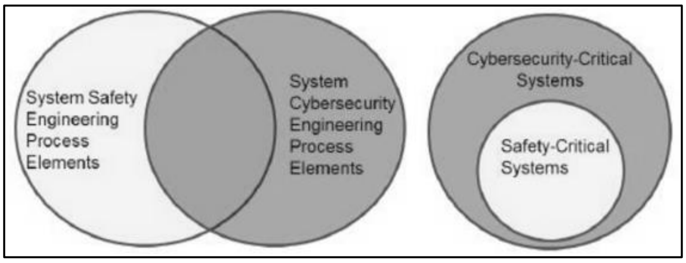

System Safety Engineering Process Elements
System Cybersecurity Engineering Process Elements
Cybersecurity-Critical Systems
Safety-Critical Systems

Figure 5: Intersections of functional safety and cybersecurity.
Source: SAE (2021, p. 17).

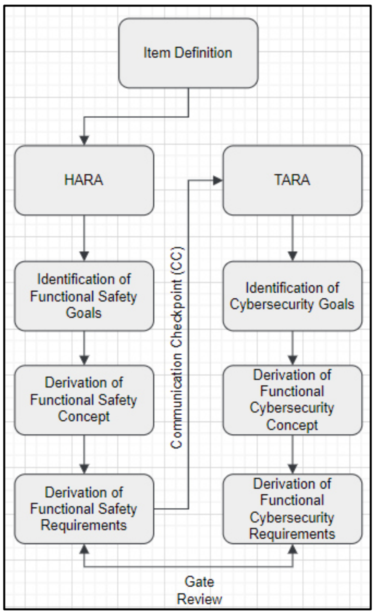

Item Definition
HARA
TARA
Identification of Functional Safety Goals
Derivation of Functional Safety Concept
Derivation of Functional Safety Requirements
Communication Checkpoint (CC)
Identification of Cybersecurity Goals
Derivation of Functional Cybersecurity Concept
Derivation of Functional Cybersecurity Requirements
Gate Review

Figure 6: Exemplary linking of HARA and TARA.
Source: Own Figure based on SAE (2021, p. 40).

The SoQrates initiative is driving forward the project to support German industry in the implementation of Automotive SPICE (SoQrates, 2022). The European Union Agency for Cybersecurity (ENISA) also publishes a comprehensive report on incidents, trends and prime threats by sector as well as mitigation measures on the topic of cybersecurity. One of the three main areas classified by ENISA as particularly threatened and considered in the report is the transportation sector (ENISA, 2021, p. 29). In the "E-safety Vehicle Intrusion Protected Applications (EVITA)" project, which is supported in consortial cooperation with the Fraunhofer Institute, the BMW Group, Bosch, Infineon and other partners, a document was published that sets out procedures for determining and assessing security requirements.

The proposed EVITA approach is applied, for example, in Ruddle et al. (2009) using the example of vehicle on-board networks. The "Security requirements for automotive on-board networks" (Ruddle et al., 2009, pp. 24-57) developed therein provide contributions to the design of a secure on-board architecture. EVITA pursues the goal "to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle" (EVITA, 2022).

In addition, the 5StarS Consortium is working on developing a framework for assessing vehicle cybersecurity from an insurance perspective (5Star, 2021). A taxonomy called AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target) was introduced back in

1995 for the classification of vulnerabilities in the cyber domain, which can support users in assessing risks (Möller et al., 2019, p. 328). Product developers are faced with the challenge of merging models from physical security, functional safety and IT security across domains as well as the challenge of merging metrics from physical security or functional safety and IT security. One reason for this is the quantitative analysis required. Wurm (2022) clarifies this:

> Redundant safety paths are insufficient for protection against security attacks. [...] However, the criticality is not limited to safety aspects. Without sufficient protection against cybersecurity attacks, networked and automated vehicles could easily be affected by theft, sabotage or hacktivism. (Wurm, 2022, p. 30).

In networked systems, there can be no functional safety without security. For this reason, no functional safety requirements should be placed on IT security functions (Wurm, 2022, p. 38). From the operator's point of view, loss of trust on the part of the customer and reputational damage can be a realistic consequence of successful attacks (Wurm, 2022, p. 30). A quantitative analysis of IT threat scenarios is difficult to perform (Scala et al., 2019). Requirements must be weighed against each other, but approaches that could enable a quantitative analysis are not yet to be found in current standards (Macher et al., 2020a).

However, UNECE WP.29 requires vehicle manufacturers to conduct a "risk assessment [...] of individual vehicle systems and their interaction with each other and with external systems" (Elektronik Automotive, 2020, pp. 27-28). Fosch-Villaronga & Mahler (2021) describe that functional safety and security are largely considered separately in previous guidelines: "Cybersecurity and physical product safety legal requirements are governed separately in a dual regulatory framework, presenting a challenge in governing uniformly and adequately cyber-physical systems" (Fosch-Villaronga & Mahler, 2021, p. 1). Möller et al. (2019) take a similar view:

> The growing complexity and networking of today's automotive systems increases the importance of functional safety and security. Safety and security issues have been treated separately for the most part [...] Trends such as remote access via the internet require rethinking this separation and setting up concepts for systems that allow common usage safely and securely. (Möller et al., 2019, p. 350).

One reason for the largely separate approach to date is the lack of an effective mechanism in IT security (Jacobs et al., 2019). IEC 61508 Edition 2.0, for example, proposes an integrated approach for linking the assessment of functional safety and IT security: IT security threats should be taken into account during the hazard analysis and risk assessment from functional safety. However, the integrated threat analysis is not further specified in IEC 61508. Recommendations regarding the interaction between safety and security are also given in ISO 26262 Edition 2.0 in Annex E (Macher et al., 2020a). However, these do not offer a solution for synthesizing the incompatible metrics from both disciplines. Macher et al. (2020a) summarize the current state of standardization of products in the automotive sector: "The available standard[s] are frequently fragmented or incomplete, and typically assume that their open issues are covered by other guidelines or standards" (Macher et al., 2020a, p. 3). When designing automotive products that combine security functions from both domains, there are two central problems: "(a) the availability of appropriate expertise in each single engineering domain [e.g. functional safety and cybersecurity], and (b) the consistent merging of the individual aspects to a multidisciplinary product" (Macher et al., 2020a, p. 2).

Data must be able to be exchanged, stored and processed for the provision of services. Questions relating to the storage and handling of data in the use case are to be answered in the course of developments driven by Europe. Examples of this are the General Data Protection

Regulation (GDPR, 2021) and GAIA-X (2021). GAIA-X is a project funded by the EU member states to establish a trustworthy European data traffic infrastructure. By using the International Data Spaces (IDS) standard (IDSA, 2021), which has been incorporated into DIN SPEC 27070 (DIN e.V., 2020) "Requirements and reference architecture of a security gateway for the exchange of industry data and services", the EU countries want to create a legal and commercial framework for companies to be able to offer data-driven business models that comply with privacy aspects, including those relating to the vehicle ecosystem (MDS, 2022). Essentially, the implementation of IDS should enable the standardized networking of systems and applications (MaaS Alliance, 2022). The consideration of privacy aspects in particular makes the implementation of a risk assessment even more complicated. Overall, the state of the art in locking technology and in the automotive sector shows a need for the metric merging of physical security and IT security (see Table 3).

Locking Systems - Mechanics	Locking Systems - Electromechanics, Electronics	Locking Systems - RFID
DIN EN 1303	EN 15684	VDA 5500
DIN 18252	VdS 2156-2	ISO/IEC 10536
VdS 2156-1	TL 03405	VDA 5501
DIN 18257	IEC 60068 series	ISO/IEC 14443
VdS 2386	VdS 2215	ISO/IEC 15693
DIN EN 1154	EN 61000-4 series	ISO/IEC 10373
DIN EN 112209	Locking Systems - Intrusion Detection	ISO/IEC 15961
DIN 18273	VdS 2119	ISO/IEC 15962
DIN 18251-1, -2	VdS 2271, VdS 2314	ISO/IEC 18000
DIN EN 1906	VdS 3112	VDI 4470
DIN EN ISO 7046	VdS 2110	Locking Systems IT
VdS 2201	Locking Systems - Biometry	Digital Key Standard (DKS)
VdS 2396	VdS 3112	International Data Spaces / DIN SPEC 27070
DIN 18252	ISO/IEC 2382-37	OSSSO
Automotive Security	Automotive Safety	Safety and IT Security
ISO/SAE 21434	IEC 61508	IEC TR 63069
UNECE WP.29 (R 155, R 156)	ISO 26262	ISO TR 22100
NIST SP 800-160 volume 1	SAE J2980	IEC 61508 Edition 2.0
ENISA	VDA 702	ISO 26262 Edition 2.0
SAE J3061	ISO 12100	
ISO/FDIS 24089	ISO/IEC Guide 51	Projects, Methods, Reports and Associations
VDA (ACSMS)	ISO TR 4804	EVITA
ISO 27000 Series	ISO 21448	SAHARA
ISO 20077	UNECE R 157	Alliance for Cyber Security (BSI)
ISO 31000:2018	ISO 8800	automotive.wiki
ISO PAS 5112	NHTSA	SoQrates
Auto ISAC		ENX Association
VDA Automotive SPICE Extension for Cybersecurity		Cybersecurity Council Germany e.V.
EU Cybersecurity Act		ISO/SAE AWI 8475
EU-GDPR		ISO/IEC 5888
Automotive Security Quality & Process relevant		ISO/SAE AWI 8477
ITAF 16949		FA 512 Safety & Security Wiki
IEC 62443		COVESA
IT baseline protection compendium		AUTOSAR, SHE, SHE+, OMG, CCC, HIS
DfT UK (Principles for Cybersecurity)		NIS2 Directive
ACEA		SafEUr
		PRESERVE

Table 3: Projects, standards and associations in the locking systems and automotive sector.
Source: Own table expanded according to Schwerdtfeger (2018)[17]

[17] Standards and guidelines for the automotive sector were developed as part of the activities of VDI Technical Committee 512 "Safety & Security". RFID := Radio Frequency Identification.

2.2 Research into Cyber-Physical Security

Scientific research into the risk assessment of MAS is relatively new. The Institute for Security Systems (ISS) has already published scientific papers on MAS. Examples include Schwerdtfeger (2018) on the security risk assessment of immobile MAS and Termin et al. (2020) and Termin et al. (2021) on automotive MAS. Because MAS can be characterized as CPS, the state of research on the security of CPS is considered below. CPS security has received scientific attention since 2006. The term "cyber-physical system" is said to have been first used by Helen Gill of the National Science Foundation (NSF) in 2006 (Ittermann et al., 2018, pp. 33-60). In Cardenas et al. (2009), security challenges posed by the use of CPS are named, such as "software patching and frequent updates" (Cardenas et al., 2009, p. 2) and "real-time availability" (Cardenas et al., 2009, p. 2). In addition, the same scientific article highlights unique characteristics of CPS compared to traditional IT systems. These include, for example, "network dynamics" (Cardenas et al., 2009, p. 3) and "dynamics of the physical system" (Cardenas et al., 2009, p. 4). Finally, Cardenas et al. (2009) present mechanisms for threat prevention (including deterrence), detection and recovery (resilience). A central problem in the design of CPS is described as follows: "Researchers have not considered how attacks affect the [...] control algorithms - and ultimately, how attacks affect the physical world" (Cardenas et al., 2009, p. 3).

Specific requirements for a CPS, particularly with regard to different use cases, are set out in Neuman (2009). Neuman (2009) points out that CPS elements can be spatially separated and orchestrated in a decentralized manner. Due to the fact that CPS operate in different applications, which can be accompanied by different environmental boundary conditions, individual security requirements are needed: "One needs to define the authorized and unauthorized information-flow, control-flow, and availability requirements of the application, taking into account the physical as well as the cyber consequences of a breach of any of these requirements" (Neuman, 2009, p. 2). This makes the security assessment complicated (Neuman, 2009). In Ashibani & Mahmoud (2017), CPS are distinguished from IoT devices:

> IoT is defined as a communication network connecting things which have naming, sensing and processing abilities. [...] [whereas CPS] is mainly related to real-time systems including distributed real-time control systems that integrate computing and communication capabilities with monitoring and control of entities in the physical world.
> (Ashibani & Mahmoud, 2017, p. 3).

CPS are divided into three layers in Ashibani & Mahmoud (2017): Application (use case), Transmission (communication interface) and Perception (hardware). This tripartite division is recommended as the basis for conducting a CPS risk assessment (Ashibani & Mahmoud, 2017). In contrast to the approach in Ashibani & Mahmoud (2017), Möller et al. (2019, p. 356) propose a five-part division. This division consists of the application layer, the transportation layer, the network layer, the link layer and the physical layer. A more detailed breakdown into a total of seven categories is provided in Alguliyev et al. (2018), for example: These include the physical layer, protocol layer, session layer and application layer. In the Open Systems Interconnection (OSI) model of the International Telecommunication Union (ITU) from ISO/IEC 7498-1:1994, a system is divided into a total of seven layers: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and Application Layer (Kumar et al., 2014).

In the model proposed in Ashinabi & Mahmoud (2017), security is divided into two areas: information and data security on the one hand and control security on the other. In Ashinabi & Mahmoud (2017), control security includes physical security. The interfaces between the three layers must be protected to a particularly high degree (Ashinabi & Mahmoud, 2017). Alguliyev et al. (2018) suggest using suitable authentication protocols and encryption algorithms to secure a CPS. The focus in Alguliyev et al. (2018) is on IT security and also privacy violations. Attack vectors are differentiated between external (external attackers) and internal (malicious employees).

In addition, general countermeasures, such as multi-layer security solutions, are proposed (Alguliyev et al., 2018). The aim is to develop a robust assessment model for verifying all threats and vulnerabilities in order to be able to contribute to decision-making regarding investment in security measures in a defined context (use case) (Alguliyev et al., 2018). Ashibani & Mahmoud (2017) describe that CPS security is a new field in which only a few papers have been published to date. Lun et al. (2019) counted a total of 57 publications on the topic of CPS security in 2015 (see Figure 7). Figure 7 shows the trend that addressing CPS security is becoming increasingly important from the perspective of the scientific community.

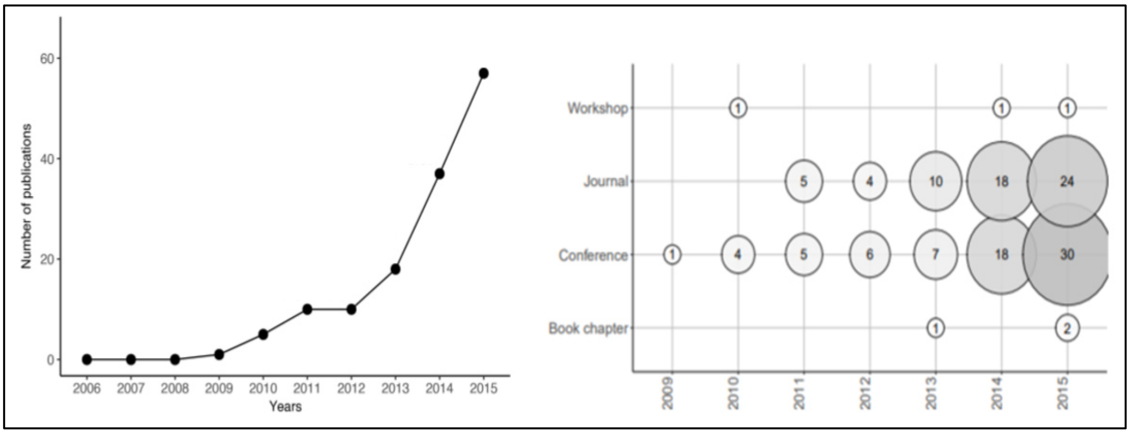


Figure 7: Publications on CPS security over the year (left) and by format and year (right). Source: Lun et al. (2019).

Graja et al. (2020) analyze which modeling languages are used to model CPS and in which application areas publications are available in this context. The following approaches are identified in Graja et al. (2020): Architecture Analysis & Design Language (AADL), Body Area Networks (BAN), Business Process Model and Notation (BPMN), Modelica, Planning Domain Definition Language (PDDL), Multi-Modeling Techniques (MMT) and Unified Modeling Language (UML). For the total of 62 publications examined, the proportions of the modeling languages used are summarized as follows (see Figure 8):

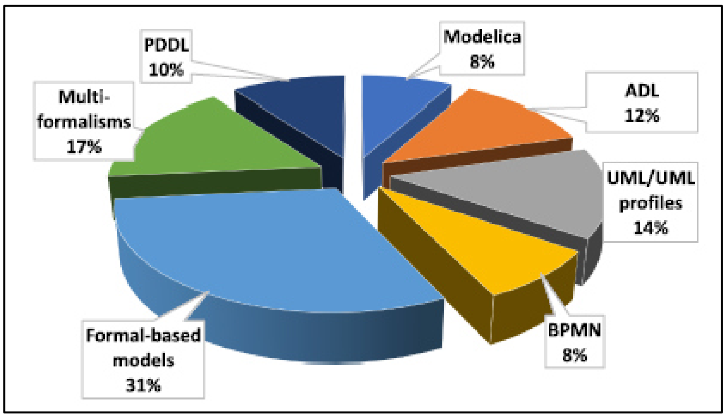


Figure 8: Proportion of modeling languages used in the modeling of CPS. Source: Graja et al. (2020).[18]

[18] Number of publications analyzed: n = 62.

According to Graja et al. (2020), CPS modeling approaches are divided into four application areas: "Transportation Systems", "Emergency Rescue Systems", "Health-Care" and "Smart Home/Area" (see Figure 9). The results of the research by Graja et al. (2020) show that Architecture Description Languages (ADL), Unified Modeling Language (UML), multi-modeling techniques and formal-based methods are widely used for CPS in the automotive sector.

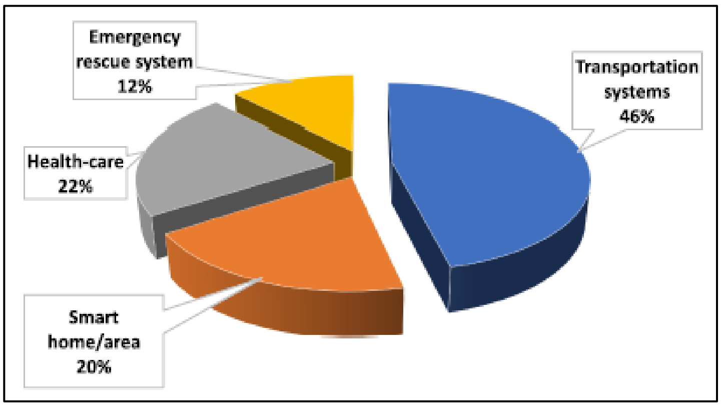
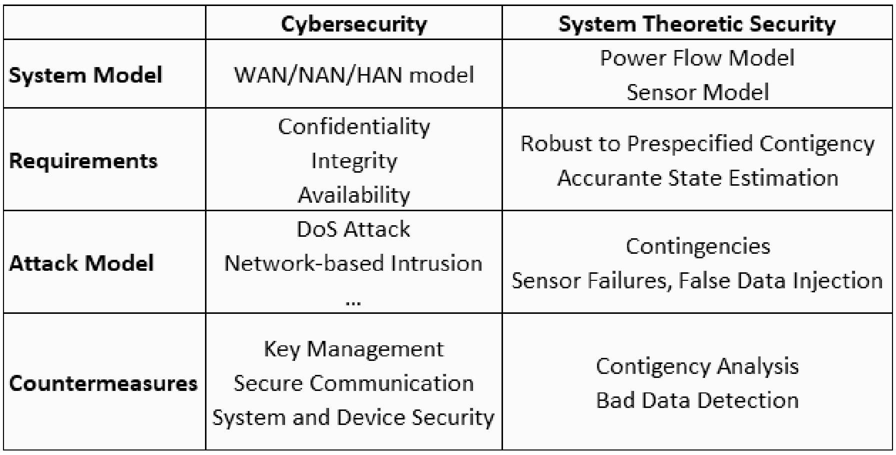


Figure 9: Proportion of application areas in the modeling approaches for CPS applications. Source: Graja et al. (2020).[19]

A challenge in the system design of CPS is that an attacker can potentially have different entry points to manipulate, destroy or steal physical assets or data assets (Wang et al., 2010; Möller et al., 2019, pp. 306, 362-368). This is different from the purely physical approach assuming a ground-based attacker: this attacker must overcome physical barriers along an attack path one after the other from the first to the last barrier (Lichte et al., 2016). Due to the networking of physical and logical components[20] , an attack can lead to interactions with other components, which can influence the functionality of the overall system (Mo et al., 2011). Security measures of physical or IT barriers can, depending on the attack scenario, be completely undermined in the worst case and threaten key properties and key functions of the CPS (Koscher et al., 2010). It is therefore important to understand which paths an attacker can take to reach their target (Möller et al., 2019, p. 319). The networking problem is presented in Mo et al. (2011) in the context of intelligent power grids (so-called smart grids). System-theoretical approaches are compared in Mo et al. (2011) with approaches for modeling and assessing cybersecurity contributions (see Figure 10).

[19] Number of publications analyzed: n = 62.

[20] The logical layer comprises all the processing mechanisms of a specific application. IT components are required to enable processing.



	Cybersecurity	System Theoretic Security
System Model	WAN/NAN/HAN model	Power Flow Model Sensor Model
Requirements	Confidentiality Integrity Availability	Robust to Prespecified Contigency Accurante State Estimation
Attack Model	DoS Attack Network-based Intrusion ...	Contingencies Sensor Failures, False Data Injection
Countermeasures	Key Management Secure Communication System and Device Security	Contigency Analysis Bad Data Detection

Figure 10: Approaches to modeling and assessing CPS.
Source: Mo et al. (2011).[21]

Cybersecurity modeling approaches and systems theory approaches are used in Mo et al. (2011) to determine the detection rate of sensor failures considering an attack. The approach chosen in Mo et al. (2011) is similar to a fault-tolerant control. Möller et al. (2019, pp. 272-273) also consider five security concepts that can help users to avoid the successful realization of a threat scenario for cybersecurity-relevant components. These include "Artificial Intelligence", "Control Theory", "Epistemic Theory", "Game Theory" and "Graph Theory". A discussion of the detection and localization of attacks can be found in Pasqualetti et al. (2013). Pasqualetti et al. (2013) use the Unified Modeling Language (UML) as a model framework. CPS security is described as a control engineering problem. In Konstantinou et al. (2015), data protection issues are also examined at various cyber-physical system levels. The application areas of smart homes and critical infrastructures (KRITIS) are considered in this context. Cyber-physical attack models are developed in Teixeira et al. (2015). The starting point for this is the cyber-physical attack space (see Figure 11).

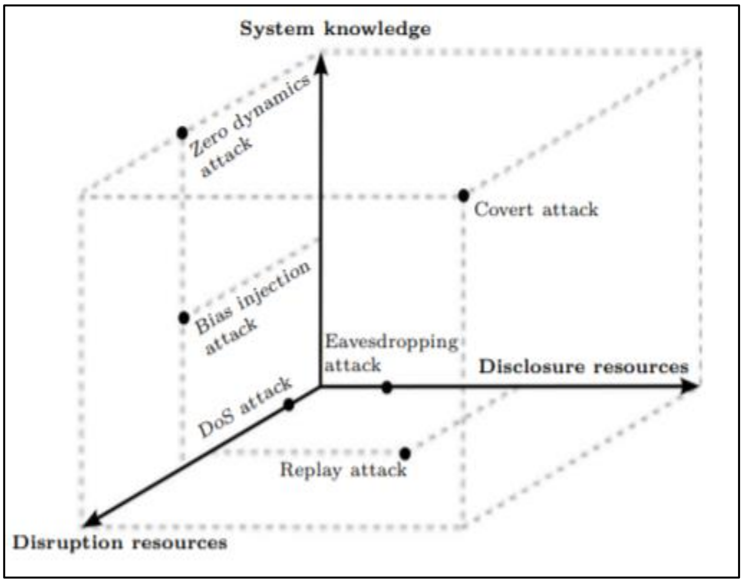


Figure 11: Cyberphysical attack space.
Source: Teixeira et al. (2015).

[21] WAN := Wide Area Network, NAN := Near Area Network, HAN = Home Area Network, DoS := Denial of Service.

Compared to pure IT infrastructures, the (additional) physical components in CPS add considerable complexity, which makes a security assessment more difficult (Rajkumar et al., 2010): On the one hand, the increase in complexity means more effort for the attacker to understand the system, but on the other hand, there are also more gateways for attackers and thus real-time requirements that must be taken into account in the system design. According to Martins et al. (2015), this requires more effort on the part of the defenders in order to be able to protect themselves adequately. A generic framework for assessing CPS security is proposed in Humayed et al. (2017) (see Figure 12). In this framework, CPS are divided into cyber, cyber-physical and physical components. The three components are assessed qualitatively with regard to the parameters of threats, vulnerabilities, attacks and controls.

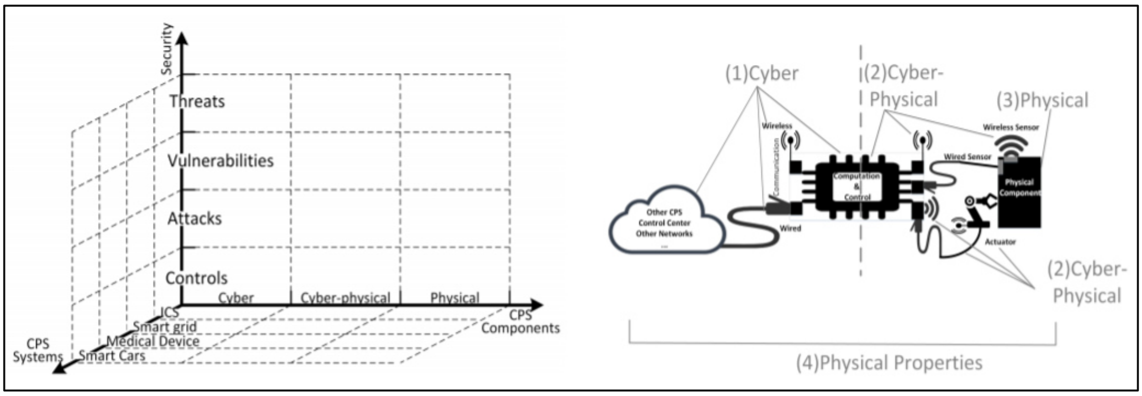


Figure 12: CPS security risk framework.
Source: Humayed et al (2017).

Humayed et al. (2017) also analyze potential sources of threats in the application areas of smart grids, smart cars and medical devices. Vulnerabilities are also explained and the causes of these vulnerabilities are identified using specific examples. Subsequently, Humayed et al. (2017) define security measures for identified, abusive scenarios. The assignment of measures to scenarios is similar to the risk register according to Harnser (2010, B7, p. 71) from the physical security assessment. In contrast to previous scientific contributions, Aigner & Khelil (2020) analyze the applicability of selected security metrics for the risk assessment of CPS. To conduct an analysis of the applicability of specific security metrics for CPS use cases, Aigner & Khelil (2020) first define a series of guiding questions. An example of a key question is: "Can the metric handle the interaction of heterogeneous systems within a CPS environment?" (Aigner & Khelil, 2020, p. 2). In Aigner & Khelil (2020), the key questions are applied to the security metrics under consideration, i.e. it is checked whether the key questions can be answered using the metrics. A total of twelve security metrics are considered, whereby a distinction is made between attack detection metrics, system design metrics and security rating metrics (see Figure 13).

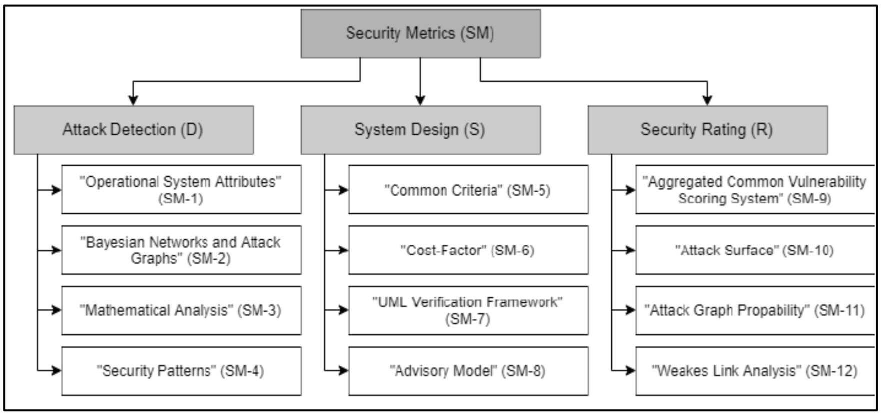

Security Metrics (SM)
Attack Detection (D)
System Design (S)
Security Rating (R)
"Operational System Attributes" (SM-1)
"Bayesian Networks and Attack Graphs" (SM-2)
"Mathematical Analysis" (SM-3)
"Security Patterns" (SM-4)
"Common Criteria" (SM-5)
"Cost-Factor" (SM-6)
"UML Verification Framework" (SM-7)
"Advisory Model" (SM-8)
"Aggregated Common Vulnerability Scoring System" (SM-9)
"Attack Surface" (SM-10)
"Attack Graph Propability" (SM-11)
"Weakes Link Analysis" (SM-12)

Figure 13: Comparative analysis of security metrics for suitability for CPS assessment.
Source: Aigner & Khelil (2020).

The results of the benchmark by Aigner & Khelil (2020) are presented in the form of a matrix, below using the example of the attack detection metrics (see Table 4): The number of questions answered is counted in each case, divided by the total number of questions asked. The result is multiplied by the number 100 to obtain the percentage of answered questions. As Table 4 can be seen, the security metric (SM) "4" (Security Patterns) can be used to answer all seven key questions posed to the metric. In contrast, only 14 % of all selected questions can be answered with SM "1" (Operational System Attributes), for example. It should be noted that not every question is applied to every metric and that not all thirteen questions defined at the beginning can be answered using the metrics (see Figure 14). This shows the qualitative strengths and weaknesses of available security metrics.

Question	SM-01	SM-02	SM-03	SM-04
Q-7	N	N	N	Y
Q-8	N	Y	N	Y
Q-9	N	N	N	Y
Q-10	N	Y	N	Y
Q-11	Y	Y	Y	Y
Q-12	N	Y	N	Y
Q-13	N	Y	N	Y
Total	1	5	1	7
Total (%)	14 (1/7)	71 (5/7)	14 (1/7)	100 (7/7)

Table 4: Results of the benchmark of the attack detection metrics.
Source: Aigner & Khelil (2020).

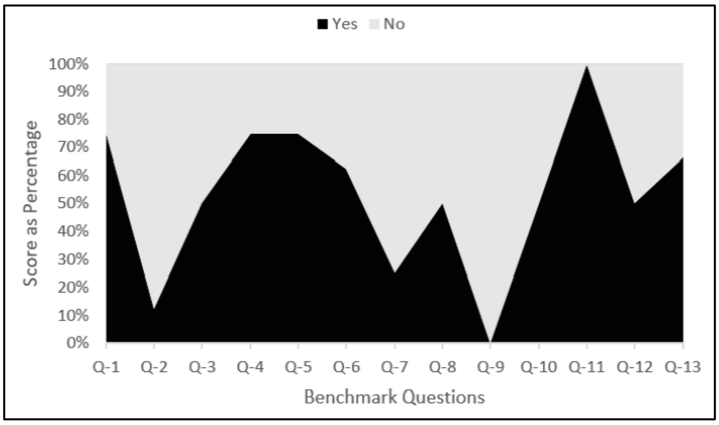


Figure 14: Total benchmark scores by question.
Source: Aigner & Khelil (2020).

The sub-benchmarks according to individual metric types are merged into an overall benchmark (Aigner & Khelil, 2020) (see Figure 15). The result provides a ranking of the applicability of the metrics considered for the risk assessment of CPS (here in descending order): SM 4, SM 2, (SM 5, SM 7, SM 9, SM 10, SM 11), (SM 6, SM 8, SM 12), SM 3, SM 1.

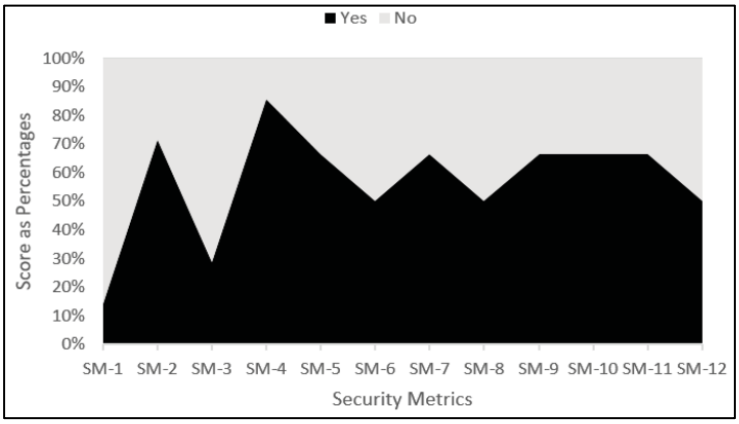
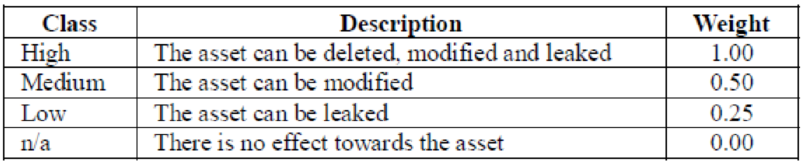


Figure 15: Overall benchmark on security metrics for CPS.
Source: Aigner & Khelil (2020).

From the analysis results in Aigner & Khelil (2020), it is concluded that a combination of different metrics is required for the risk assessment of CPS. The following option is mentioned in Aigner & Khelil (2020): The approach of aggregated CVSS scores (SM "9") can be extended by the concept of attack surfaces (SM "10") and coupled with probability aspects from SM "11" (Aigner & Khelil, 2020). The need to combine different approaches to enable a cross-domain risk assessment is also emphasized in Macher et al. (2020a). A framework for quantifying security in CPS applications is proposed in Aigner & Khelil (2021). This metric is intended to assess interactions between IT assets. First, assets are scored in Aigner & Khelil (2021). A score category is assigned a numerical value between "0" and "1", similar to the CVSS scoring scheme. After the asset scoring (see exemplary Table 5) is followed by the scoring of the "Impacts", the scoring of the "Attackers" and the scoring of the "Mitigations".



Class	Description	Weight
High	The asset can be deleted, modified and leaked	1.00
Medium	The asset can be modified	0.50
Low	The asset can be leaked	0.25
n/a	There is no effect towards the asset	0.00

Table 5: Asset assessment, effect scoring.
Source: Aigner & Khelil (2021).

In contrast to the approaches already presented, Aigner et al. (2021) do not only consider the effects of a specific attack on a single system. The existing system types within a CPS and several attack scenarios (here: attack vectors) are also analyzed (see Figure 16).

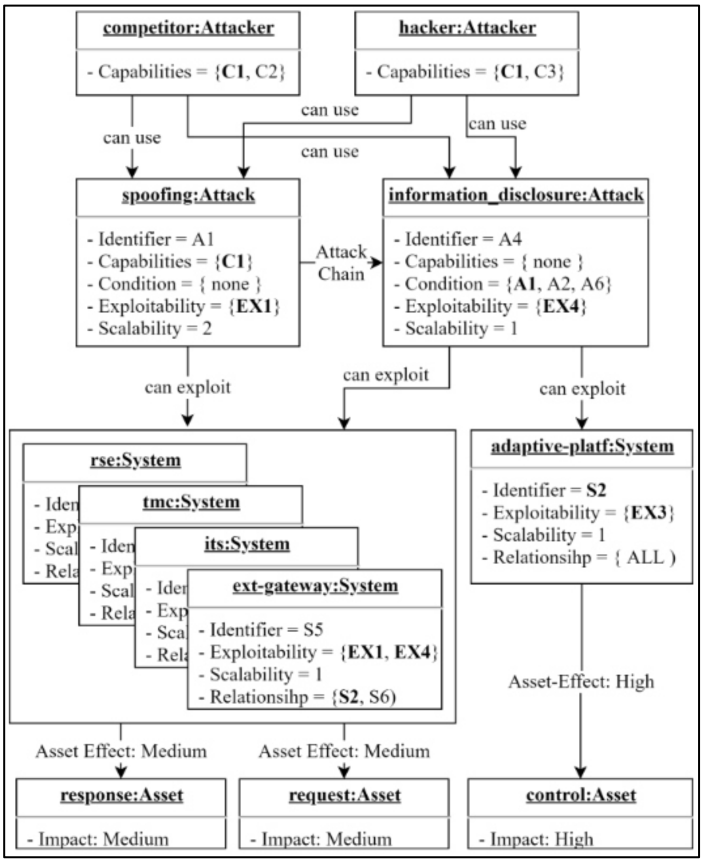


Figure 16: Risk assessment process according to Aigner & Khelil (2021).
Source: Aigner & Khelil (2021).

The calculation matrix for determining the security score (see Figure 16 below) shows that numerical values that are written after the descriptors of an assessment parameter are, for example, added together and also multiplied in the course of the risk assessment process. The metric proposed in Aigner & Khelil (2021) involves ordinal values (such as "High" or "Medium"). However, the ordinal scale only allows rankings (higher and lower; see chapter 2.4). In Aigner & Khelil (2021), the descriptors are still assigned numerical score values between "0" and "1". However, the approach lacks a justification for the choice of numerical values.

The assessment of interactions between threat scenarios is also being discussed in the CVSS community. A work item sheet collects suggestions for improvement for "Version 4" of the CVSS metrics (currently available in version 3.1, see First.org (2022)) (CVSS Work Items, 2022). Some of them originate from the publication by Spring et al. (2018). In two contributions to the work item sheet entitled "Measure physical "kinetic" outcome of an exploited vulnerability" and "Measure up-stream and/or down-stream "collateral damage" impacts", it is proposed that the effect of a successful IT attack on the physical domain or the effect of a physical attack on the IT domain be described by the "kinetic impact": "Explore a new metric to measure the direct up and down stream impact of an impacted component" (CVSS Work Items, 2022, p. 9). A solution for the concrete mapping of the kinetic impact in a metric is not presented in detail.

In IT security, a classic approach to identifying and categorizing threat scenarios is STRIDE (S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege) (Microsoft Corporation, 2005). STRIDE was developed in the 1990s by the engineers Koren Kohnfelder and Praerit Garg at Microsoft. It is used by security experts to answer the question: "What can go wrong in the system under consideration?". STRIDE is comparable to the what-if technique as used in the physical security assessment according to Harnser (2010, B1, pp. 4-6). The what-if technique asks what functional effects can arise if a system element is mentally removed from the system. Threat modeling with STRIDE can be seen as a security counterpart to the Hazard Analysis and Risk Assessment (HARA) from ISO 26262 (Macher et al., 2015). In Macher et al. (2015), it is proposed to combine STRIDE and HARA into a new quantitative approach, the Security-Aware Hazard and Risk Analysis Method (SAHARA).

SAHARA aims to quantify security threats according to the resources (R) and know-how (K) required to conduct an attack, as well as the criticality of the threat (T). R, K and T are each scored (see Table 6) and arranged in a matrix in a similar way to the determination of the ASIL from safety (ISO 26262-3:2018) (see Table 7). As Table 6 on the right-hand side, the threat criticality corresponds to an impact category.

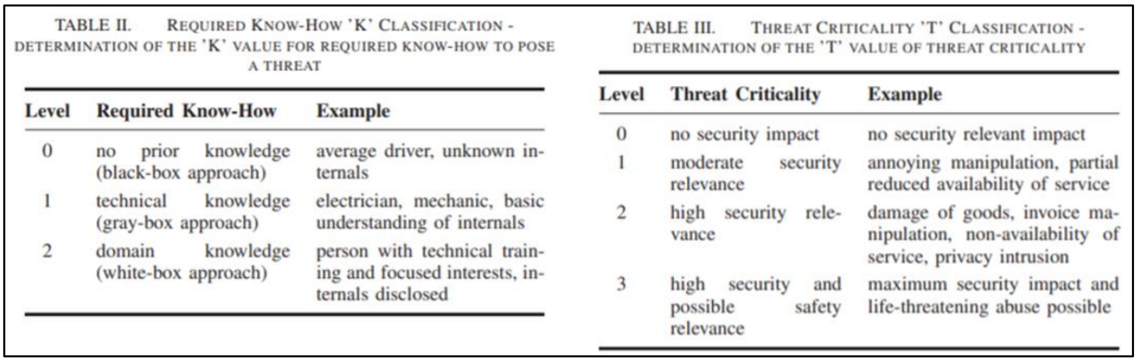


TABLE II. REQUIRED KNOW-HOW 'K' CLASSIFICATION - DETERMINATION OF THE 'K' VALUE FOR REQUIRED KNOW-HOW TO POSE A THREAT

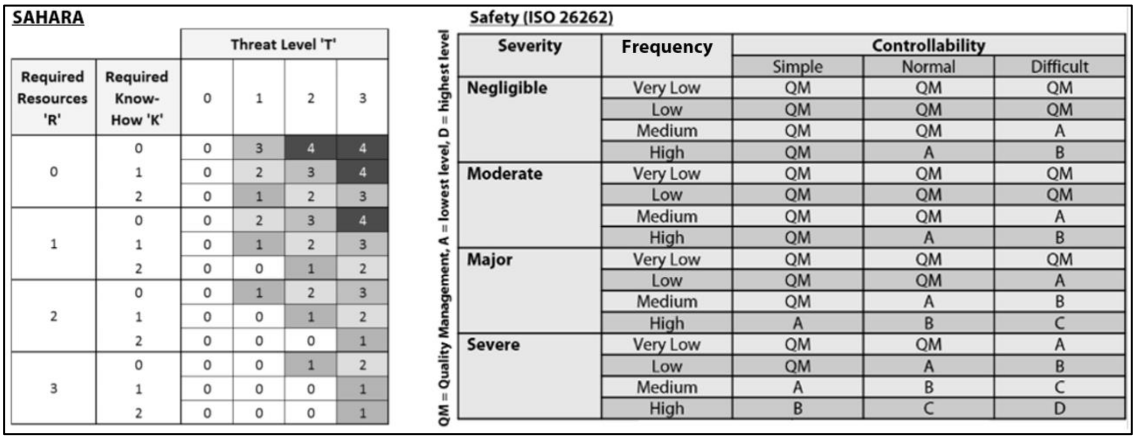
Level	Required Know-How	Example
0	no prior knowledge (black-box approach)	average driver, unknown internals
1	technical knowledge (gray-box approach)	electrician, mechanic, basic understanding of internals
2	domain knowledge (white-box approach)	person with technical training and focused interests, internals disclosed

TABLE III. THREAT CRITICALITY 'T' CLASSIFICATION - DETERMINATION OF THE 'T' VALUE OF THREAT CRITICALITY

Level	Threat Criticality	Example
0	no security impact	no security relevant impact
1	moderate security relevance	annoying manipulation, partial reduced availability of service
2	high security relevance	damage of goods, invoice manipulation, non-availability of service, privacy intrusion
3	high security and possible safety relevance	maximum security impact and life-threatening abuse possible

Table 6: Classification of know-how and threat criticality according to the SAHARA approach.
Source: Macher et al. (2015).

Each combination of R, K and T represents a security level (SecL) between "0" (lowest level) and "4" (highest level). In the assessment approach, ordinal values are arranged in a matrix. Each R-K-T triplet results in a security level: "The SecL determination is based on the ASIL determination approach". And further: "In case of a safety-related security threat, the SecL is directly converted into an ASIL and related to one or more safety goals, which might be violated by the threat" (Macher et al., 2015, p. 4). In the work by Macher et al. (2015), the SecL is therefore assigned directly to the ASILs in a 1:1 ratio: "SecL 0 - Quality Managed (QM), SecL 1 - ASIL A, SecL 2 - ASIL B, SecL 3 - ASIL C, SecL 4 - ASIL D" (Macher et al., 2015, p. 4). However, the assessment of R, K and T only allows a ranking. It is not possible to draw any further conclusions. Because this is the case, it is not possible to say how much better security level "4" is than security level "2". However, a quantitative approach would allow this. In the case of a proper quantitative approach, it would be possible to compare the assessment variables and also the SecL in terms of size and distance (see also chapter 2.4). In addition, the SAHARA approach leaves open the question of which exploitability level the SecLs are based on in each case and to what extent they can be reduced by applying suitable security measures.



SAHARA

Required Resources 'R'	Required Know-How 'K'	Threat Level 'T'			
		0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

Safety (ISO 26262)

QM = Quality Management, A = lowest level, D = highest level

Severity	Frequency	Controllability		
		Simple	Normal	Difficult
Negligible	Very Low	QM	QM	QM
	Low	QM	QM	QM
	Medium	QM	QM	A
	High	QM	A	B
Moderate	Very Low	QM	QM	QM
	Low	QM	QM	QM
	Medium	QM	QM	A
	High	QM	A	B
Major	Very Low	QM	QM	QM
	Low	QM	QM	A
	Medium	QM	A	B
	High	A	B	C
Severe	Very Low	QM	QM	A
	Low	QM	A	B
	Medium	A	B	C
	High	B	C	D

Table 7: Security level according to SAHARA (left) compared to ASIL from ISO 26262-3:2018 (p. 10) (right).
Source: Macher et al. (2015) (left); own table based on ISO 26262 (right).

Studies have already been conducted on the application of a TARA for automotive networked embedded systems (Dobaj et al. 2021). Dürrwang et al. (2021) present an approach for automating the TARA process and the security testing of a vehicle network. Dürrwang et al. (2021) introduce the concept of Attacker Privilege to describe states in which attackers can carry out certain attacks. Required Privilege Levels are divided into a total of five levels (see Figure 17). Each identified attack path from the TARA is assigned a Required Privilege Level (PL). Dürrwang et al. (2021) argue that the Required Privilege Levels can serve as a basis for security testing. In Macher et al. (2020a), a TARA is conducted using the example of an electronic steering column locking system. In the course of the TARA in Macher et al. (2020a), a structured method for the integration of cybersecurity and functional safety in the context of Automotive SPICE is applied.

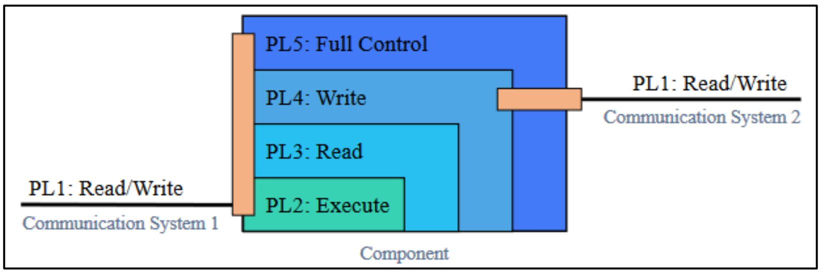


Figure 17: Required privilege levels.
Source: Dürrwang et al. (2021).

In summary, various approaches are being pursued to analyze and assess physical risk contributions and IT risk contributions in the context of cyber-physical use cases. However, research into the current state of the scientific debate on CPS security reveals a need for research into the analysis and assessment of interactions between the two domains. Previous CPS assessment approaches are largely qualitative, descriptive in nature and at an abstract meta-level, which do not take physical vulnerability into account. Aigner & Khelil (2021) even define a framework for assessing the security of CPS that takes up the key IT characteristics of CPS and is based on the industry standard Common Vulnerability Scoring System (CVSS; First.org, 2022). However, the effectiveness of physical security mechanisms is not considered. Furthermore, inherent distortions in the application of the proposed semi-quantitative metric can be identified, such as calculating with values on an ordinal scale. In conclusion, there are no quantitative approaches to synthesize physical security and IT security. As can be seen in the state of research on cyber-physical security, there is a need for research in the reduction of distortions within metrics and in the reduction of incompatibilities between metrics. Both in science and in industry, a solution approach for the consistent merging of metrics from the domains of physical security and IT security or functional safety and IT security is required. This need for research is addressed in this research work. The focus of this work is the cross-domain assessment of physical security and IT security.

2.3 Security and Risk

System security can be viewed from the user perspective, the operator perspective and the insurer perspective (Wheeler, 2018, p. 18, 50; Harnser, 2010, p. 1; Gordon et al., 2003). There is a duality of safety and security, which forms the foundation for risk analysis. In German usage, however, these are combined under a single term, “Sicherheit”. In English-speaking countries, this is clearly differentiated (Newsome, 2013, p. 7; Geiger, 2021). Safety is used to analyze how the system affects people or the environment (Burns et al., 1995). Accidents are caused by events that can be traced back to dangerous system conditions. In contrast to safety, security analyzes the effects of an attack on a system (Wheeler, 2011, p. 6). Safety therefore refers to the protection of a person from a technical system, while security describes the protection of a technical system from a person (Wurm, 2022, p. 70). Attackers can be extrinsic (hackers, terrorists, burglars, etc.) or intrinsic (e.g. angry employees) (Harnser, 2010, B2, p. 16). Threat vectors in the context of CPS can be physical or digital (Kofler et al., 2018, p. 32). Since MAS are categorized as CPS, both threat vectors apply to these systems. The consequences of threats that have occurred are similar in safety and security. One cause of consequences in safety is, for example, technical failure of hardware (Zio, 2007, p. 1). This type of failure is stochastic and the probability of occurrence can be determined, for example, by fatigue tests (Bertsche & Lechner, 2006, pp. 7-8).

The failure behavior can be represented by failure curves (Zio, 2007, p. 50). Human errors in the form of operating errors are further causes of failures. This type of failure is not consistently stochastic. In this case, experiments can be used to estimate how likely operating errors are (Ritz, 2015, pp. 26, 28, 110). In security, on the other hand, there are deliberate attacks on a technical system or a person (Wheeler, 2011, p. 18). Here, it is more difficult to estimate the frequencies due to the arbitrariness of an attacker (Wheeler, 2011, pp. 58, 70). In addition, no historical references for attacks are yet available for new systems. In security, a prospective analysis based on scenarios is therefore traditionally used (Harnser, 2010, B4, p. 50). Due to the many uncertain parameters involved, conducting a risk assessment is a challenge.

The concept of risk "is [...] a vague notion that carries different meaning under different domain contexts and perspectives." (Wang et al., 2011, p. 1). "Risk is unobservable but we can indirectly measure its realization as losses" (Woods et al., 2021, p. 1). From a security perspective, risk can be understood as an expected extent of damage that is influenced by the probability of occurrence and the severity of damage (Harnser, 2010, B6, p. 64) (see Figure 18). When determining probability, there are basically two directions of statistical thinking, the Bayesian perspective (degree of conviction) and the frequentist perspective (objective probability: temporal frequency) (Vallverdú, 2008).

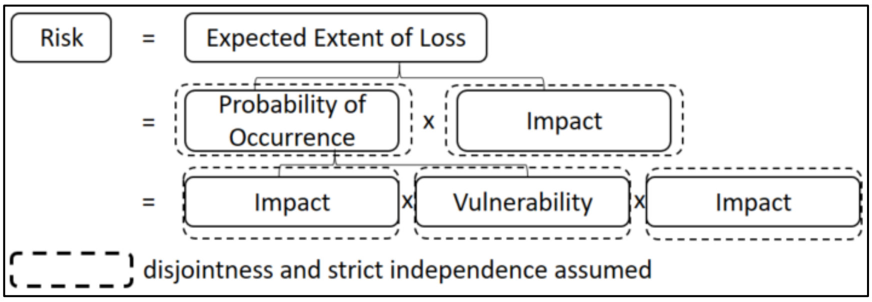

Risk
=
Expected Extent of Loss
=
Probability of Occurrence
x
Impact
=
Impact
x
Vulnerability
x
Impact
disjointness and strict independence assumed

Figure 18: Two- and three-tier risk model.
Source: Own Figure based on Lichte et al. (2017).

Impacts can also be monetized. This means that they are expressed in monetary terms (Harnser, 2010, B3, pp. 39-41). Monetization is necessary in order to be able to compare different risks. In this two-part risk definition, probabilities of occurrence are linked to effects, but multiplication does not always have to link the two risk contributions[22] with each other. If the events of the risk contributions are disjoint (incompatible), this means that there is no common intersection for the events of probability of occurrence and loss. Causality between the risk contributions is excluded in this idealization, i.e. the probability of occurrence and the loss are strictly independent of each other. In such a case, the risk can be written as the product of the individual probability and the extent of the loss.

In the domains of physical security and IT security, the probability of occurrence is further divided into threat and vulnerability (Lichte et al., 2017; Cheng et al., 2014, p. 4). The threat is the probability that an attack will be conducted by an attacker with a specific tool. In security, for example, sabotage or attacks are primarily analyzed, whereas in functional safety, accidents caused by component failure or human error are considered (see Figure 19). Traditionally, a frequentist view is adopted for the threat (e.g. 15 attacks per year). Because in the case of this work, worst-case scenarios are considered for new systems that have not yet occurred, a frequentist view is difficult to depict. What can be done, however, is to adopt a Bayesian view (degree of belief) (Witte et al., 2020). In contrast to physical security or IT security, the probability of a threat occurring in functional safety can be quantitatively assessed using statistical methods.

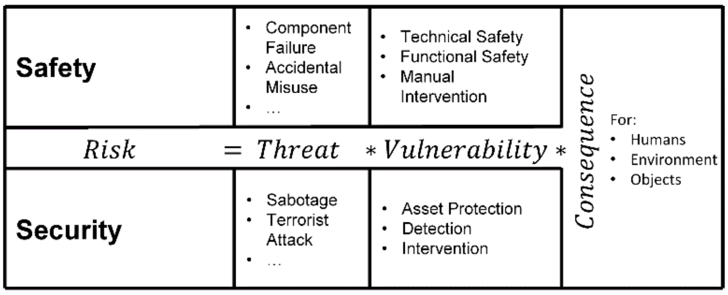


Figure 19: Holistic risk definition of safety and security.
Source: Lichte et al. (2017).

Vulnerability comprises the probability of a successful attack. Disjointedness and strict independence allow the individual risk contributions to be analyzed and assessed separately, e.g. (aleatory) uncertainties[23] in vulnerability have no cause-and-effect relationships with the

[22] The probability of occurrence and the effects are, for example, risk contributions. A risk contribution indicates the share of the respective risk contribution to a risk in the form of a quantitative value. The identification and analysis of individual risk contributions are important so that safety or security measures can be developed to reduce the probability of occurrence and the impact.

[23] Aleatory uncertainties arise from natural and random fluctuations.

(epistemic) uncertainty[24] in the threat probability or the impact. This facilitates the risk assessment because uncertain variables, e.g. those that are strongly epistemic, can be excluded. If there are disjunctive events, then threat, vulnerability and impact can be assessed in isolation and combined into a risk assessment after the individual considerations. The risk is usually calculated as the product of all three risk contributions. If the assumptions are made that

a) threat, vulnerability and impact are completely disjoint, and strict independence is assumed for this ideal case,
b) a system is assessed in the event of an attack (worst-case scenario; P(threat) = 100 % as the degree of conviction),

then the risk description "Risk = Threat · Vulnerability · Impact" can be simplified (see Eq. (1)):

$$\begin{aligned} &\text{Risk} = \text{Threat} \cdot \text{Vulnerability} \cdot \text{Impact} \mid_{\text{Assumption: Attack case, P(threat) = 100\%}} \\ &\text{Risk} = 100\ \% \cdot \text{Vulnerability} \cdot \text{Impact} \\ &\text{Risk} = 1 \cdot \text{Vulnerability} \cdot \text{Impact} \\ &\text{Risk} = \text{Vulnerability} \cdot \text{Impact} \end{aligned} \tag{1}$$

It should be noted that the mere multiplication of vulnerability and impact without taking the threat into account is not synonymous with risk. Without the threat component, risk is merely a vulnerability weighted with the impact. Risk, however, measures how likely the occurrence of a generally undesirable event is (consisting of a threat component and a vulnerability component) and how great the potential damage is if this event occurs (Lichte et al., 2016). The threat probability is therefore an essential component of a risk assessment. Consequently, all three risk contributions - threat, vulnerability and impact - must be considered in order to develop risk-appropriate metrics. However, this research focuses on the comparison of metrics for assessing vulnerability and impact in physical security and IT security. For this purpose, the simplification from Eq. (1) is taken as a basis.

The greater the impact, the greater the operator's interest in reducing the threat probability and vulnerability (Harnser, 2010, B3, pp. 39-41). In physical security risk assessment, it is common practice to assess the vulnerability part of the three-part risk model. On the one hand, vulnerability can be used to assess the effect of the properties of a security measure in terms of vulnerability reduction in specific scenarios (Garcia, 2005, p. 20). On the other hand, an operator can carry out cost-benefit analyses on the basis of a vulnerability assessment (Wheeler 2011, p. 8). From a defense perspective, vulnerability is the control instrument in security risk assessment. Both in physical risk assessment, e.g. according to Lichte et al. (2016) or Garcia (2005), and in IT risk assessment, e.g. according to CVSS (First.org, 2022) or OWASP[25] (Williams, 2022), risk is classically assessed on the basis of vulnerability contributions and impact contributions; provided that it is assumed that the system is also attacked or a vulnerability is exploited (see Eq. (1)).

Metrics for threat, vulnerability and impact must be introduced for the assessment of risks. These describe the individual risk contributions. Models are also required that are linked to specific boundary conditions and expert knowledge (Bandow & Holzmüller, 2009, p. IX). In contrast to the risk assessment of critical infrastructures (KRITIS), where environmental boundary conditions are largely static, and the use case-specific dynamics must also be taken into account in the security risk assessment of MAS (Möller et al., 2019, pp. 304-306). Use case-specific boundary conditions make the measurement of risks and the recording of uncertainties even more complicated, which is why a well thought-out approach is required to conduct a threat analysis and risk assessment of such systems.

[24] Epistemic uncertainties arise from incomplete knowledge.
[25] OWASP: Open Web Application Security Project.

2.4 Metrics

Metrics are the starting point for measuring risks (Wheeler, 2011, pp. 38, 39, 229). A metric is a method for measuring quantifiable units or quantities (Sowa, 2011, p. 4; Stephens, 1946). It is a decision-making tool for management to improve safety and security (Arabsorkhi & Ghaffari, 2018). "The main task of metrics is to use indicators to make the status and impact of influencing factors [...] visible, comparable, assessable and traceable" (Broy et al., 2013, p. 334). In Katsikas et al. (2005), the main objective of metrics is defined as follows: "The overall aim [of using metrics] is to simplify a complex socio-technical system into models and further to numbers, percentages or partial orders" (Katsikas et al., 2005, p. 150). In Cheng et al. (2014), the aim of security metrics is described as follows: "The ultimate aim of security metrics is to ensure business continuity (or mission success) and minimize business damage by preventing or minimizing the potential impact of [...] incidents" (Cheng et al., 2014, p. 3).

The National Institute of Standards and Technology (NIST) defines metrics as tools to facilitate and improve decision-making by collecting, analyzing and reporting relevant performance-related data (Cheng et al., 2014, pp. 2-3). To improve product security, a security assessment is necessary because "If you can't measure it, you can't manage it" (Drucker, 2015, p. 685). A useful assessment depends on the choice of an appropriate metric (Arabsorkhi & Ghaffari, 2018). Useful means that management can make good decisions regarding the investment of resources in security measures. To do this, it is necessary to understand which properties a metric must have in order to create a good basis for decision-making. Arabsorkhi & Ghaffari (2018) set out two ways of categorizing the required properties of a good security metric, CORES and PRAGMATIC. CORES comprises a total of five criteria:

- Clarity: Easy to interpret
- Objectiveness: Uninfluenced by personal opinion
- Repeatability: Achievement of the same results under the same assessment conditions
- Easiness (simplicity): Ease of use of the assessment metric
- Succinctness (conciseness): Accuracy of the assessment metric or benefit for the target group

PRAGMATIC, on the other hand, consists of nine properties:

- Predictive (predictability): Good prediction of results
- Relevant (significance): The metric assesses security aspects
- Actionable (usability): The metric supports decision-making
- Genuine (authenticity): Unambiguity and correctness of the information fed into the metric.
- Meaningful (significance): Easy to interpret
- Accurate (precision): Accuracy of the results
- Timely: Minimizing the time between data collection and data assessment
- Independent: Complete, verifiable and correct
- Cheap (cost-effectiveness): Analysis of the metric is associated with low, capacitive effort.

Broy et al. (2013, p. 336) define the following principles in the field of software engineering that a good metric must fulfill: objectivity, measurement accuracy, meaningfulness and suitability, comparability, appropriateness of effort and usefulness. The required properties of the three options mentioned for describing good security metrics can be assigned to each other, as illustrated in Table 8.

CORES	PRAGMATIC	Software Engineering
Clarity: Easy to interpret	Actionable: The metric supports decision-making; Meaningful: Easy to interpret	Significance and suitability, usefulness
Objectiveness: Uninfluenced by personal opinion	Independent: Complete, verifiable and correct	Objectivity
Repeatability: Achievement of the same results under the same assessment conditions	Predictive (predictability): Good prediction of results Timely: Minimizing the time between data collection and data assessment	Comparability
Easiness (simplicity): Ease of use of the assessment metric	Cheap (cost-effectiveness): Analysis of the metric is associated with low, capacitive effort.	Reasonableness of the effort
Succinctness (conciseness): Accuracy of the assessment metric or benefit for the target group	Relevant (significance): The metric assesses security aspects Genuine (authenticity): Unambiguity and correctness of the information fed into the metric. Accurate (precision): Accuracy of the results	Measuring accuracy

Table 8: Assignment of metric properties.
Source: Own table based on Broy et al. (2013) and Arabsorkhi & Ghaffari (2018).

Security metrics should not only fulfill the aforementioned properties. They must also be aligned with common industry standards and business objectives (Cheng et al., 2014, p. 2). Metrics should be able to record defined properties of a product, a development process or a project so that the fulfillment of requirements on the part of the customer or internal management can be checked (Broy et al., 2013, p. 335). This requires the measurement of influencing variables on the requirements criteria. According to Hubbard et al. (2016), in decision sciences a measurement is "a quantitatively expressed reduction of uncertainty based on one or more observations. [...] A measurement is, ultimately, just information [that is processed within a metric]" (Hubbard et al., 2016, p. 21). According to Hubbard et al. (2016), "Uncertainty" is "the lack of complete certainty, that is, the existence of more than one possibility. The "true" outcome/state/result/value is not known" (Hubbard et al., 2016, p. 29).

The fact that different variables are at the forefront of measurement means that there are different views of metrics. Broy et al. (2013, p. 335) differentiate between the management view (customer satisfaction, costs, productivity), the developer view (efficiency, maintainability) and the customer view (adherence to delivery dates, cost compliance, product quality, safety and security). In order to select a suitable metric, the functionality of a metric and its respective scope of application must be understood (Arabsorkhi & Ghaffari, 2018). The scope of application describes what is assessed and to what extent (for whom) (Broy et al., 2013, p. 336). There are a variety of metrics for assessing security, such as those presented in Sowa (2011), Wang et al. (2017), Arabsorkhi & Ghaffari (2018) or Cheng et al. (2014). In Broy et al. (2013), a general warning is issued with regard to the use of metrics: "Even if a metric uses complicated formulas, this says nothing about the validity of the resulting figures with regard to the measured variable" (Broy et al., 2013, p. 338).

Metrics can be qualitative, semi-quantitative or quantitative (Newsome, 2013, pp. 104-106) (see Figure 20). The qualitative assessment corresponds to compliance, i.e. there is a list of necessary elements that are successively checked for presence and ticked off (Harnser, 2010, B4, p. 46). It serves to ensure that no security measure is forgotten in the system design.

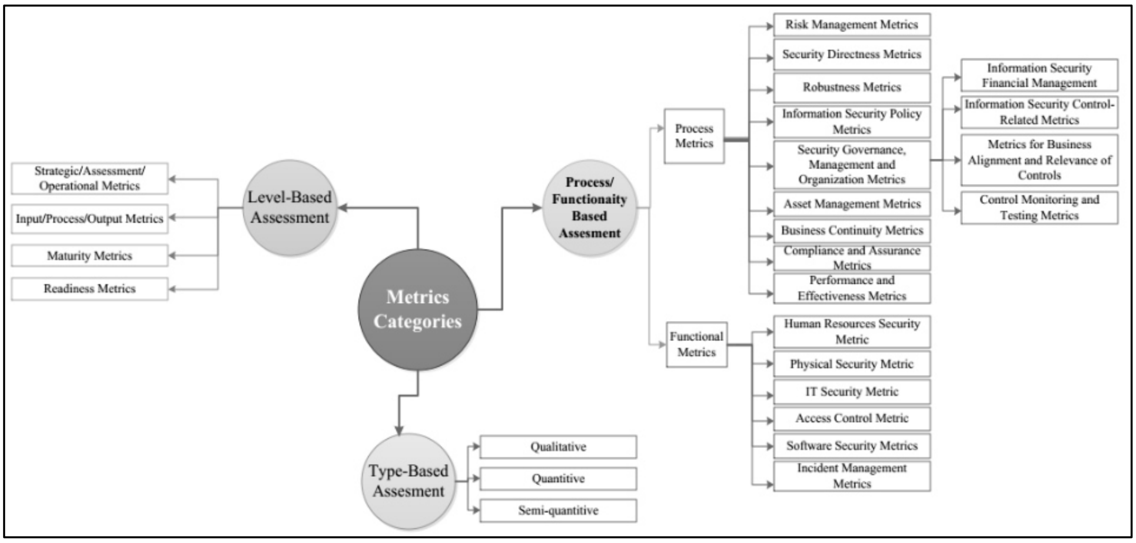

Strategic/Assessment/ Operational Metrics
Input/Process/Output Metrics
Maturity Metrics
Readiness Metrics
Level-Based Assessment
Metrics Categories
Process/ Functionaity Based Assesment
Type-Based Assesment
Qualitative
Quantitive
Semi-quantitive
Process Metrics
Functional Metrics
Risk Management Metrics
Security Directness Metrics
Robustness Metrics
Information Security Policy Metrics
Security Governance, Management and Organization Metrics
Asset Management Metrics
Business Continuity Metrics
Compliance and Assurance Metrics
Performance and Effectiveness Metrics
Information Security Financial Management
Information Security Control-Related Metrics
Metrics for Business Alignment and Relevance of Controls
Control Monitoring and Testing Metrics
Human Resources Security Metric
Physical Security Metric
IT Security Metric
Access Control Metric
Software Security Metrics
Incident Management Metrics

Figure 20: Taxonomy of metrics.
Source: Arabsorkhi & Ghaffari (2018).

Essentially, however, the presence of certain barriers ("a fence and a wall are present", for example) says nothing about how good they are at delaying a specific attacker in the application case. If a yardstick is applied that allows statements such as "something is bigger, smaller or the same", then the assessment is semi-quantitative (Newsome, 2013, p. 105). It can only be said, for example, that certain measures are more effective than others, without specifying exactly in absolute figures to what extent ("x times as much"). Qualitative and semi-quantitative approaches are widely used in IT security, e.g. in CVSS (First.org, 2022) or in the Open Web Application Security Project (OWASP) Risk Rating Methodology (Williams, 2022). Quantitative approaches enable the calculation of probabilities of occurrence and monetary costs. Monetary expenses (e.g. losses due to successful attacks) are traditionally linked to the probability of occurrence of a damaging event. In physical security, such an approach is pursued, for example, by using the vulnerability metric according to Lichte et al. (2016).

Metrics can also be differentiated according to application type. Security assessments at top management level can be of a strategic nature. In addition, security assessments are possible at middle management level and at lower management level. Executive metrics are traditionally used at middle management level. Executive metrics relate to corporate process maturity. At the lower level, operational metrics are used to assess the release readiness of hardware and software, for example (Arabsorkhi & Ghaffari, 2018). A third categorization of metrics is possible according to the process or functionality to be assessed. Metrics for measuring physical security and IT security can be assigned to the functional metrics group. Ahmed et al. (2019) differentiate between eight types of IT security metrics: Vulnerability Assessment Metric, Red and Blue Teaming Metric, Indicators of Attack Metric, Resilience Metric, Indicators of Compromise, Penetration Testing Metric, Riks Assessment Metric and Intelligence Drive Defense Metric.

Examples of metrics can be found in various fields of application: Linguistic measures (how something is spoken), structural measures (how something is set up) (Sowa, 2011, p. 2), process measures (how something proceeds) (Torgerson, 2007), system measures (how something is measured) (Grossert, 1989) and probabilistic or statistical measures (how random events are recorded) (Gracia, 2007). The latter is concerned with recording the probability of occurrence of events. System measures and probabilistic or statistical measures are of particular importance in the context of risk analysis. Metrics that are used in the security context to assess situational awareness can also be divided into objective measures, subjective measures, performance measures and behavioral measures (Cheng et al., 2014, pp. 5-6). Scales are a central tool for presenting the results of a measurement (Sowa, 2011, pp. 54, 107-111). A scale or measurement level describes an important property of characteristics in empirical research (Opiera et al., 2016). Empiricism comprises a methodical and systematic collection of data according to specific criteria (Sowa, 2011, p. 58). This is a central part of the risk analysis and risk assessment of CPS. Scales can be systematized according to DIN EN ISO/IEC 27000:2017-10 (DIN e.V., 2018). Scale levels are differentiated into "nominal-scaled", "ordinal-scaled" and "ratio-scaled" (zero point/reference given) (Stevens, 1946; Krisper, 2021) (see Table 9). Nominal scales are used to categorize properties (Hubbard et al., 2016, pp. 22-24). It is possible to determine whether a characteristic occurs more frequently, less frequently or equally frequently. Only frequencies can be measured and therefore displayed. No statement can be made as to whether something ranks higher or lower, worse or better. Only the absolute frequency can be viewed.

If nominal scales are used, the results can be used to determine whether they are equal or unequal. The proportionality of individual categories can be described using the mathematical operators "$= und\ \neq$ " can be used to describe the proportionality of individual categories. The ordinal scale is the increase of the nominal scale; this scale can be sorted (see Figure 21). However, there is no reference point. An ordinal scale can be used to determine an order (e.g. Bundesliga table, where the place is expressed via points and these via certain characteristics). The ordinal scale mathematically provides an extended field in which ranks can be defined using operators ($=, \neq$ resp. $>$ oder $<$). In addition to a frequency specification, a gradation can be made. This type of metric is used in the vulnerability analysis according to Harnser (2010, B4, p. 46) as well as Schwerdtfeger's list of questions according to the Common Criteria (CC) (Schwerdtfeger, 2018). Further mathematical operations are not possible with ordinal values. The use of the ordinal scale does not enable any further knowledge to be gained. A cardinal scale is required for this. It is subdivided into the interval scale on the one hand and the ratio scale on the other.

Scale Type		Measuring Property	Mathematical Operators	Feasible Operation	Position Parameters	Example
Nominal		Frequency	=, ≠	Grouping	Mode	Zip code
Ordinal		Frequency, ranking	=, ≠, >, <	Sorting	Median	Sheet music
Cardinal	Interval	Frequency, ranking, distance	=, ≠, >, <, +, -	Comparison	Arithmetic mean	Date
	Ratio	Frequency, ranking, distance, zero point	=, ≠, >, <, +, -, x, /	Ratio	Geometric mean	Age

Table 9: Scale types and measurable properties within the scale types.
Source: Own table based on DIN e.V. (2018) and Witte (2018, p. 8).

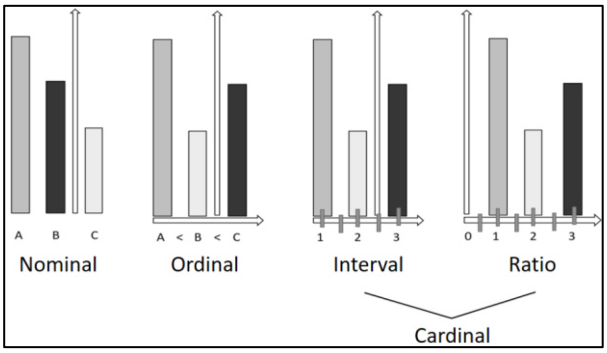


Figure 21: Schematic abstraction of scale types.
Source: Own Figure based on DIN e.V. (2018, p. 8).

With the interval scale, additions and subtractions can be made within the defined intervals (Braband, 2019). It is also possible to determine the distance between individual frequencies. The distance between two measurements can be determined by the user, e.g. by introducing a defined time scale that is continuous with an arbitrarily defined zero point, or by logarithmizing to a base (Braband, 2008). This artificial zero point can be set in different ways, as can be seen, for example, in the comparison of the Chinese calendar with the Islamic calendar or the European calendar. Interval scales can be used to define differences in characteristics. Addition or subtraction shows how far apart something is. The superordinate scale is the ratio scale (Puhani, 2020, p. 9-10). This scale allows the determination of frequency, relative distance and ranking. In addition to the interval scale, a fixed zero point is introduced here. The absolute distance of a frequency can be represented via this natural point. Probability calculation can be realized in particular with this scale form (Lichte et al., 2016). Newsome (2013, pp. 103-107) explains that various authorities and institutions use incompatible scales and incompatible quantitative interpretations of qualitative expressions, such as "frequent" or "unlikely".

An analyst must therefore ask themselves what the requirements of a good metric are and what the weaknesses may be (Krisper, 2021). A good metric generally allows independent consideration of sub-areas of risk. For example, based on the assumptions of the three-part risk model in chapter 2.3 a separate vulnerability analysis can be conducted without affecting the threat or impact (Lichte et al., 2016). A good metric generally allows conclusions to be drawn from sub-areas to the whole. If it is not possible (mathematically) to separate the parameters, the results of a risk assessment are as fuzzy as the most uncertain information in the entire assessment process (Lichte et al., 2020a; Saltelli et al., 2010, Preface). A metric does not have to be able to determine the entire risk, but must allow well-founded decisions to be made on the basis of the decoupled analysis and assessment of sub-areas. A risk assessment with a good metric can lead to a risk-appropriate distribution of scarce resources in measures (Lichte et al., 2019; Cheng et al., 2014, p. 27; Virlics, 2013). When merging the physical security assessment and the IT security assessment, the choice of a suitable metric is a challenge, as described in particular in chapters 2.1 and 2.2 is explained.

2.5 Assessment Approaches in Security

Qualitative and semi-quantitative risk assessment approaches are widely used in both physical security and IT security. Physical security is highly standardized (Walz, 1992; Charter Global, 2020; Schwerdtfeger, 2018). Models and metrics are already established internationally and there are clear guidelines for the design of so-called physical protection systems (PPS) (Garcia, 2005, p. 3). Metrics and models in IT security, on the other hand, are still quite new. In contrast to physical security, there are greater challenges in quantifying vulnerability through attack scenarios (Wang et al., 2017, Preface). Unlike physical security, IT security is still immature:

> Despite the massive investments in information security technologies and research over the past decades, the information security industry is still immature. In particular, the prioritization of remediation efforts within vulnerability management programs predominantly relies on a mixture of subjective expert opinion, severity scores, and incomplete data. (Jacobs et al., 2019, p. 1).

In IT security, for example, the FAIR Institute's Factor Analysis of Information Risk (FAIR) offers an approach for quantifying risk variables (FAIR 2021). However, this presupposes that the so-called loss event frequency can be determined, i.e. that evidence is available. "[...] the main problem [in threat analysis] is that the attacker or attackers are usually not known in advance or only after an attack has taken place and been detected" (Wurm, 2022, p. 33). If scenarios are considered that have not yet occurred, it is difficult to determine the absolute probability (Witte et al., 2020). Hubbard et al. (2016) state:

> Measuring the cyber risk present at an organization is nontrivial, and when you set the requirement of delivering on quantitative measurements rather than subjective and qualitative measurements, it becomes almost beyond daunting. (Hubbard et al., 2016, p. xii).

In Woods et al. (2021), the challenge of quantification in the IT security domain is described as follows:

> Creating knowledge about cyber harms and possible mitigation measures depend on available data. The size of a data-set is not everything as samples must also be representative of the broader population of interest. [...] [For specific compromises], there are no empirical results. (Woods et al., 2021, pp. 12-13).

Aldasso et al. (2016) also state: "However, cyber costs are [also] difficult to quantify" (Aldasso et al., 2016, p. 2). In conclusion, the lack of data is a key hurdle in quantitative assessment. Malavasi et al. (2022) state: "The scarcity of good quality datasets is a common limitation among the many areas of study on cyber risk" (Malavasi et al., 2022, p. 30). Despite the challenges in quantifying IT risk contributions, Hubbard et al. (2016) defend the use of probabilistic approaches as follows:

> Those who agree with the statement that probabilistic methods need exact data misunderstand a basic point in probabilistic methods. We use quantitative, probabilistic methods specifically because we lack perfect information, not in spite of it. If we had perfect information, we would need probabilistic models at all. (Hubbard et al., 2016, p. 102).

Due to the lack of an objective mechanism in IT security that could be used to assess the effect of measures to reduce vulnerability, compliance and scoring-based approaches are widely used. Examples of scoring-based metrics include the CVSS (First.org, 2022), E-Authentication Guidance for Federal Agencies, or OMB M-04-04 for short (NIST, 2021), or assessments based on OMB M-04-04. These include Kantara (Kantara 2021) or InCommon (2013). The latter three approaches are used to assess identity management specifications, whereas CVSS, for example, consists of different metrics that are used to infer a vulnerability score from the exploitability of a system-inherent vulnerability and the impact of an exploited vulnerability: "This score runs from 0.0 to 10.0, in increments of 0.1, giving 101 potential degrees of severity" (Chester, 2021).

In IT security, CVSS version 3.1 is "essentially the way in which vulnerability severities are assessed and ranked. Not everyone agrees that it is a virtuous or effective measurement. It is, however, a measurement in a problem area that defies easy empiricism" (Chester, 2021). CVSS is also proposed in ISO/SAE 21434 as a way to assess the attack feasibility of threat scenarios (ISO/SAE, 2021b, p. 47). Similar to the CVSS metrics are e.g: Microsoft Exploitability Index (MEI, 2021), Security Update Severity Rating System (SUSRS 2021), Red Hat Security Rating (Red Hat, 2021), Stakeholder-Specific Vulnerability Categorization (SSVC, 2021), Exploitability Prediction Scoring System (EPSS, 2021), Vulntology (NIST Vulntology, 2021), DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) (Microsoft, 2021) and the Open Web Application Security Project (OWASP) Rating Methodology (Williams, 2022).

In IT security in particular, it is common practice to conduct a pseudo-quantification in order to assess risks. For example, "Risk Likelihood Factors" are weighted in Kandasamy et al. (2020). Weighting factors for the probability of occurrence and weighting factors for the impact are multiplied together in Kandasamy et al. (2020) to obtain a risk value for a threat scenario. One example of such a "pseudo-quantification" from physical security is the modular Performance Risk-based Integrated Security Methodology (PRISM). The methodology is a key component of the Harnser Reference Security Management Plan (RSMP), which was commissioned by the European Commission (EC) and is intended to improve the security management of critical infrastructures (KRITIS). Among other things, it is based on the DuPont scheme from 1919, a system of key performance indicators used in business administration (Weber et al., 1999). It consists of a threat metric, a vulnerability metric and an impact metric. In the Harnser metric, vulnerability is assessed via the elements of protection, observation and recognition (detection) and reaction (intervention). Different types of score combination, including summation, averaging and product formation, are used to aggregate the risk contributions, consisting of threat components, vulnerability components and impact components, into a risk score.

In IT security, an effectiveness-based assessment is difficult to find. Metrics already exist to enable an effectiveness-based assessment of security measures in physical security: In physical security, the interaction of protection, observation or detection and intervention is mapped quantitatively by an underlying, time-based metric, for example in the vulnerability model according to Garcia (2005) and Lichte et al. (2016). In Garcia (2005), discrete time values are assumed for the three assessment variables. In Lichte et al. (2016), uncertainties are also taken into account by assuming density functions for the valuation parameters. The application of this approach enables the consideration of sharp vulnerability criteria in the security risk assessment:

> The [...] analytic approach shows that vulnerability modeling based on probabilistic methods allows the treatment of the system's inherent uncertainties in assessment. Additionally, the approach theoretically enables a scenario spanning system analysis by using the method of the weakest path and therefore considering the whole system. Going beyond existing methods, this model is suitable for vulnerability optimization.
> (Lichte et al., 2016, p. 7).

An equally time-based approach is also used in the Estimate of Adversary Sequence Interruption (EASI) model and its derivatives (Garcia, 2007, pp. 251-263; Bennett 1977; Bowen et al., 2021). The derivations include, for example, Analytic System and Software for Assessing Safeguards and Security (ASSESS), Forcible Entry Safeguards Effectiveness Model (FESEM), Insider Safeguard Effectiveness Model (ISEM), Safeguards Automated Facility Assessment (SAFE), System Analysis of Vulnerability to Intrusion (SAVI) and Safeguards Network Analysis Procedure (SNAP). The Common Criteria for Information Technology Security Assessment (CC) of the Common Criteria Recognition Arrangement (CCRA) (Herrmann, 2002) are also widely used in IT security assessment. The CCRA is represented in Germany by the Federal Office for Information Security (BSI). It is an internationally recognized collection of security standards for assessing the functionality and trustworthiness of IT systems (CC, 2021). The CC define functional classes, such as communication, protection of user data, cryptography or identification and authentication. The CC specify requirements that are summarized in protection profiles. Protection profiles represent degrees of vulnerability, similar to the physical resistance classes (RC) in accordance with DIN EN 1627-1630.[26]

A total of seven Assessment Assurance Levels (EAL) are distinguished in the CC (CC, 2022). The higher the level, the more a provider can be confident that the functional security require-

[26] The physical hardness level, which is represented by an RC, indicates the respective effectiveness against defined attacker profiles. It depends on the attacker's resistance time and tools.

ments are met based on testing, reviews, etc. In Schwerdtfeger (2018), a list of guiding questions for the assessment of immobile mobile access systems (MAS) is derived on the basis of the CC, the BSI basic protection catalogs and guidelines for physical locking systems. The compliance-based list of key questions can be used to check conformity with the fulfillment of requirements. A high degree of compliance corresponds to a low vulnerability level. Fault tree analysis (FTA, Zio, 2007) is used in functional safety and attack tree analysis (ATA, ISO/SAE, 2021b) in physical security and IT security to identify critical system units and determine the probability of undesired damage events. Attack graph analysis (AGA) is a generalization of attack tree analysis. In the safety case, the event is described by the detected error or the failure of a component (i.e. lack of availability according to the task) (Zio, 2007, p. 115). The ATA was introduced by Schneider (1999) and focuses on the intention of a potential attacker to achieve a goal (e.g., impairing the availability of a unit according to the task) (Ingoldsby, 2016, pp. 3, 7). The aim of the FTA is to identify a cause of failure, while the ATA is used to investigate (implementation) paths that may be attractive to an attacker (ISO/SAE, 2021b, pp. 75-76). The graphical representation of the interaction of failure events (safety) and attack realizations (security) is based on a top-down approach (Ostrom & Wilhelmsen, 2019, pp. 185-187; Harnser, 2010, B4, p. 50).

The tree display begins with the top event. This is the formulation of the undesired event. Logical links, so-called gates or gates based on Boolean operators (e.g. "and" and "or"), are used to create branches to triggering (causal) events.[27] This allows the diversity of component failure to be mapped in the case of the fault tree (FT) and the diversity of the implementation of an attack in the case of the attack tree (AT). The use of AT or Attack Graphs (AG) in a specific context can be assigned to a metric family, such as Connectivity Metrics, Exploitability Metrics or Attack Vector Metrics (Wang et al., 2017, pp. 144-167). In a connectivity metric, for example, the AG is used to assess the influence of the degree of connectivity of components on security (Wang et al. 2017, p. 153). FT and AT or AG thus also implicitly show how threats are dealt with (Wheeler, 2011, p. 101). The tree structure can therefore be used to map causal dependencies between events. If, for example, discrete probabilities are assigned to the undesired events, they can be used to calculate the probability of a system failure or a successful attack on the basis of Bayesian probability theory. One ATA-based method for risk assessment is RISKEE (Krisper et al., 2019).

Bayesian networks are an extension of fault trees and attack trees. Bayesian networks are a method for representing the dependencies of variables on the basis of Bayesian probability theory (Pearl, 2011; Jansen et al., 2006, pp. 11-13). Real conditions are described using stochastic relationships (Jansen et al., 2006, p. 3). A Bayesian network consists of a graph and conditional probability distributions. It also consists of nodes, which represent variables, and edges, which represent causal dependencies between these variables. These are directed and connect nodes with each other (Jansen et al., 2006, p. 6). They describe the effect of a cause (of a node) on at least one other node. Bayesian networks represent cause-and-effect relationships via conditional probabilities (Pearl, 2011). The investigation of uncertainties is also possible with Bayesian networks. Bayesian networks are used in both security domains. When using this method, it is assumed that probabilities are relative quantities that can be influenced by information or additional information gained over time. This means that Bayesian networks are also suitable for artificial intelligence (AI) applications (Niedermayer, 2008). In particular, the method allows the transfer of expert knowledge into subjective probabilities (Ben-Gal, 2008).

[27] The attack tree is a special form of the attack graph. While events of an implementation branch are isolated in an attack tree, events of an implementation branch can have a cause-effect relationship with another branch in an attack graph.

2.6 Elicitation of Expert Knowledge

2.6.1 Methods

Experts need to be consulted in order to answer safety and security questions (EFSA, 2014, p. 35; Hubbard et al., 2016, p. 66). According to Gabler-Wirtschaftslexikon, expert knowledge includes

> Knowledge and intellectual abilities of individuals whose performance in a particular field is far above average. Expert knowledge usually consists of large amounts of information combined with simplifications, little-known facts, rules of thumb and clever procedures (heuristics) that enable efficient problem solving (in this field). (Gabler, 2021).

Experts are therefore people who have several years of relevant professional experience. According to a survey conducted by the personnel service provider Gulp (2022), experts can be divided into junior experts and senior experts. According to the survey results from Gulp (2022), junior experts have an average of 5.7 years of professional experience. To be a senior expert, an average of 7.6 years of experience is required.

In order for expert knowledge to be used for a risk assessment, it must be elicited (Elias et al., 2018, p. 1-6). This means that experts are specifically interviewed in order to obtain knowledge about the security features and functions of the security system. A survey is necessary because uncertain variables must be estimated so that an assessment is possible in the first place (EFSA, 2014, p. 42). The transfer of expert knowledge into, for example, a probability statement is important, but at the same time particularly difficult because experts can give different answers (EFSA, 2014, p. 11; Elias et al., 2018, p. 28). Expert knowledge as the input of a security metric, for example, has a significant influence on the output of a security assessment and, consequently, the investment in security measures (Saltelli et al., 2004, p. 42, 91, pp. 152-167; Lichte et al., 2020, 1). The question is which method can be used to quantify this knowledge in the best possible way (Vogl, 2017). The challenge lies in the process of generating information for a model or metric (Elias et al., 2018, p. 144). In Shadbolt et al. (2015), this process is summarized under the term "knowledge engineering". In the following, elaborated methods for eliciting expert knowledge are presented in the form of an excerpt and advantages and disadvantages are named.

There are two variants for expert surveys. In the first variant, the probability statements of the individual members of an expert group are determined and then aggregated (EFSA, 2014, p. 35). However, the numerical aggregation is not conducted in equal parts. Expert statements can sometimes differ greatly from one another. Experts can also differ in the certainty of their statements. In order to incorporate this certainty into the determination of a probability distribution, a weighting is useful. Less certain statements therefore have less influence than more certain statements on the overall result. With this approach, the influence of in-group dynamics is minimized because experts are assigned a weighting according to their experience. Intra-group dynamics include, for example, socio-psychological effects (dominance of certain experts, introversion of other experts). These effects can be compensated for by a suitable moderator.

In the second variant, the selected group of experts is given the task of finding consensus among themselves. This variant is therefore referred to as behavioral aggregation (EFSA, 2014, p. 35). The output of this approach depends on the participants in the survey. The collector of expert knowledge must be confident that the opinion of each expert is adequately taken into account. In behavioral aggregation, discussion is stimulated when opinions diverge strongly (Randle et al., 2019). In contrast to numerical aggregation, in behavioral aggregation, assumptions made by experts that lead to disagreement can be resolved through effective moderation. In behavioral aggregation, a probability distribution is determined by discussion, whereas in numerical aggregation it is determined by a mathematical formula (EFSA, 2014, p. 57). Common survey methods according to Oakley & O'Hagan (2010), Cooke (1994) and the Research and Development Corporation (RAND, 2021) are briefly presented below.

The Sheffield Elicitation Framework (SHELF) is a protocol for eliciting expert knowledge and was developed by Oakley & O'Hagan (2010) (EFSA, 2014, p. 67). It comprises a set of specifications to support the generation of probability distributions. In Tonyohan (2021) templates are made available for free download. The Sheffield method is based on behavioral aggregation. The so-called quartile method is used for the survey, as shown in Figure 22.

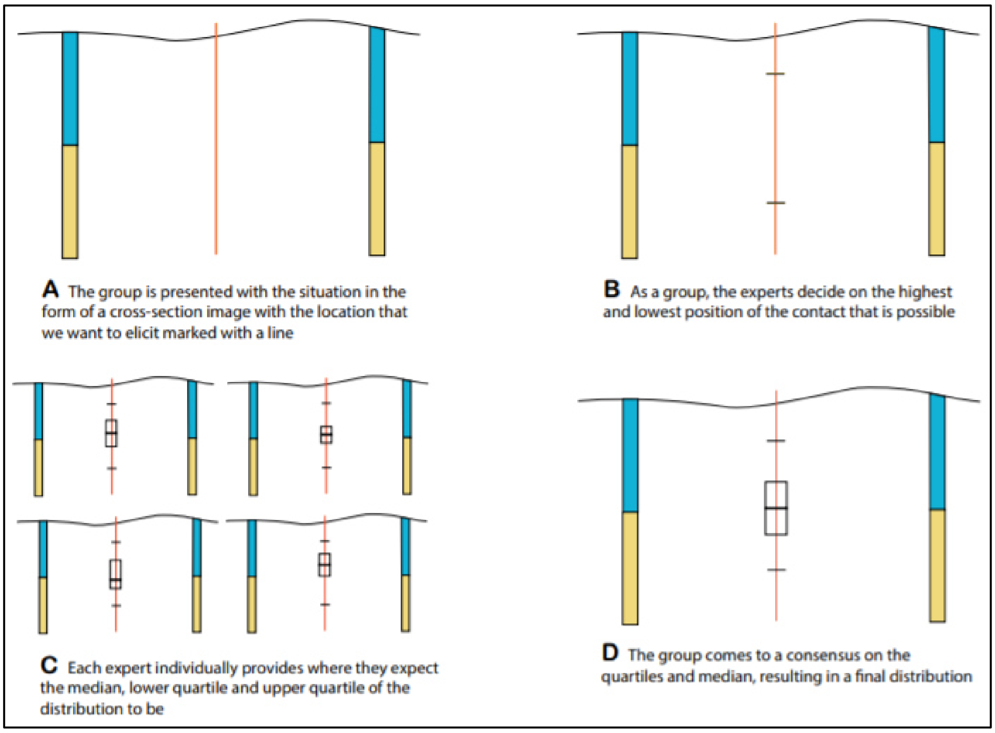

A The group is presented with the situation in the form of a cross-section image with the location that we want to elicit marked with a line
B As a group, the experts decide on the highest and lowest position of the contact that is possible
C Each expert individually provides where they expect the median, lower quartile and upper quartile of the distribution to be
D The group comes to a consensus on the quartiles and median, resulting in a final distribution

Figure 22: Summary of process steps A -D of the SHELF.
Source: Randle et al. (2019).

The model for converting expert knowledge into probability distributions according to Cooke (1994), also known as the classic survey model (Colson et al., 2020), is an approach for the numerical aggregation of expert knowledge (EFSA, 2014, p. 85). Two types of questions are used to validate expert judgments: target questions and calibration questions. Target questions are used to obtain expert statements on the uncertainties of all variables of interest, the so-called target variables (Colson et al., 2020). With calibration questions, also known as seed questions, experts are supposed to indicate uncertainties in variables (seed variables) whose true value is known to the surveyor but not to the experts. Calibration questions are asked before the target questions and, according to Colson et al. (2010), have three purposes:

- Validation of expert performance
- Performance-based expert weighting
- Mechanism for assessing different combinations of expert assessments

In Cooke's model, it is assumed that the experts' performance in answering calibration questions can be used to infer their performance in answering target questions (Cooke 1994). For this reason, the seed variables must be as similar as possible to the target variables (EFSA, 2014, p. 85). According to the European Food Safety Authority EFSA (2014, p. 85), the assessment of the quality of expert statements, known as performance aggregation, is conducted using two variables, calibration and information. Calibration measures the statistical probability that an expert's assessment corresponds to the actual realization of a seed variable (Elias et al., 2018, pp. 103-105). If the probability values of an expert are below a certain tolerance threshold, this expert is not weighted. The threshold value is defined by a reviewer. The calibration is assessed with values between "0" (low) and "1" (high), where "1" means high statistical accuracy and "0" means low statistical accuracy (EFSA, 2014, p. 85). In the case of a high calibration, an expert's answers to the calibration questions are close to the true values of the seed variables.

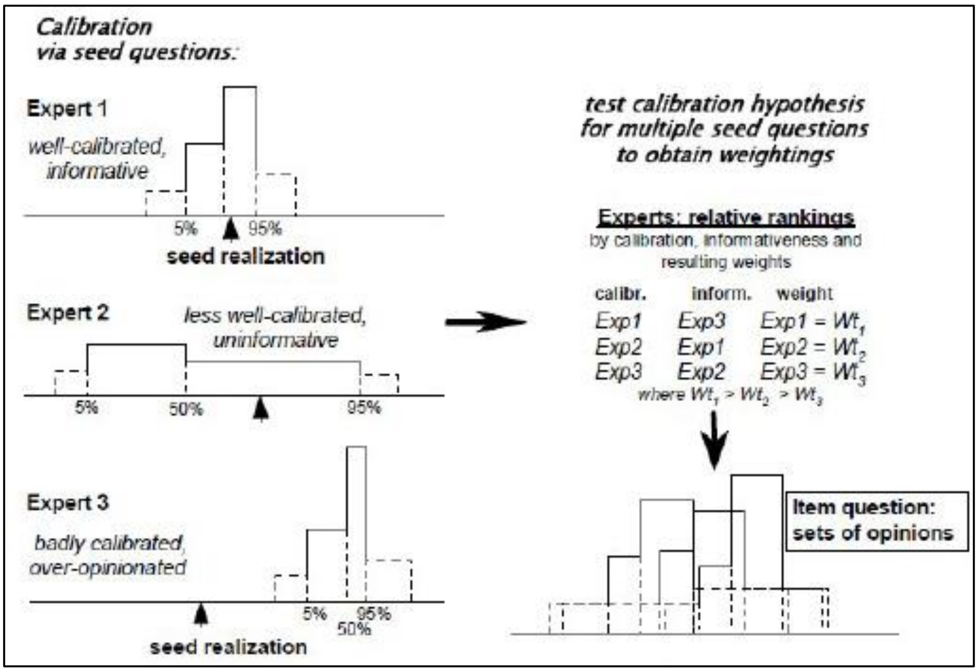
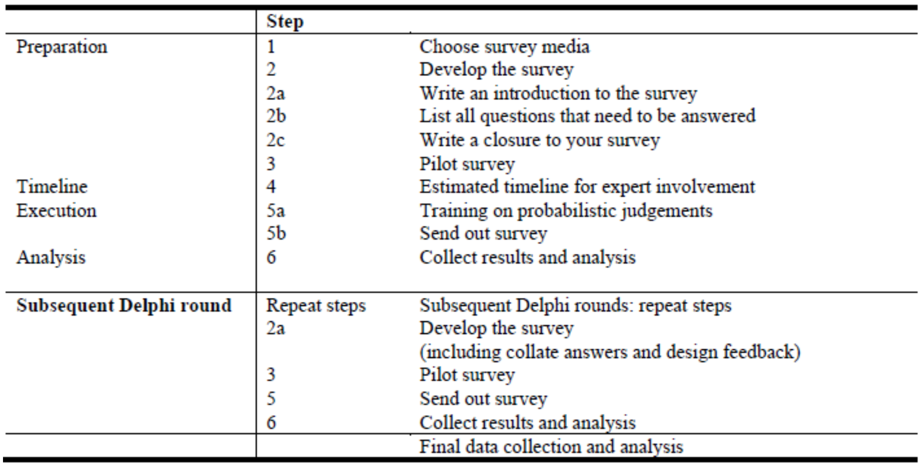


Figure 23: Schematic description of performance aggregation via seed question.
Source: EFSA (2014, p. 86).

The performance measure "information" describes the degree of entropy in the performance of an expert (sample entropy) and the degree of entropy in the answers to calibration questions (answer entropy) (Elias et al., 2018, pp. 105-106). According to Cooke (1994), an average information value is calculated for each expert. In this context, there are different approaches as to how the calculation can be conducted (Elias et al., 2018, pp. 102-106). In general, good expertise corresponds to good calibration and a large amount of information. In summary, calibration provides an answer to the question "How close is the expert's statement to the true value?", while information provides an answer to the question "How consistent is the expert's statement (across multiple calibration questions)?" represents. To simplify, it can be said that the calibration expresses how close the mean value is to the actual value, while the information represents the dispersion around this mean value (see Figure 23). Experts classically indicate a 5 % quantile and a 95 % quantile according to Cooke's approach. According to EFSA (2014, pp. 85-86), the performance-related weights of the individual experts are proportional to the product of calibration and information.

In addition to the SHELF approach according to Oakley & O'Hagan (2010) and the classic survey approach according to Cooke (1994), the Delphi method is a widely used approach for eliciting expert knowledge (EFSA, 2014, p. 8). The Delphi method was developed by the Research and Development Corporation (RAND) in the 1950s to predict the impact of technologies on warfare (RAND, 2021). The purpose of the Delphi method is to test the consensus of opinion of a group of experts (Vernon, 2009). Essentially, Delphi is a repetitive survey in which questions are asked in a way that allows for cross-expert comparability (see Table 10). The Delphi survey can be conducted in several consecutive rounds. After each round, the expert feedback is used by the surveyor to improve the questions for the next round. In addition to the questions, further information can be provided by the surveyor to the experts. This information should help to strengthen confidence in the expert opinion (confidence). As new expert knowledge is incorporated with each new round, a limited degree of expert interaction is possible (EFSA, 2014, p. 101). In addition, expert statements can be revised and readjusted on the basis of newly acquired information (Hubbard et al., 2016, p. 72). The aim of further rounds is ideally to reach a consensus.



	Step	
Preparation	1	Choose survey media
	2	Develop the survey
	2a	Write an introduction to the survey
	2b	List all questions that need to be answered
	2c	Write a closure to your survey
	3	Pilot survey
Timeline	4	Estimated timeline for expert involvement
Execution	5a	Training on probabilistic judgements
	5b	Send out survey
Analysis	6	Collect results and analysis
Subsequent Delphi round	Repeat steps	Subsequent Delphi rounds: repeat steps
	2a	Develop the survey (including collate answers and design feedback)
	3	Pilot survey
	5	Send out survey
	6	Collect results and analysis
		Final data collection and analysis

Table 10: Steps for conducting a Delphi survey.
Source: EFSA (2014, p. 101).

The anonymity of the participants is a special feature of the Delphi method. This is intended to ensure that an expert opinion can be obtained that is not directly influenced by other opinions, as is the case with typical behavioral aggregation. Each expert opinion is classically weighted equally (Vernon, 2009). The responses are summarized and analyzed in a final round (EFSA, 2014, p. 101). An overview and classification of other options for eliciting expert knowledge is presented in Shadbolt et al. (2015).

2.6.2 Applications in Security Assessment

The use of expert knowledge is an integral part of all the methods, models and metrics presented in chapter 2.5 in order to deal with uncertainties due to a small database in the security assessment. The following are examples of applications of methods for eliciting expert knowledge in security assessments.

In a study on the influence of uncertainties in physical security assessment, it is pointed out that semi-quantitative modelling is widely used and parameterization by expert knowledge is classically conducted in the form of scores (Lichte et al., 2018). However, scoring-based models allow uncertainties to be taken into account, which is why Lichte et al. (2018) introduce an approach that makes it possible to transfer from semi-quantitative modeling to quantitative modeling. Using the example of a fictitious production infrastructure, Lichte et al. (2018) present a simplified semi-quantitative method for assessing security risks based on a ranking of protection (P), observation (O) and intervention (I). Lichte et al. (2018) explain that it is necessary to note time intervals after the scores of the assessment variables, e.g. P-score "1" = 0 - 90 seconds, P-score "2" = 90 - 180 seconds, etc. "The ranking scale that is chosen depending on the considered infrastructure as well as the corresponding estimations [of experts]" (Lichte et al., 2018, p. 4). For each barrier, experts give their ranking for the characteristics of protection, observation and intervention. It is then explained how the rankings can be converted into triangular probabilistic density functions and how this input can be used to determine a quantitative vulnerability value for protection, observation and intervention.

Coffey et al. (2016) examine ways of gathering expert knowledge in the context of conceptual modeling in the development of service-oriented architectures. It is essentially about identifying security and trust issues in the development of continuously evolving software systems. Coffey et al. (2016) suggest ways to elicit expert knowledge in the context of conceptual modeling: First, it is recommended to develop concept maps to represent software development-relevant events and their relationships to each other (Coffey et al., 2016, p. 44) (see Figure 24). The concept maps form the basis for conducting a two-stage expert interview, with stage one focusing on the "desktop and tool federation level" and stage two on the "enterprise level". Coffey et al. (2016, p. 50) provide a set of questions for interviewing experts in software development. The concept maps can then be sharpened on the basis of the qualitative answers. As a result, security and trust in software development are increased by optimizing processes.

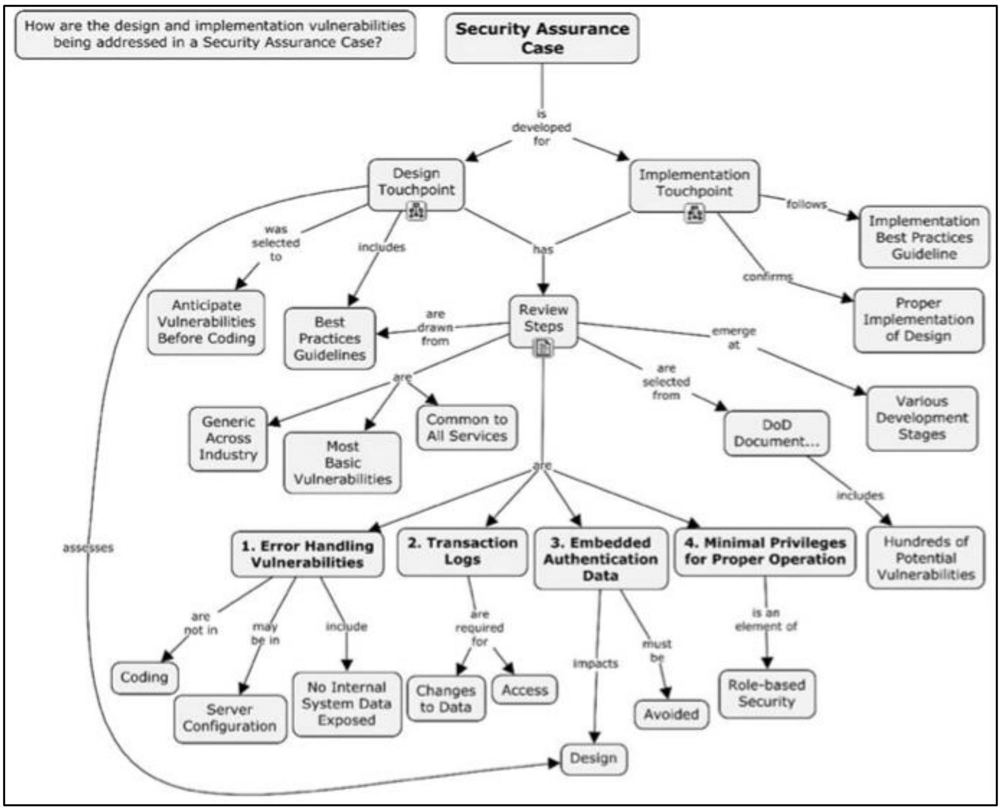
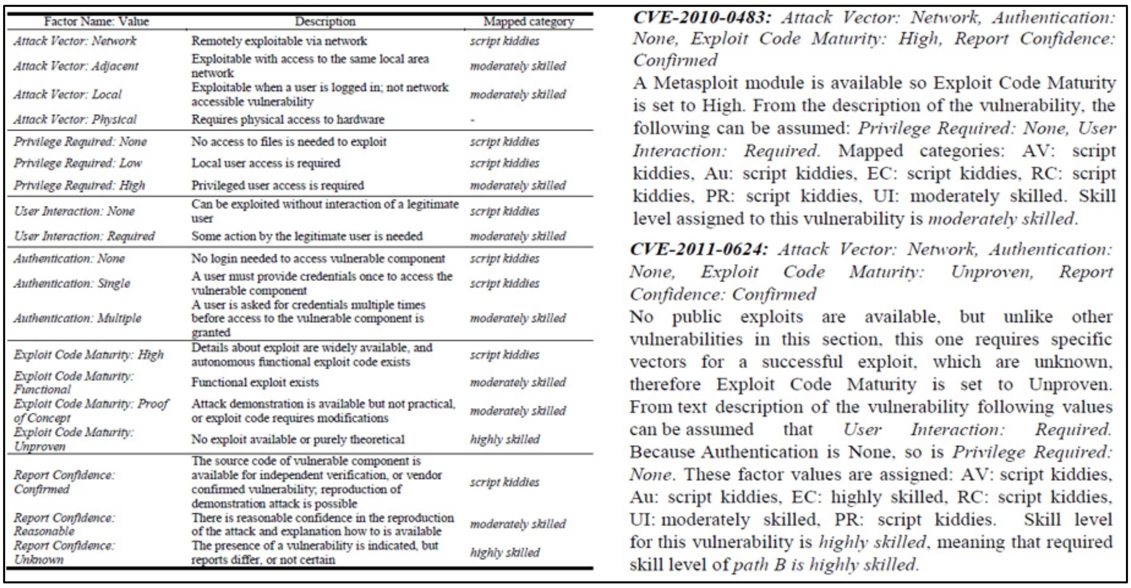

How are the design and implementation vulnerabilities being addressed in a Security Assurance Case?
Security Assurance Case
is developed for
Design Touchpoint
Implementation Touchpoint
follows
Implementation Best Practices Guideline
was selected to
includes
has
confirms
Proper Implementation of Design
Anticipate Vulnerabilities Before Coding
Best Practices Guidelines
are drawn from
Review Steps
emerge at
Various Development Stages
are
are selected from
Generic Across Industry
Most Basic Vulnerabilities
Common to All Services
DoD Document...
includes
Hundreds of Potential Vulnerabilities
are
assesses
1. Error Handling Vulnerabilities
2. Transaction Logs
3. Embedded Authentication Data
4. Minimal Privileges for Proper Operation
are not in
may be in
include
are required for
impacts
must be
is an element of
Coding
Server Configuration
No Internal System Data Exposed
Changes to Data
Access
Avoided
Role-based Security
Design

Figure 24: Exemplary concept map.
Source: Coffey et al. (2016, p. 47).

The article by Luxhøj et al. (2016) presents a knowledge elicitation process to support the probabilistic analysis of safety risks in aviation. It also discusses the application of a verbal-numerical scale to elicit conditional probabilities for a Bayesian Belief Network (BBN). The basic idea is similar to the approach proposed in Lichte et al. (2018). In IT security, for example, there is the "CyberRank" method. This is intended to support the making of security-relevant decisions with the help of expert statements (Grushka-Cohen et al., 2016). Grushka-Cohen et al. (2016) introduce an approach for classifying alerts about anomalous activities and policy violations. CyberRank is an algorithm for automatically prioritizing alerts so that experts can assess their criticality more quickly. This in turn can enable reactive measures to be derived more quickly (Grushka-Cohen et al., 2016).

In Mézešová et al (2019), the question of how the minimum requirement for a certain attacker skill level can be inferred from the characteristics of CVSS scores is investigated. A categorization method is proposed to assess the skill level required by an attacker to exploit an IT vulnerability or multiple IT vulnerabilities along an attack path (Mézešová et al., 2019). From the point of view of the defense, a conclusion is drawn on the basis of an expert survey from the prerequisites for conducting an attack to the skill level of an attacker. The expert survey in Mézešová et al (2019) is divided into two rounds. In the first round, IT experts are consulted to provide information about plausible attacker types and their characteristics. The three skill levels "Scrypt Kiddie", "Moderate" and "High" result from the survey (see Figure 25). In a second round, the experts are asked which skill level is required to conduct certain threat scenarios using specific examples. The feasibility of the selected threat scenarios is scored for each skill type. The threat scenarios are then traced back to the assessment parameters Attack Vector, Attack Complexity, Privileges Required, User Interaction, Authentication, Exploit Maturity Code and Report Confidence according to CVSS (First.org, 2022). The minimum skill levels are then assigned to the characteristics of the CVSS assessment variables.



Factor Name: Value	Description	Mapped category
Attack Vector: Network	Remotely exploitable via network	*script kiddies*
Attack Vector: Adjacent	Exploitable with access to the same local area network	*moderately skilled*
Attack Vector: Local	Exploitable when a user is logged in; not network accessible vulnerability	*moderately skilled*
Attack Vector: Physical	Requires physical access to hardware	-
Privilege Required: None	No access to files is needed to exploit	*script kiddies*
Privilege Required: Low	Local user access is required	*script kiddies*
Privilege Required: High	Privileged user access is required	*moderately skilled*
User Interaction: None	Can be exploited without interaction of a legitimate user	*script kiddies*
User Interaction: Required	Some action by the legitimate user is needed	*moderately skilled*
Authentication: None	No login needed to access vulnerable component	*script kiddies*
Authentication: Single	A user must provide credentials once to access the vulnerable component	*script kiddies*
Authentication: Multiple	A user is asked for credentials multiple times before access to the vulnerable component is granted	*moderately skilled*
Exploit Code Maturity: High	Details about exploit are widely available, and autonomous functional exploit code exists	*script kiddies*
Exploit Code Maturity: Functional	Functional exploit exists	*moderately skilled*
Exploit Code Maturity: Proof of Concept	Attack demonstration is available but not practical, or exploit code requires modifications	*moderately skilled*
Exploit Code Maturity: Unproven	No exploit available or purely theoretical	*highly skilled*
Report Confidence: Confirmed	The source code of vulnerable component is available for independent verification, or vendor confirmed vulnerability; reproduction of demonstration attack is possible	*script kiddies*
Report Confidence: Reasonable	There is reasonable confidence in the reproduction of the attack and explanation how to is available	*moderately skilled*
Report Confidence: Unknown	The presence of a vulnerability is indicated, but reports differ, or not certain	*highly skilled*

CVE-2010-0483: *Attack Vector: Network, Authentication: None, Exploit Code Maturity: High, Report Confidence: Confirmed*
A Metasploit module is available so Exploit Code Maturity is set to High. From the description of the vulnerability, the following can be assumed: *Privilege Required: None, User Interaction: Required.* Mapped categories: AV: script kiddies, Au: script kiddies, EC: script kiddies, RC: script kiddies, PR: script kiddies, UI: moderately skilled. Skill level assigned to this vulnerability is *moderately skilled.*

CVE-2011-0624: *Attack Vector: Network, Authentication: None, Exploit Code Maturity: Unproven, Report Confidence: Confirmed*
No public exploits are available, but unlike other vulnerabilities in this section, this one requires specific vectors for a successful exploit, which are unknown, therefore Exploit Code Maturity is set to Unproven. From text description of the vulnerability following values can be assumed that *User Interaction: Required.* Because Authentication is None, so is *Privilege Required: None*. These factor values are assigned: AV: script kiddies, Au: script kiddies, EC: highly skilled, RC: script kiddies, UI: moderately skilled, PR: script kiddies. Skill level for this vulnerability is *highly skilled*, meaning that required skill level of *path B is highly skilled.*

Figure 25: Transfer of CVSS scores into attacker skill level.
Source: Mézešová et al. (2019).

From the consideration of all characteristics of the CVSS ranking, the highest skill level is defined as the minimum qualification level for the possibility of successfully exploiting an IT vulnerability. In summary, Mézešová et al. (2019) use expert knowledge to transfer CVSS scores into a single attacker category (see Figure 26). The method can be used to determine the minimum skill requirements of an attacker for an attack path. This makes it possible to rank attack paths, vulnerabilities and assets. The method thus provides a decision-making aid for risk managers ("What needs to be remedied first?"). CVSS is a degree of criticality that assesses the exploitability of vulnerabilities. Skill categorization based on (technical) minimum requirements is in principle a different interpretation; not with points on a semi-quantitative scale, as is the case with CVSS, but on a scale that assesses the following question: "What minimum skills must an attacker have?"

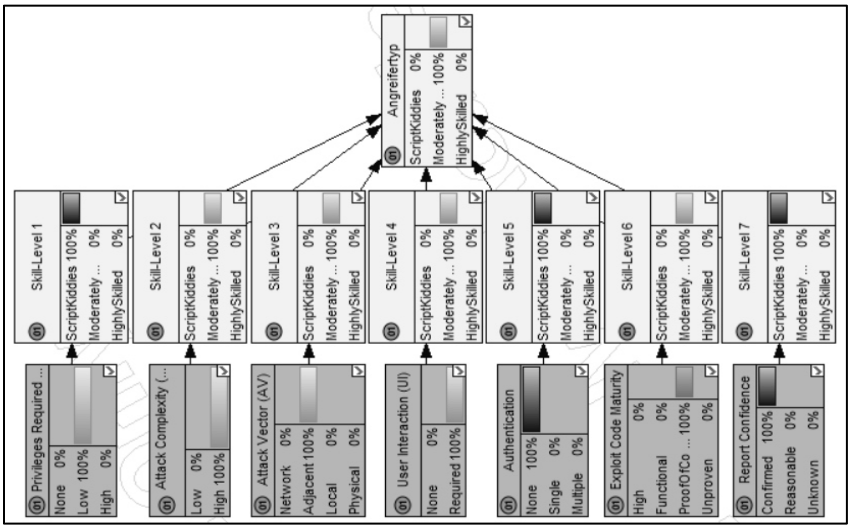


Figure 26: Bayesian network for determining the attacker requirements.
Own Figure based on Mézešová et al. (2019).

CVSS maps the criticality of exploited vulnerabilities at an abstract level, whereas the translation of CVSS parameters into skill levels enables the relationship between minimum requirements and a specific situation. "Concrete facts" means the possibility of a use case-specific interpretation. Possible effects are also implicitly linked to the skill level. High skill levels are generally necessary to steal more critical assets than in the case of lower skill levels. Critical" means "high impact". Critical assets are assets worth protecting, the compromise of which has a particularly high impact. Mézešová et al. (2019) present a technically oriented or technically conceived approach to assessing the need for technical capabilities to conduct an attack using expert knowledge. This is not yet the threat probability for a particular attack. An attacker must meet each assessed CVSS factor in order to exploit certain vulnerabilities. For some vulnerabilities, not every scoring factor is taken into account, depending on the information available. The previous examples show that the collection of expert knowledge plays an important role in answering security questions.

2.7 Summary of the State of the Art in Science and Technology

In summary, physical security assessment has evolved over a long period of time. Physical security is assessed on the basis of the three-part risk model of threat probability, vulnerability and impact. The assessment of vulnerability is a particular focus of both security domains. Physical vulnerability can be assessed using a quantitative metric with a stored, objective impact mechanism to describe the effect of measures on vulnerability reduction (Lichte et al., 2016). The three-part modeling approach from physical security can also be found in IT security. However, the assessment basis is different, as a comparison of PRISM and CVSS or FAIR reveals. IT security is subject to different paradigms than in purely physical security, as shown in Wheeler (2011), Anderson (2001) and Kofler et al. (2018), for example:

An attacker can beam themselves into the IT domain from minus infinity to the doorstep and override barriers by exploiting vulnerabilities. Similarly, there are only a few mechanisms for detecting attackers (Kofler et al., 2018, p. 37). Although architectures such as defense-in-depth (DiD) exist in IT security (Anderson, 2001, p. 513), they do not correspond to the spatial topological principle from physical security. In IT security, DiD rather refers to a series of successive security measures to protect confidentiality, integrity and availability. "As with castles, the aim with vehicles is to make it as difficult as possible for the attacker to overcome each stage", says Wurm (2022, p. 43). The principle corresponds to multilateral security (Anderson, 2001, p. 276).

Approaches for assessing physical mobile access security measures and IT mobile access security measures are developed in Schwerdtfeger (2018) on the basis of CC (2021) for immobile MAS. In this approach, a target security profile is defined and the actual security profile is compared with the target security profile by answering key questions. A low target security profile generally means that only a certain number of available questions from the catalog need to be answered, e.g. only two of a total of five mandatory questions and two additional questions. However, the choice of questions is at the discretion of the examiner. This is problematic insofar as an auditor can select the questions that are favorable to him if he does not have to answer all questions due to the selected target security profile. This degree of freedom in answering the questions can lead to an illusion of security: If, for example, only two out of five questions need to be answered, it can be falsely assumed that the system is sufficiently secure once the questions have been answered.

However, failure to answer the remaining questions, which are not selected by the auditor, can be the cause of a (future) successful attack. Some questions in the list of key questions, such as "What access options are there in principle?" or "Are other services used for access options?" (Schwerdtfeger, 2018, p. 127), a parallel can be drawn with the CVSS according to First.org (2022): The type of access options or the use of other services generally allows conclusions to be drawn about possible attack vectors. However, when answering questions such as "Are other services used for access options?", it is necessary to examine what it means specifically for security if other services are used to provide a service. In the guiding question-based approach, as proposed in Schwerdtfeger (2018), the performance-based assessment is left out.

CPS research shows initial approaches for assessing physical security and IT security in different fields of application. However, the approaches presented take insufficient account of the interaction between the domains of physical security and IT security. The Performance Risk-based Integrated Security Methodology (PRISM), for example, offers an elaborated guideline for physical security, but not for the assessment of IT security or interactions (Harnser, 2010, C4). Although CVSS can be used to assess threat scenario-describing characteristics from an IT perspective, there is no specific reference to hardware. CVSS only distinguishes between physical access (Attack Vector = context Physical) and IT access (e.g. Attack Vector = context Network). The influence of IT exploitability on physical vulnerability or vice versa is not assessed. In previous standards and guidelines, there are no proposed solutions for the metric merging of physical security and IT security. In Table 11 common security metrics in the domains of physical security and IT security are listed. In Table 12 and in Table 13 the advantages and disadvantages of selected methods, models and metrics from IT security and physical security are summarized.

Domain	Excerpt of Metrics and Models
IT Security	Microsoft Exploitability Index (MEI), Security Update Severity Rating System (SUSRS), Red Hat Security Rating (RHR), Stakeholder-Specific Vulnerability Categorization (SSVC), Exploitability Prediction Scoring System (EPSS), National Institute of Standards and Technology Vulntology (NIST Vulntology), Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD), Open Web Application Security Project (OWASP) Rating Methodology (OWASP RM), Factor Analysis of Information Risk (FAIR), Common Vulnerability Scoring System (CVSS), National Institute of Standards and Technology (NIST), Center for Internet Security (CIS).
Physical Security	Performance Risk-based Integrated Security Methodology (PRISM), Intervention Capability Metric (ICM), Estimate of Adversary Sequence Interruption (EASI), Analytic System and Software for Assessing Safeguards and Security (ASSESS), Safeguards Automated Facility Assessment (SAFE), System Analysis of Vulnerability to Intrusion (SAVI), Forcible Entry Safeguards Effectiveness Model (FESEM), Safeguard Effectiveness Model (ISEM), Safeguards Network Analysis Procedure (SNAP).

Table 11: Extract from security metrics.
Source: Own Figure.

IT Security			
Approach	**CVSS**	**FAIR**	**CC, list of key questions**
Type	qualitative, semi-quantitative, scoring-based	Quantitative	qualitative, semi-quantitative, scoring-based
Advantages	o Simple interpretation of results, o Employees without security expertise can be involved, o Clear instructions and guidelines, o Extensions possible, o Provision of a calculator	o Quantification of risk variables, o Calculation of IT risks in relation to financial losses, o Clear definition of terms, o Increasing accuracy over time (accumulation of experience and evidence)	o No quantification of variables o Easy handling due to guided questionnaire
Disadvantages	o No mapping of the interaction with the physical world, o Vulnerability assessment only at high-level system level o No mechanism of performance stored o Ordinal values are offset	o Static model that does not provide for editing/expansion o High level of expertise and experience required o Evidence required	o Interaction with the physical world not taken into account, o Results are subjective assessments, o No comparability of risks
Approach	**OMB M-04-04, NIST 800-63, Kantara, IAFF**	**Attack trees**	**Bayesian networks**
Type	Qualitative, semi-quantitative, scoring-based	qualitative, semi-quantitative, quantitative	Quantitative
Advantages	o Standardized, o Technical specifications define clear instructions for action	o Presentation of the implementation possibilities of an attack, o Probability theory applicable	o Mapping of real processes, o Probabilistic consistency, o Sufficient basis for cost-benefit analysis, o Versatile in terms of usability in risk assessment

Disadvantages	o No sufficient basis for cost-benefit analysis, o Strong focus on identity management o Technical know-how required for implementation	o Creation requires expert knowledge o Interactions between IT and physics insufficiently mapped	o Dependent on expert knowledge o Partly very complex

Table 12: Advantages and disadvantages of selected models, methods and metrics, IT security. Source: Own Figure.

Physical Security			
Approach	**EASI & derivatives**	**PRISM**	**Vulnerability model according to Lichte et al. (2016)**
Type	quantitative, time-based	qualitative, semi-quantitative, scoring-based	quantitative, time-based
Advantages	o Different perspectives can be mapped (external, internal attackers) o Consideration of topological and device-inherent properties	o Easy interpretation of the results, o Risk register provides an overview of the entire risk assessment	o Mapping of uncertainties, o Increasing accuracy through information gathering over the years, o Assessment of risks according to monetary values, o Cost-benefit analysis can be supported
Disadvantages	o sometimes very attribute-heavy, many parameters that have to be assessed subjectively, o expert knowledge required, o sometimes highly complex, o challenges in interpreting results	o Very complex, o Requires access to sensitive data via an infrastructure, o No adequate consideration of strict vulnerability criteria (protection, observation and intervention are only added together despite interdependencies, and the values are ordinal)	o High expenditure of time to obtain useful results, o High technical competence and skills required.
Approach	**Resistance Classes**	**Attack trees**	**Bayesian networks**
Type	quantitative, time-based	qualitative, semi-quantitative, quantitative	Quantitative
Advantages	o Highly standardized, o Easy to interpret, o Comparability possible	o Presentation of the implementation possibilities of an attack, o Probability theory applicable	o Mapping of real processes, o Probabilistic consistency, o Sufficient basis for cost-benefit analysis, o Versatile in terms of usability in risk assessment
Disadvantages	o Only common misuse scenarios are taken into account, o Use case-specific deviations in intrusion prevention are not taken into account, o Only consideration of physical security (interactions with IT are not recorded)	o Creation requires expert knowledge, o Interactions between IT and the physical world insufficiently mapped	o Dependent on expert knowledge, o Partly very complex

Table 13: Advantages and disadvantages of selected models, methods and metrics, physical security. Source: Own Figure.

The current state of expert knowledge collection shows that the definition and estimation of risk contributions that are difficult to quantify can only succeed if expert knowledge is elicited using suitable methods and fed into security metrics as input. Three methods for the elicitation expert knowledge are commonly used: SHELF, Cooke and Delphi. The advantages and disadvantages of the methods presented are summarized in Table 14.

Method	Advantages	Disadvantages
SHELF	o Expert assumptions can be reflected on immediately (direct feedback). o Creating consensus through discourse.	o Socio-psychological effects can occur (dominance by extroverted experts). o High demands on the moderator. o It may not be possible to reach a consensus.
Cooke	o Weighting of expert opinions. o Pre-filtering of experts on calibration issues. o Quantitative aggregation using mathematical formulas. o Moderator assesses the expert's professional competence and the expert in turn assesses the facts to be examined.	o Calibration issues not easy to find. o Data collection effort high. o Weighting of expert statements is not trivial. o A high level of technical expertise is required for the selection of target variables. o Mathematical expertise required from moderator.
Delphi	o Anonymous reporting of results, thus no mutual influence. o Survey of several independent experts. o Survey can be scaled from a few to hundreds of experts.	o Preparation of meetings time-consuming. o Compilation of results time-consuming. o Quality of the estimate depends on the skills of the experts. o Experts are selected subjectively. o Repeatability must be questioned if experts learn about the opinions of others after a round

Table 14: Advantages and disadvantages of elaborated methods for eliciting expert knowledge. Source: Own Figure.

The main function of all three methods mentioned is to translate the subjective degree of conviction of one or more experts into a quantitative expression by means of key questions and, if necessary, several rounds of questioning. In a next step, the output of an expert survey can be used as input for an assessment metric or the optimization of models, for example. The following challenges must be met when eliciting expert knowledge: 1) selecting one or more experts; 2) selecting a moderator who can deal with socio-psychological effects (e.g. dominance of individuals) in particular; 3) formulating the right questions in relation to the objective of the survey; 4) analyzing and assessing the expert statements. Following the considerations in Aigner & Khelil (2020), survey methods could be combined in order to enable the best possible elicitation and utilization of expert knowledge.

3 Approach for Cross-Domain Risk Assessment

The procedure for assessing cyber-physical vulnerability is based in part on the existing approaches according to Lichte et al. (2016), Braband (2019), Harnser (2010) and CVSS (First.org, 2022). It should be possible to assess the physical vulnerability of mobile access security systems based on effectiveness. The components of the physical effectiveness mechanism, protection, observation and intervention, should describe the physical security capabilities to prevent a physical attacker from successfully stealing the vehicle or mobile access product. In addition, it should be possible to take into account uncertainties in the assessment of security capabilities due to different attacker profiles. The physical attack process and the underlying time sequence for overcoming system barriers are quantitatively mapped on the basis of the vulnerability metric according to Lichte et al. (2016), referred to in this work as the Intervention Capability Metric. Measures are developed in a metric analysis so that the results of the scoring-based metric according to Harnser (2010) can be aligned with the results of the Intervention Capability Metric according to Lichte et al. (2016). As a result, a comparable vulnerability classification is achieved with both vulnerability metrics. This is necessary so that real vulnerability levels can be mapped with the Harnser scoring. It also explains how distortions within the Harnser metric can be reduced.

In IT security, it should be possible to assess vulnerability via the exploitability of system-inherent IT vulnerabilities, which particularly affect the integrity, confidentiality and availability of the MAS. The exploitability is determined using the threat scenario-describing parameters from the CVSS (First.org, 2022). In this work, distortions in the CVSS exploitability metrics and the barrier-based CVSS approach, as proposed in Braband (2019), are analyzed. Subsequently, suggestions for improvement are developed to reduce the detected distortions, e.g. the application of a log transformation, logical inconsistencies related to the designation or the characteristics of assessment parameters. The reduction of inconsistencies helps to reduce contradictions within the scoring systems and to harmonize the assessment parameters of a scoring with regard to the degree of abstraction or information content. The defined requirements and measures from the metric analysis of the Harnser metric and the Intervention Capability Metric are used as a starting point for harmonizing the description and assessment of vulnerability and risks in both security domains. This thesis examines the requirements to be defined for vulnerability descriptions so that a barrier-based path model can be used as a star-ting point for vulnerability assessment in both physical security and IT security.

In a further step, it will be shown how the risk descriptions and risk assessments in both security domains can be brought together and what prerequisites are required for this. The Harnser metric is used to assess physical vulnerability. The CVSS metric is used to assess IT vulnerability. In this thesis, measures are developed to consistently set up the assessment of threat scenarios in both domains (at process level). It also explores how interactions can be assessed and how security levels in both domains can be coordinated in the event of an interaction. As there are insufficient options for quantifying vulnerability in IT security due to the lack of an objective mechanism of performance, it is proposed that only interactions of IT scenarios be mapped to physical scenarios. This choice is also due to the fact that the results of the scoring-based, physical vulnerability assessment can be quantitatively recalculated.

The basis for the assessment of cyber-physical interactions by expert assessments are the topological connections of the cyber-physical structures, which can be described by the server-client model (see chapter 8.2.1 in the appendix). According to the server-client concept, a compromised unit can lead to the compromise of subordinate units. In this context, the interfaces between physical barriers and IT units represent possibilities that an attacker can exploit to compromise physical security functions. The IT Impact on Physical Vulnerability (ITIPV) is introduced to map the interaction. The ITIPV describes the degree to which physical security functions are compromised by an IT scenario. To determine the ITIPV, the physical vulnerability is determined twice: once under the assumption that there is only one physical scenario and once under the assumption that an IT scenario affects physical security functions before the physical scenario. The assessment of the impairment is based on expert assessments.

Specifications from the ISO/SAE 21434 (Cybersecurity Assurance Level, CAL) and ISO 26262 (Automotive Safety Integrity Level, ASIL) standards are used to derive and harmonize physical and IT security levels. Differences in the definition of CAL and ASIL are worked out and possibilities for deriving physical security levels and IT security levels according to the same system are presented. It also discusses how security levels can be set depending on the ITIPV if there is an interaction. The impact scale of both domains is harmonized so that the effects of physical attacks and the effects of IT attacks can be identified. The standardization of the impact scale is an important prerequisite for a successful cross-domain assessment. To enable a holistic risk analysis to be conducted, it is shown how the metric approaches developed for vulnerability assessment in physical security and IT security can be integrated into the TARA in accordance with ISO/SAE 21434 and thus extended to the cyber-physical TARA (CPTARA) in the sense of a prospective risk assessment for CPS. [28] Methods are proposed for the sub-steps for conducting a CPTARA, such as the what-if technique for assessing assets or attack tree analysis for assessing attack paths. The proposed threat analysis and risk assessment are combined using the Bayesian network method in order to link the expert knowledge on security capability in physical security and IT security in a probabilistically consistent manner.

The choice of Bayesian networks allows expert knowledge about the topological links within the system and the capabilities of the security measures used to be taken into account. For this purpose, a survey procedure based on the Delphi method and Cooke's survey approach is proposed in order to quantify expert knowledge and transfer it to the model as input. The generic procedure of the mixed-metric and mixed-methods approach allows domain-specific and cross-domain risk analyses to be conducted. Work steps in the course of developing an approach to enable a cross-domain security assessment are described below at a higher level:

1. Conducting a metric analysis on ways to reduce the incompatibility between semi-quantitative and quantitative metrics using the example of physical security: The semi-quantitative vulnerability metric according to Harnser (2010) is compared with the quantitative Intervention Capability Metric according to Lichte et al. (2016). Suggestions for reducing distortions within the Harnser metric are proposed.
2. Analysis of the distortions in the Common Vulnerability Scoring System (CVSS) according to First.org (2022) and the barrier-based CVSS: Investigation of the weaknesses of the basic metric and discussion of possible improvements, e.g. reduction of distortions.
3. Definition of boundary conditions so that the unequal assessments in the domains of physical security and IT security result in equal vulnerability and risk classifications and security levels: Using CVSS (IT security) and the Harnser metric (physical security) as examples.
4. Structure of the risk analysis, based on ISO/SAE 21434: Extension of the Threat Analysis and Risk Assessment (TARA) to the Cyber-Physical Threat Analysis and Risk Assessment (CPTARA).

[28] Delimitation according to Morr et al. (2019): Predictive: "What will happen?", diagnostic: "Why did it happen?", descriptive: "What happened?", prescriptive: "What should be done?". In a prospective analysis, data is collected and analyzed, e.g. to check the effectiveness of a system's safety or security measures. In predictive analysis, (historical) data is used to predict future events.

5. Implementation of the risk analysis steps in a Bayesian network in order to link the expert knowledge about the security capability for the physical security and IT security domains in a probabilistically consistent manner.

The paper concludes with a summary of the results and a description of possible follow-up research.

3.1 Analysis of the Harnser Metric and Intervention Capability Metric

The problem with using semi-quantitative metrics is explained 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. (Krisper 2021, p. 5).

The Harnser scores are not based on an underlying metric based on time, as is the case with the ICM according to Lichte et al. (2016). For example, the Harnser score "5" is defined as: "There is no capability to prevent this scenario from occurring and causing worst-case consequences" (Harnser, 2010, p. 109). A sharp vulnerability criterion can be objectively mapped with the Intervention Capability Metric (ICM) according to Lichte et al. (2016). This is not possible with the Harnser metric because the vulnerability scores are not based on specific probabilities. Krisper (2021) writes in this context: "It is important to check the validity of methods by measuring their prediction strength and comparing this with other methods to find the most suitable method for a purpose" (Krisper, 2021, p. 10). In the problem definition from chapter 1.1 the incompatibility between the additive approach according to Harnser and the probabilistic approach according to Lichte et al. (2016) is already pointed out in qualitative form. Both vulnerability assessments consider the physical security capability of a system in the event of an attack, i.e. the vulnerability assessment assumes that an attacker actually attacks the system by physical means (see also Chapter 1.2).

If the vulnerability scale of the Harnser metric were compatible with the vulnerability results of the ICM, then the Harnser metric could be used to determine real vulnerability levels. This would have the advantage that in a physical threat analysis and risk assessment, scenarios could be assessed by experts on a scoring basis and a realistic assessment of vulnerability could be made using the vulnerability scores. Product development experts can therefore use simple scoring for physical security assessment, which does not require in-depth mathematical knowledge. Adapting the Harnser metric to objective vulnerability levels also creates advantages for a cross-domain security assessment. Suppose there are IT scenarios that can have an impact on physical security functions. However, the IT threat probability and IT vulnerability are not known in detail. Once an expert has identified an IT scenario with an impact on physical security measures, they can use the Harnser metric adapted to the ICM to assess the following: What is the physical security capability of the system in the event of a physical attack if an IT scenario has previously impacted the physical security capability? Following this idea, physical vulnerability is assessed on the assumption of a physical attack, taking into account a previous IT attack. The result of the Harnser scoring then provides a vulnerability score, behind which is an objective vulnerability level. Further information on cross-domain assessment can be found in chapter 3.2.

From a scientific point of view, the questions arise as to how great the incompatibilities between the two metrics actually are under certain assumptions and what possibilities there may be to reduce them. In this paper, a mathematical analysis is conducted to answer these questions. Krisper (2021), for example, suggests using quantitative metrics as a tool to assess the quality of qualitative and semi-quantitative assessment schemes. In principle, these can be quantitative safety or quantitative security metrics. In a comparison of semi-quantitative and quantitative metrics, Krisper (2021) states: "The identification of influence factors plays a massive role in risk assessment. [...] Multiplicative methods also tend to use lesser factors, like two or three, and additive ones use more in general" (Krisper, 2021, p. 3). The differences between the vulnerability results of the Harnser metric and the vulnerability results of the ICM are calculated using different types of scoring scheme in the Harnser metric and using the variation of means and dispersions in the ICM. Measures to reduce the metric differences are then examined. For example, discrete values for protection, observation and intervention are selected for the ICM in one analysis run. The result should be a vulnerability function depending on the capabilities of a protection system, which shows mathematically which differences arise and how large these are when working semi-quantitatively according to Harnser - in comparison to quantitatively according to the ICM. This makes it possible to objectively demonstrate where the quantitative approach according to the ICM delivers different results than the semi-quantitative approach according to Harnser. To ensure comparability, the following reference scenario is selected:

A system consisting of a barrier and an asset is considered. The barrier must be overcome in order to access the asset. It has the properties of protection, observation and intervention. The effectiveness of measures in the event of an attack is assessed in relation to vulnerability. The protection, detection and intervention assessment variables are each scored between "1" (minimum) and "5" (maximum) by Harnser. The detection score is replaced here by the observation score. The reason for this is that detection is an event that results from the interaction of protection and observation. On the basis of the five scores for protection (P), observation (O) and intervention (I), the permutations of all possible values (5 x 5 x 5 = 125) are then calculated in accordance with the specified calculation specifications according to Harnser (2010). The following analyses are conducted: 1) Formation of the vulnerability score via the sum of the scores of protection, observation and intervention; 2) Formation of the vulnerability score via the sum of the logarithmized scores of protection, observation and intervention. To determine vulnerability with the ICM, quantitative counterparts are formulated for each Harnser score. These are also used to calculate the permutations of all possible values (5 x 5 x 5 = 125). It is assumed that the times for protection, observation and intervention are normally distributed variables. The control variables are the mean value and the standard deviation, i.e. it is a matter of assigning a P-score, O-score or I-score to a mean value and a standard deviation of a normal distribution (see Table 15).

P Score	P, ICM 1 (sec)	O Score	O, ICM 1 (sec)	I Score	I, ICM 1 (sec)
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	$\mu = 15, \sigma = 30$

Table 15: Mapping of Harnser scores to mean values and standard deviations in the ICM. Source: Own table.

The standard deviations are set at 30 seconds for all scores. The protection time increases as the score increases, whereas the observation time and intervention time each become shorter as the score increases. ICM 1 stands for ICM variant number one. An ICM variant is a convention regarding the determination of the mean values and standard deviations for the levels "1" to

"5". In the case of the ICM, a total of 37 variants are calculated, whereby one variant (ICM discrete) considers the consideration of discrete time values for protection, observation and intervention. The configurations ICM 1, ..., ICM 36, on the other hand, are based on density functions for protection, observation and intervention. In Table 16 the values of the standard deviations are substituted by letters: Ax stands for the standard deviation of the protection. Bx stands for the standard deviation of the observation, and Cx stands for the standard deviation of the intervention. The index "x" denotes the respective ICM variant (see Table 16 and Table 17).

P Score	P, ICM x (sec)	O Score	O, ICM x (sec)	I Score	I, ICM x (sec)
1	μ = 15, σ = Ax	1	μ = 135, σ = Bx	1	μ = 135, σ = Cx
2	μ = 45, σ = Ax	2	μ = 105, σ = Bx	2	μ = 105, σ = Cx
3	μ = 75, σ = Ax	3	μ = 75, σ = Bx	3	μ = 75, σ = Cx
4	μ = 105, σ = Ax	4	μ = 45, σ = Bx	4	μ = 45, σ = Cx
5	μ = 135, σ = Ax	5	μ = 15, σ = Bx	5	μ = 15, σ = Cx

Table 16: Generalization of the assignment of Harnser scores to mean values and standard deviations. Source: Own table.[29]

ICM ("x")	Ax [σ_P (sec)]	Bx [σ_O (sec)]	Cx [σ_I (sec)]
discrete	0.0000001	0.0000001	0.0000001
1	30	30	30
2	30	30	60
3	30	30	90
4	30	60	30
...	...	...	...
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
36	μ_P = 30, 60, 90, 120, 150; σ_P = 30	μ_O = 150, 120, 90, 60, 30; σ_O = 30	μ_I = 150, 120, 90, 60, 30; σ_I = 30

Table 17: Extract of the ICM variants.
Source: Own table.[30]

As an example of how Table 17 is to be read, Table 18 gives an example of the ICM variant 30.

[29] "x" stands for the ICM variant. Ax := standard deviation of the protection, Bx := standard deviation of the observation, Cx := standard deviation of the intervention.

[30] Since normal distributions are used in the metric, the mapping of discrete values is approximated by small standard deviations.

P Score	P, ICM 30 (sec)	O Score	O, ICM 30 (sec)	I Score	I, ICM 30 (sec)
1	μ = 15, σ = 10	1	μ = 135, σ = 75	1	μ = 135, σ = 100
2	μ = 45, σ = 10	2	μ = 105, σ = 75	2	μ = 105, σ = 100
3	μ = 75, σ = 10	3	μ = 75, σ = 75	3	μ = 75, σ = 100
4	μ = 105, σ = 10	4	μ = 45, σ = 75	4	μ = 45, σ = 100
5	μ = 135, σ = 10	5	μ = 15, σ = 75	5	μ = 15, σ = 100

Table 18: Harnser score assignment to the mean values and standard deviations of ICM 30.
Source: Own table.

The higher the number of the variant up to and including no. 27, the higher the standard deviations used. The mean values used remain the same, as shown in Table 15 remain the same. One exception is ICM 36 from Table 17. Variants 28 to 36 represent configurations in which further modifications are tested. The result for each permutation is a quantitative vulnerability value between 0 (minimum) and 1 (maximum), which can be assigned to the vulnerability results according to Harnser. In the first Harnser scoring variant, protection (P), observation (O) and intervention (I) are each scored between "1" and "5" and added together. As a result, a score range of "3" to "15" is possible. The score range from "0" to "2" is not included in the rating scale due to the calculation rule. "15" means low vulnerability and "3" means high vulnerability. The Harnser rating system is not comparable with the ICM in this form. To enable comparison, the Harnser rating scheme must be expanded to include a scale with probabilistic values.

The transformation of qualitative descriptors (or scores) into quantitative expressions is necessary because the Harnser results are to be compared with the results according to the ICM. Because, according to Krisper (2021) and Newsome (2013, p. 105), uncertainties are inherent in scores, the scores or the categories on the rating scale into which the scores are sorted should not be given discrete values, but rather an "approximate range" of probabilistic values (Newsome, 2013, pp. 104-105). The conversion of scores into other assessment variables is also called "conversion" (Howard, 1958). Initially, an equally large probability interval is assumed behind each vulnerability score, i.e. 0 % to 100 % of the possible probability of vulnerability is distributed equally among the vulnerability scores from "3" to "15" (see Table 19). The probability intervals are chosen to be equidistant in their width because it is not yet known how close the semi-quantitative results according to Harnser are to the quantitative results of the ICM. Such a classification is common practice among authorities and institutions (Newsome, 2013, p. 106).

V Score	3	4	5	6	7	8	9	10	11	12	13	14	15
Lower Value	0.924	0.847	0.77	0.693	0.616	0.539	0.462	0.385	0.308	0.231	0.154	0.077	0
Upper Value	1	0.924	0.847	0.77	0.693	0.616	0.539	0.462	0.385	0.308	0.231	0.154	0.077
Mean Value	0.962	0.8855	0.8085	0.7315	0.6545	0.5775	0.5005	0.4235	0.3465	0.2695	0.1925	0.116	0.035

Table 19: Harnser scale setup to enable a metric comparison.
Source: Own table.[31]

Not all calculated ICM variants and comparisons made between the Harnser metric and the ICM are presented in this paper. Selected ICM variants are considered below in order to illustrate the scientific added value. For the first comparison between the Harnser metric and the ICM, configuration one from Table 17 is used (ICM 1). Three variants are considered: In variant

[31] V := Vulnerability. Mu := mean value, sig := standard deviation, V := vulnerability, Upper := upper limit of the assumed probability interval, Lower := lower limit of the assumed probability interval.

one, the protection and observation scores remain constant, while the intervention score is increased (see Table 20).

Variant 1													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
1	1	1	3	0.924	1	0.962	15.0	135.0	135.0	30.0	30.0	30.0	1
1	1	2	4	0.847	0.924	0.8855	15.0	135.0	105.0	30.0	30.0	30.0	0.99999998
1	1	3	5	0.77	0.847	0.8085	15.0	135.0	75.0	30.0	30.0	30.0	0.9999998
1	1	4	6	0.693	0.77	0.7315	15.0	135.0	45.0	30.0	30.0	30.0	0.99999825
1	1	5	7	0.616	0.693	0.6545	15.0	135.0	15.0	30.0	30.0	30.0	0.99998904
Variant 2													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
1	1	1	3	0.924	1	0.962	15.0	135.0	135.0	30.0	30.0	30.0	1
1	2	1	4	0.847	0.924	0.8855	15.0	105.0	135.0	30.0	30.0	30.0	0.99999987
1	3	1	5	0.77	0.847	0.8085	15.0	75.0	135.0	30.0	30.0	30.0	0.99999312
1	4	1	6	0.693	0.77	0.7315	15.0	45.0	135.0	30.0	30.0	30.0	0.99982065
1	5	1	7	0.616	0.693	0.6545	15.0	15.0	135.0	30.0	30.0	30.0	0.99765631
Variant 3													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
1	1	1	3	0.924	1	0.962	15.0	135.0	135.0	30.0	30.0	30.0	1
2	1	1	4	0.847	0.924	0.8855	45.0	135.0	135.0	30.0	30.0	30.0	0.99999987
3	1	1	5	0.77	0.847	0.8085	75.0	135.0	135.0	30.0	30.0	30.0	0.99999312
4	1	1	6	0.693	0.77	0.7315	105.0	135.0	135.0	30.0	30.0	30.0	0.99982065
5	1	1	7	0.616	0.693	0.6545	135.0	135.0	135.0	30.0	30.0	30.0	0.99765631

Table 20: Variant calculation I for comparison of Harnser metric - ICM.
Source: Own table.[32]

Since each score is followed by mean values and standard deviations in the ICM configuration one, a score combination, e.g. P = "1", O = "1" and I = "1", can be quantitatively recalculated. In variant two, protection and intervention are kept constant, while observation is increasingly emphasized. In variant three, protection is the only one of the three assessment parameters that is varied. In all three variants, it can be seen that the difference between the results of the Harnser metric and the results of the ICM increases as the score increases. The drop in the vulnerability values according to Harnser can be explained by the definition of the scale categories in Table 19 can be explained. Behind each vulnerability score according to Harnser is a presumed probability interval that is clearly distinguishable from the other intervals: the lower the vulnerability score, the higher the presumed probability. Consequently, if one of the three assessment parameters is varied, the score sum becomes larger and the assumed probability smaller. The vulnerability results according to the ICM, on the other hand, remain constantly high.

A closer look at the calculation of the assessment variables in the ICM provides information on this: a low protection score means a short time in the inhibition of overcoming. A low observation score indicates a long observation time. Despite the fact that the intervention improves as the score increases, i.e. becomes shorter from the perspective of the quantitative metric, the vulnerability remains high. The reason for this shape of the vulnerability curve according to the ICM is the poor observation time. A short observation time is a prerequisite for the intervention to be successful. A good intervention time is useless if an attacker is not recognized

[32] V := Vulnerability.

as such or is recognized too late in the course of his attack. The example illustrates the interplay between the intrusion and reaction time as represented by the ICM. The calculations of the three variants illustrate the differences between the Harnser metric and the ICM.

With a minimum interpretation of two assessment parameters in each case, it is irrelevant whether the third assessment parameter, be it protection, observation or intervention, is emphasized: Vulnerability, as the quantitative calculation using the parameter combination in ICM 1 shows, remains above 99 %. However, the calculation using the scoring system suggests that the score increase would bring about an improvement. Another object of investigation could be to calculate how the vulnerability changes if the following setup is defined: Two scoring parameters are particularly emphasized, while the third mechanism of performance is to increase. In the same way as in Table 20 three variants are calculated. First of all, however, protection and observation are kept constantly high, while the intervention is varied. According to the same principle, the observation is varied in variant two and the protection in variant three, while the other two assessment parameters remain particularly pronounced. The calculated permutations are shown in Table 21. The results of the ICM reveal that the best vulnerability reduction can be achieved with the first variant. Variants two and three are identical in terms of vulnerability reduction and lower than variant one.

Variant 1													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
5	5	1	11	0.308	0.385	0.3465	135.0	15.0	135.0	30.0	30.0	30.0	0.61448878
5	5	2	12	0.231	0.308	0.2695	135.0	15.0	105.0	30.0	30.0	30.0	0.38785009
5	5	3	13	0.154	0.231	0.1925	135.0	15.0	75.0	30.0	30.0	30.0	0.19512502
5	5	4	14	0.077	0.154	0.1155	135.0	15.0	45.0	30.0	30.0	30.0	0.07662206
5	5	5	15	0	0.077	0.0385	135.0	15.0	15.0	30.0	30.0	30.0	0.02394229
Variant 2													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
5	1	5	11	0.308	0.385	0.3465	135.0	135.0	15.0	30.0	30.0	30.0	0.8067925
5	2	5	12	0.231	0.308	0.2695	135.0	105.0	15.0	30.0	30.0	30.0	0.53352204
5	3	5	13	0.154	0.231	0.1925	135.0	75.0	15.0	30.0	30.0	30.0	0.25668962
5	4	5	14	0.077	0.154	0.1155	135.0	45.0	15.0	30.0	30.0	30.0	0.0901429
5	5	5	15	0	0.077	0.0385	135.0	15.0	15.0	30.0	30.0	30.0	0.02394229
Variant 3													
P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
1	5	5	11	0.308	0.385	0.3465	15.0	15.0	15.0	30.0	30.0	30.0	0.8067925
2	5	5	12	0.231	0.308	0.2695	45.0	15.0	15.0	30.0	30.0	30.0	0.53352204
3	5	5	13	0.154	0.231	0.1925	75.0	15.0	15.0	30.0	30.0	30.0	0.25668962
4	5	5	14	0.077	0.154	0.1155	105.0	15.0	15.0	30.0	30.0	30.0	0.0901429
5	5	5	15	0	0.077	0.0385	135.0	15.0	15.0	30.0	30.0	30.0	0.02394229

Table 21: Variant calculation II for comparison of Harnser metric - ICM.
Source: Own table.[33]

Assuming the selected parameter combinations, a lot of observation and a lot of protection should generally be used. Ultimately, this depends on the cost function behind the parameters. This effect is not reflected by the Harnser metric. Nevertheless, it can be seen that the results of variant one can be best approximated with the scoring assessment system in the three analysis runs considered. The difference between the Harnser mean and the result according to the ICM is almost 27% for the first permutation, P = "5", O = "5" and I = "1". For the

[33] V := Vulnerability.

second permutation, the difference is approx. 12 %, for the third permutation it is 0.26 %, for the fourth permutation it is 4 % and for the fourth permutation it is 1.5 %. In a further step, all possible combinations, such as the permutations P = "2", O = "3", I = "5" or P = "4", O = "2", I = "4", are calculated and compared using the Harnser metric and ICM 1. In a first step, the assumed probability intervals can be compared with the scale from Table 19 for each of the (5 x 5 x 5 =) 125 score combinations. In a second step, these are ordered permutation-wise to the ICM results. The results of the Harnser metric and the results of the ICM are then sorted according to the size of the Harnser values (see Figure 27).

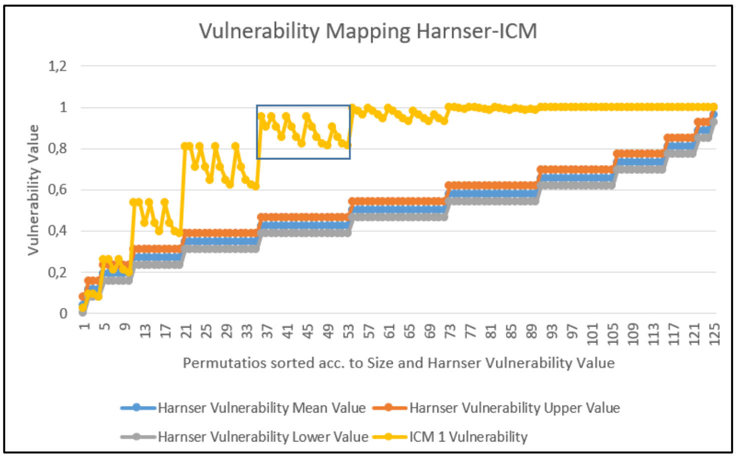


Figure 27: Sorted results of the permutations, ICM 1 - Harnser.
Source: Own Figure.

This results in an objective ICM vulnerability function. The results according to Harnser form a quasi-continuous mapping in relation to a discrete basis of the Harnser values. The course of the assignment contains jumps (plateaus) and is therefore not "continuous". The probability intervals per plateau are spanned by the "Lower Vulnerability Value" and the "Upper Vulnerability Value". The vulnerability results assigned to the Harnser values according to the ICM jump against this. The ICM results form a discontinuous curve of limited growth. When looking at the Figure 27 a question is raised: Why do the values of the ICM vulnerability function jump? To answer the question of why the ICM function values jump, a series of permutations is used as an example, in Figure 27 marked by a blue rectangle. Excerpted from the diagram shown in Figure 27, Table 22 lists the calculation results of the permuted variants. A high value (red), a medium value (orange) and a low value (yellow) are marked as examples. The designations high value, medium value and low value refer to the considered range of the available quantitative results. The score sum is the same for these three variants.

P	O	I	Sum Score	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
1	4	5	10	0.385	0.462	0.4235	15.0	45.0	15.0	30.0	30.0	30.0	0.95367115
1	5	4	10	0.385	0.462	0.4235	15.0	15.0	45.0	30.0	30.0	30.0	0.90338094
…	…	…	…	…	…	…	…	…	…	…	…	…	…
3	4	3	10	0.385	0.462	0.4235	75.0	45.0	75.0	30.0	30.0	30.0	0.85309073
3	5	2	10	0.385	0.462	0.4235	75.0	15.0	105.0	30.0	30.0	30.0	0.82195999
4	1	5	10	0.385	0.462	0.4235	105.0	135.0	15.0	30.0	30.0	30.0	0.95367115
4	2	4	10	0.385	0.462	0.4235	105.0	105.0	45.0	30.0	30.0	30.0	0.90338094
4	3	3	10	0.385	0.462	0.4235	105.0	75.0	75.0	30.0	30.0	30.0	0.85309073

Table 22: Extract from the calculated permutations, sorted according to the Harnser results.
Source: Own table.[34]

[34] V := Vulnerability.

Although the assumed probability interval is the same in all three cases from the point of view of the Harnser metric, there is one P = "1", O = "4", I = "5", one P = "3", O = "4", I = "3" and one P = "4", O = "2", I = "4". From a quantitative metric perspective, there are therefore differences. The score sum of "10" can be interpreted as the amount of available resources, which is divided between the protection, observation and intervention slots. The calculated vulnerability results based on the ICM show quantitatively that the interaction of the assessment parameters is better with P = "3", O = "4", I = "3" than with P = "1", O = "4", I = "5". Using this example, the ICM can be used to show that certain configurations that are assumed to have the same level of vulnerability from a Harnser perspective are more effective than others. This is the reason why there are differences in the vulnerability results between the ICM and the Harnser metric. This results in the jumps in the vulnerability function of the ICM.

The probability intervals that are assumed to lie behind the score sums of the Harnser metric are demonstrably suboptimal because they do not reflect the results of ICM 1. The comparison of Harnser vulnerability values and ICM 1 vulnerability values can be used as an example to illustrate that there are large differences in certain areas. From the user's point of view, it would be useful to have a scale classification in the scoring system that allows classifications to be made that correspond better with the quantitatively calculated vulnerability values. To this end, the progressions of both vulnerability curves are first analyzed qualitatively: The jumps in the ICM vulnerability values are differently pronounced depending on the assigned Harnser plateau. While the fluctuation of the vulnerability values at the beginning and end of the ICM vulnerability curve is low, it is significantly greater in the midfield (see Figure 28).

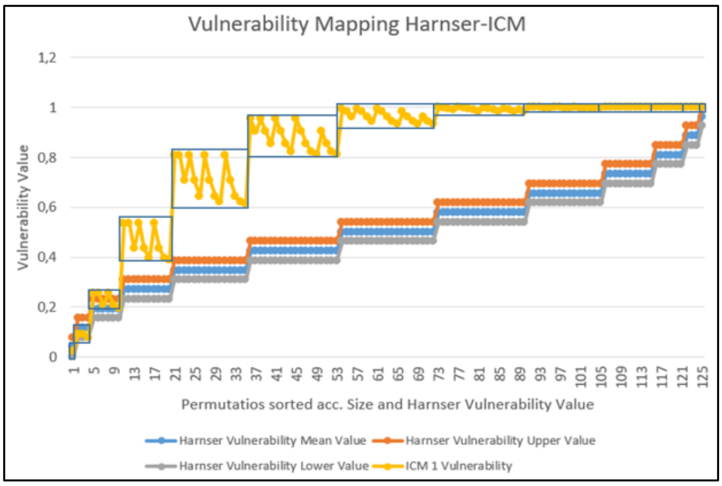


Figure 28: Probability intervals to be changed for the calculated permutations.
Source: Own Figure.[35]

Consequently, in order to capture all ICM vulnerability values within a Harnser plateau by a presumed probability interval, it is necessary to choose different widths of presumed probability intervals per Harnser score. A further insight is that the assumed probability intervals can overlap, for example score "10" := 0.98 - 1.00, and score "15" := 0.99 - 1.00. In order for the scale adjustment to be successful, an analysis of the vulnerability values of the permutations sorted by Harnser 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 is to be set accordingly as the new upper interval limit (see for example Table 23).

[35] The blue rectangles show the jumps in the ICM vulnerability values per plateau length.

P	O	I	Sum	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value	**New Harnser Interval**
4	5	5	14	0.077	0.154	0.1155	105.0	15.0	15.0	30.0	30.0	30.0	0.090142903	Upper Limit
5	4	5	14	0.077	0.154	0.1155	135.0	45.0	15.0	30.0	30.0	30.0	0.090142903	
5	5	4	14	0,077	0.154	0.1155	135.0	15.0	45.0	30.0	30.0	30.0	0.076622058	Lower Limit

Table 23: Extract from the results with score sum "14" according to Harnser and ICM 1.
Source: Own table.[36]

The same principle is used to adjust each assumed probability interval on the 15-point scale. The results are shown in Table 24:[37]

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

Table 24: Harnser-Vulnerability scale adapted to ICM 1.
Source: Own table.

The plot of the vulnerability values of all 125 permutations according to the size of the Harnser mean values shows a successful alignment of the Harnser scoring system with ICM variant 1 (see Figure 29).

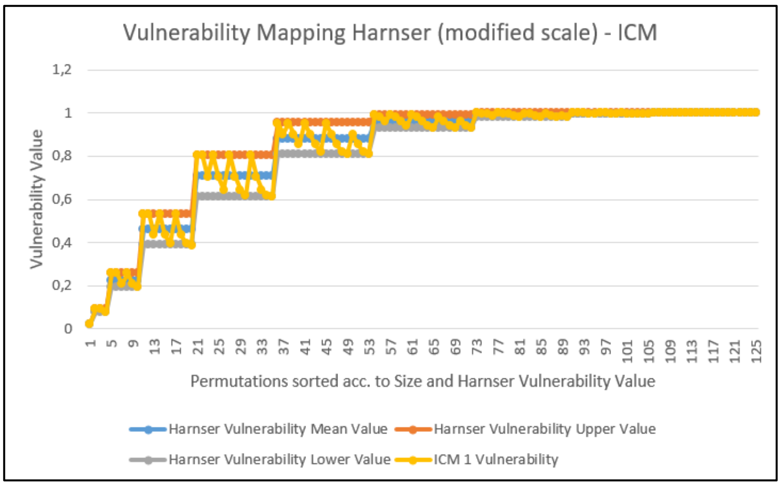


Figure 29: Sorted results of the permutations, ICM 1 - Harnser with modified scale.
Source: Own Figure.

If the Harnser plateaus are sorted according to the ICM-1 values, the result is an almost continuous curve of limited growth (see yellow curve in Figure 30).

[36] New upper interval limit: marked yellow; new lower interval limit: marked blue.

[37] The mean values of the new assumed probability intervals are shown below.

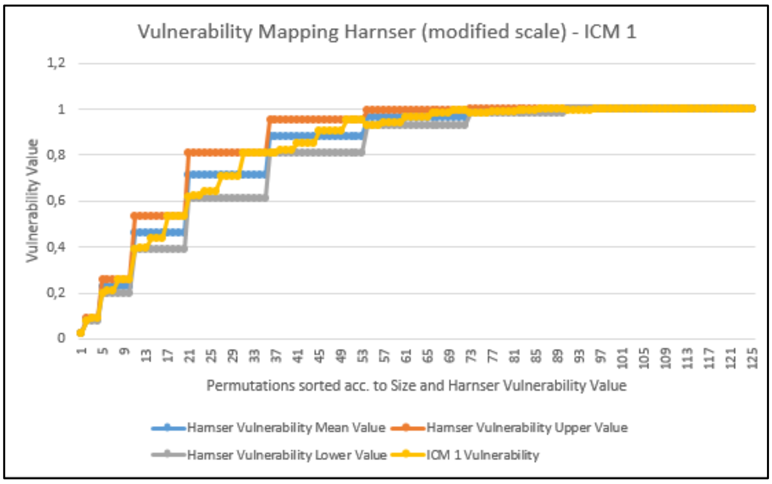


Figure 30: ICM 1 sorted in approximately equal distribution within the Harnser plateaus.
Source: Own Figure.

The yellow curve is a function of the three parameters protection, observation and intervention. These are changed discretely via the arbitrary order of the permutations under consideration (see Table 25). Because the scale of the Harnser metric is adapted to ICM 1 in such a way that it can be used to make objective vulnerability classifications, this modified Harnser metric can be used to make more risk-appropriate decisions regarding investment in security measures. All this with the restriction of the arbitrarily chosen ICM model of a barrier and an asset. It can be shown that the Harnser metric can in principle be significantly improved.

P	O	I	Sum Score	Lower V Value	Upper V Value	Mean V Value	mu_P	mu_O	mu_I	sig_P	sig_O	sig_I	ICM 1 V Value
5	5	5	15	0.024	0.024	0.024	135.0	15.0	15.0	30.0	30.0	30.0	0.0239423
5	5	4	14	0.077	0.09	0.084	135.0	15.0	45.0	30.0	30.0	30.0	0.07662206
4	**5**	**5**	**14**	**0.077**	**0.09**	**0.084**	**105.0**	**15.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.0901429**
5	**4**	**5**	**14**	**0.077**	**0.09**	**0.084**	**135.0**	**45.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.0901429**
5	5	3	13	0.195	0.257	0.226	135.0	15.0	75.0	30.0	30.0	30.0	0.19512503
4	**5**	**4**	**13**	**0.195**	**0.257**	**0.226**	**105.0**	**15.0**	**45.0**	**30.0**	**30.0**	**30.0**	**0.2069107**
5	**4**	**4**	**13**	**0.195**	**0.257**	**0.226**	**135.0**	**45.0**	**45.0**	**30.0**	**30.0**	**30.0**	**0.2069107**
3	**5**	**5**	**13**	**0.195**	**0.257**	**0.226**	**75.0**	**15.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.2566896**
4	**4**	**5**	**13**	**0.195**	**0.257**	**0.226**	**105.0**	**45.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.2566896**
5	**3**	**5**	**13**	**0.195**	**0.257**	**0.226**	**135.0**	**75.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.2566896**
5	5	2	12	0.388	0.534	0.461	135.0	15.0	105.0	30.0	30.0	30.0	0.38785009
...	...	...	...	...	...	...	...	...	...	...	...	...	...
4	**1**	**5**	**10**	**0.81**	**0.954**	**0.882**	**105.0**	**135.0**	**15.0**	**30.0**	**30.0**	**30.0**	**0.9536712**
3	**5**	**1**	**9**	**0.931**	**0.994**	**0.963**	**75.0**	**15.0**	**135.0**	**30.0**	**30.0**	**30.0**	**0.9313987**

Table 25: Extract of the calculated permutations, ICM values per plateau sorted by size.
Source: Own table.[38]

How Figure 30 shows, the ICM vulnerability values at the transitions between two plateaus under consideration not only show upward kinks, but also downward kinks. The lowest ICM-Vulnerability value of the "higher" plateau is lower than the highest value of the "lower" plateau. In Table 25 marked in red is an example of this: With ICM 1, a vulnerability of 95.4 % is

[38] V := Vulnerability. All table values were sorted in ascending order according to the "ICM 1 V Value" column. Permutations that generate the same vulnerability values for a specific score sum in a quantitative way are marked in orange, green and blue. A transition of the ICM vulnerability values from one plateau to the next plateau is marked in red with a downward bend.

calculated for the permutation P = "4", O = "1" and I = "5" (score sum "10"). The permutation P = "3", O = "5" and I = "1" (score sum "9") results in a vulnerability of 93.1 % based on ICM 1. In conclusion, the configuration P = "3", O = "5" and I = "1" is better than the configuration P = "4", O = "1" and I = "5". However, the Harnser scoring suggests that it is the other way around due to the different score totals.

In specific applications, however, it may be the case that the mean values and standard deviations of protection, observation and intervention take on different characteristics than in the case of ICM 1. One possibility may be that a user of the scoring system must first choose how high the scattering of the parameters protection, observation and intervention is qualitatively assessed. This assessment can be made in levels by specifying them: For example, there are levels A, B and C. Behind each of these levels is a clearly defined ICM variant with specific mean values and standard deviations for the scorings from "1" to "5". For each ICM variant there could then be a Harnser scoring with adapted scales. This scale is defined in such a way that the Harnser results can replicate the ICM results of an ICM variant. This means that ICM vulnerability values lie in the plateaus of the assumed probability intervals according to Harnser.

It is conceivable that, in the case of this work, a reference work could be developed for the special case with a barrier and an asset, in which there are adapted Harnser scales that find an equivalent in an ICM variant, for example:

- If level A is present, this corresponds to an ICM variant X, and the scoring system with scale division I must be selected.
- If level B is present, this corresponds to an ICM variant Y, and the scoring system with scale division II should be selected.
- If level C is present, this corresponds to an ICM variant Z, and the scoring system with scale division III should be selected.
- Etc.

The following is an example to illustrate this: The proposed scale from Table 24 for the scoring-based assessment of vulnerability maps the result space of ICM variant 1. If the results of all permutations of ICM variant 30 from Table 17 are also displayed in Figure 29, it becomes apparent that the scale from Table 24 can only partially replicate ICM 30 results (as indicated by the red markings in Figure 31). The results of the scoring based on the modified scale for ICM 1 are not quantitatively compliant with ICM 30 in many areas. The Harnser metric is defined as quantitatively compliant if it is calibrated with regard to the combination of the assessment parameters and the assessment scale in such a way that results can be generated that correspond to the results from the quantitative ICM. In the case of quantitative conformity of the scoring-based metric, the assessments of both metrics (Harnser and ICM) lead to the same classifications of vulnerability. In this case (ICM 30 versus Harnser), the results according to Harnser are in many parts not in agreement with the quantitatively calculated ICM 30 results. Here, the scoring scale should have different upper and lower interval limits for the assumed probability per score sum.

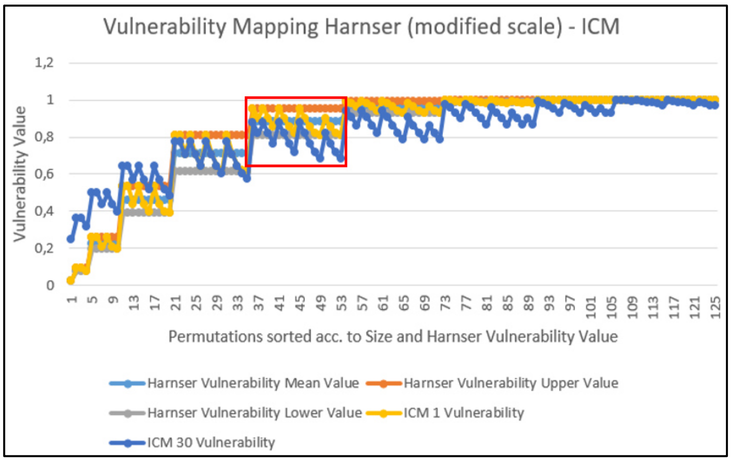


Figure 31: Sorted permutations ICM 1, ICM 30 and Harnser with modified scale for ICM 1.
Source: Own Figure.

The procedure for adjusting the scoring to ICM 30 is the same as for the previous scale adjustment: The calculated entries belonging to each individual plateau are analyzed. The minimum ICM 30 value and the maximum ICM 30 value per plateau are then determined. The maximum ICM 30 value is defined as the new upper interval limit of the assumed probability interval, the minimum ICM 30 value as the new lower interval limit. Table 26 lists the scales of the Harnser metric for mapping the ICM 1 variant and for mapping the ICM 30 variant. A column-by-column comparison between the quantitatively compliant Harnser scale for ICM 1 and the quantitatively compliant Harnser scale for ICM 30 makes it clear that each assumed probability interval is different.

Harnser scale that can replicate 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
Harnser scale that can replicate ICM 30													
V Score	3	4	5	6	7	8	9	10	11	12	13	14	15
Lower Value	0.967	0.967	0.967	0.967	0.93	0.868	0.784	0.682	0.573	0.483	0.396	0.316	0.246
Upper Value	1	1	1	1	0.992	0.976	0.941	0.876	0.773	0.641	0.497	0.36	0.246
Mean Value	0.9835	0.9835	0.9835	0.9835	0.961	0.922	0.8625	0.779	0.673	0.562	0.4465	0.338	0.246

Table 26: Comparison of the quantitatively compliant Harnser scale for ICM 1 and ICM 30.
Source: Own table.

The plot of the vulnerability results according to Harnser with a modified scale for the ICM 30 variant and according to ICM 1 and ICM 30 in Figure 32 shows that the Harnser scoring can be successfully adapted to ICM 30. At the same time, this scale adjustment means that it is no longer quantitatively consistent with ICM 1 results.

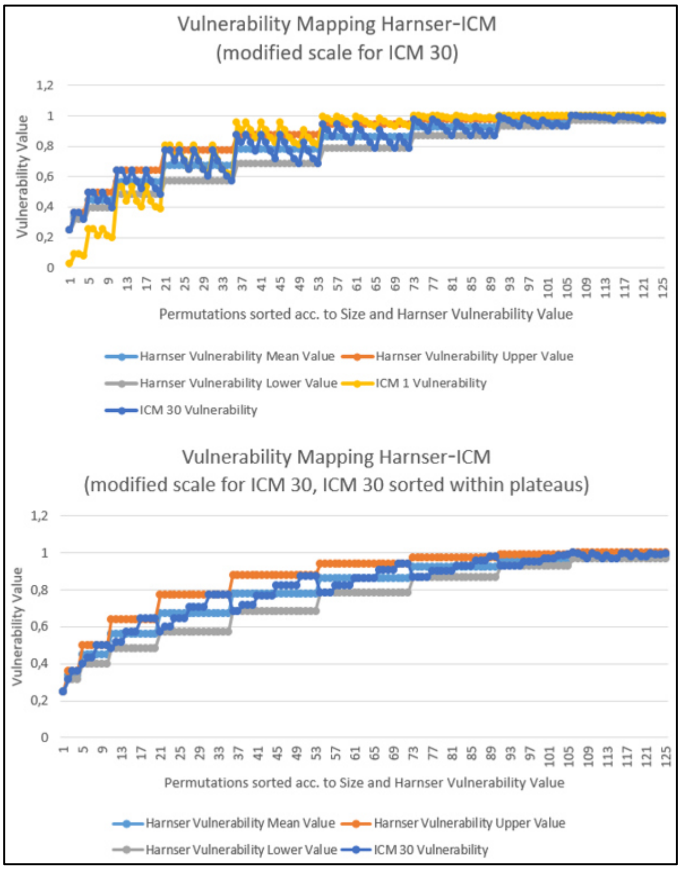


Figure 32: Sorted permutations ICM 1, ICM 30 and Harnser with modified scale for ICM 30.
Source: Own Figure.

A Harnser scale that combines both variants, i.e. covers results from ICM 1 and ICM 30 via corresponding plateaus, is shown in Table 27 is shown. For each Harnser plateau, the minimum and maximum ICM value must be determined for the ICM 1 and ICM 30 variants. These two values are defined as the lower and upper interval limits of the assumed probability interval according to Harnser. By adapting the Harnser scale to two ICM variants, a security margin can be mapped. The mean values and standard deviations behind each score therefore have a range, which is spanned here by the variants ICM 1 and ICM 30. The interval limits overlap. The results are shown in Figure 33 plotted. If two ICM variants are taken into account when converting to Harnser scores, the assumed probability intervals per plateau become larger, as in the comparison between Figure 31 and Figure 33 and between Figure 32 and Figure 33 becomes clear. The Harnser scale can be adapted to other ICM variants using the same procedure as described above. As shown in Figure 33, the interval limits overlap.

Harnser scale, which can replicate ICM 1 and ICM 30													
V Score	3	4	5	6	7	8	9	10	11	12	13	14	15
Lower Value	0.967	0.967	0.967	0.967	0.93	0.868	0.784	0.682	0.573	0.388	0.195	0.077	0.024
Upper Value	1	1	1	1	1	1	0.994	0.954	0.807	0.642	0.497	0.36	0.246
Mean Value	0.9835	0.9835	0.9835	0.9835	0.965	0.934	0.889	0.818	0.69	0.515	0.346	0.2185	0.135

Table 27: Quantitative conformal Harnser scale for ICM 1 and ICM 30.
Source: Own table.

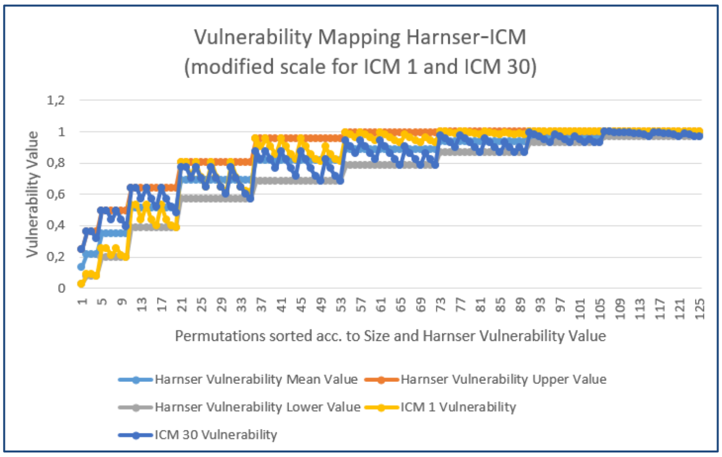


Figure 33: Sorted permutations ICM 1, ICM 30 and Harnser with "combined" scale.
Source: Own Figure.

3.2 Analysis of the Common Vulnerability Scoring System Metrics

The Common Vulnerability Scoring System (CVSS) of FIRST.org[39] is an industry standard. It was developed by the Special Interest Group (SIG) (Cheng et al., 2014, p. 11). It covers technical features of software, hardware and firmware of IT systems (First.org, 2022). CVSS is used worldwide and version 3.1 is available as of May 2022 (Risk-based Security, 2017). CVSS is an open, vendor- and platform-independent framework for assessing the severity of security vulnerabilities based on the exploitability of vulnerabilities and the impact associated with exploitation. In IT security, vulnerability is assessed based on system-inherent vulnerabilities (First.org, 2022; ISO/SAE, 2021b; Kumar et al., 2017). A vulnerability is a necessary condition for being able to conduct an attack, but not a sufficient condition. The sufficient condition is that there is an attack vector that also leads to an exploit. Exploitability means that a theoretical vulnerability can be successfully exploited. The measure for assessing vulnerabilities is therefore exploitability. In ISO/SAE 21434, the degree of exploitability is classified using an attack feasibility scale (ISO/SAE, 2021b, p. 1).

The successful exploitation of a vulnerability is accompanied by damage. This is, for example, a compromise of confidentiality, availability or integrity or a combination of the three. According to ISO/SAE 21434, a vulnerability can be understood as the absence of a measure or requirement or as an inadequate configuration (ISO/SAE, 2021b, p. 5). It is exploitable if there is at least one attack vector that leads to damage. For this reason, the Attack Vector parameter is also used in CVSS for vulnerability assessment (see Figure 34). According to ISO/SAE 21434, an attack vector combines several sub-steps in order to successfully reach a target (ISO/SAE, 2021b, p. 2). According to the CVSS specification v.3.1, attack vectors describe "the context by which vulnerability exploitation is possible" (First.org, 2022). The attack vector thus describes the effort required to successfully exploit a vulnerability. In CVSS, the effort is divided into "Physical", "Local", "Adjacent" and "Network". For the "Physical" attack vector, for example, it says "The attack requires the attacker to physically touch or manipulate the vulnerable component" (First.org, 2022). An attack path can therefore potentially consist of several attack vectors (contexts). According to ISO/SAE 21434, an attack path is "a set of deliberate actions to realize a threat scenario" (ISO/SAE, 2021b, p. 2). A threat scenario is a "potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario" (ISO/SAE, 2021b, p. 4).

[39] FIRST stands for "Forum of Incident Response and Security Teams" (First.org, 2022), a non-profit organization.

Attack paths generally represent a combination of possible sources for obtaining information. Attack paths can be arbitrarily complex across the application level (software and hardware of a product), the system level (web application servers, virtual machines), the network level (communication links and forms of connection, e.g. switches, firewalls, virtual private networks or routers) and the physical infrastructure level (building access, server rooms) (Nguyen et al., 2020). With CVSS, the compromise of a specific asset is assigned to a single attack vector (context) (First.org, 2022). The results of a CVSS assessment are vulnerability scores from "0" to "10", which can be used to prioritize security measures. As the CVSS links exploitability (vulnerability) and impact (effects), it would make more sense to rename the "vulnerability score" to "risk score". This can also be justified by the definition of "risk" in ISO/SAE 21434: "[Risk describes the] effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact" (ISO/SAE, 2021b, p. 4). One way to determine attack feasibility according to ISO/SAE 21434 is to use CVSS scoring (ISO/SAE, 2021b, p. 47).

CVSS consists of three metric groups, the Base Metric, the Temporal Metric and the Environmental Metric (see Figure 34). The base metric, referred to below as the base metric, is used to determine a constant vulnerability over time that is valid for all configurations of an IT system. The most severe effects (worst-case scenarios) are always assumed, partly due to a lack of evidence. The results of the basic metrics are generally published, e.g. under Common Vulnerabilities and Exposures (CVE, 2021), as these do not change over time and apply to all affected IT systems. The SIG proposes supplementing the basic score with temporal and environment-specific scores in order to obtain a severity level that reflects the vulnerability for a provider's specific use cases. The temporal metrics supplement the basic severity level of a vulnerability with temporally variable factors. One example of this is the assessment of the availability of exploitable code. Environmental metrics, also known as environmental metrics, adapt the basic and temporal vulnerability metrics to a specific use case and its environmental boundary conditions. Monetary losses due to successful attacks are not explicitly taken into account in CVSS, but can be supplemented accordingly as required (First.org, 2022).

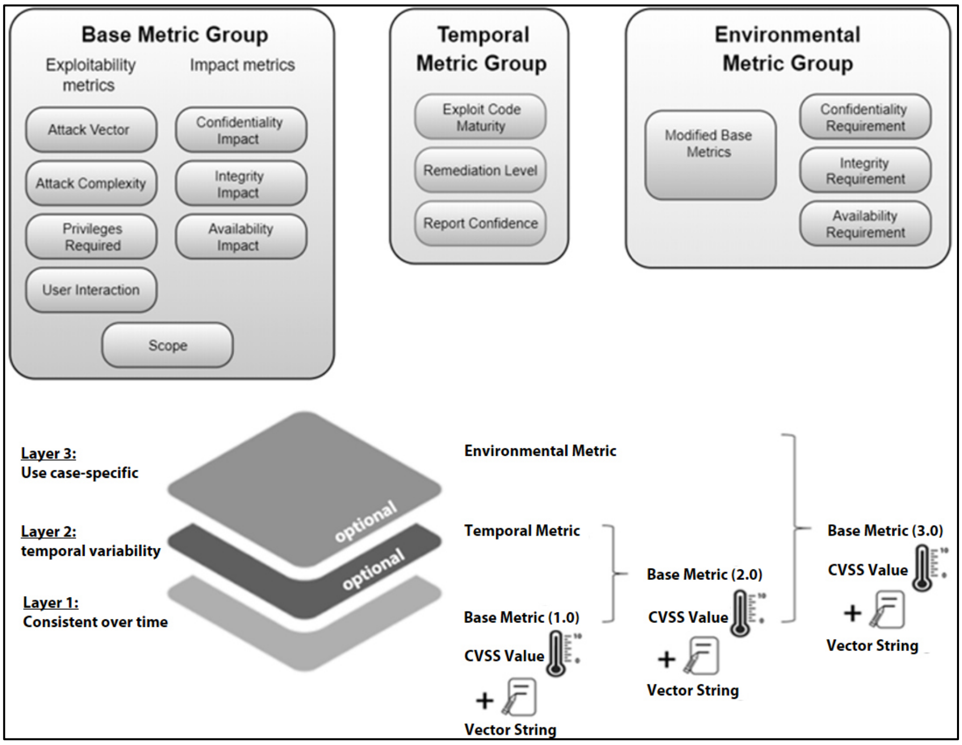
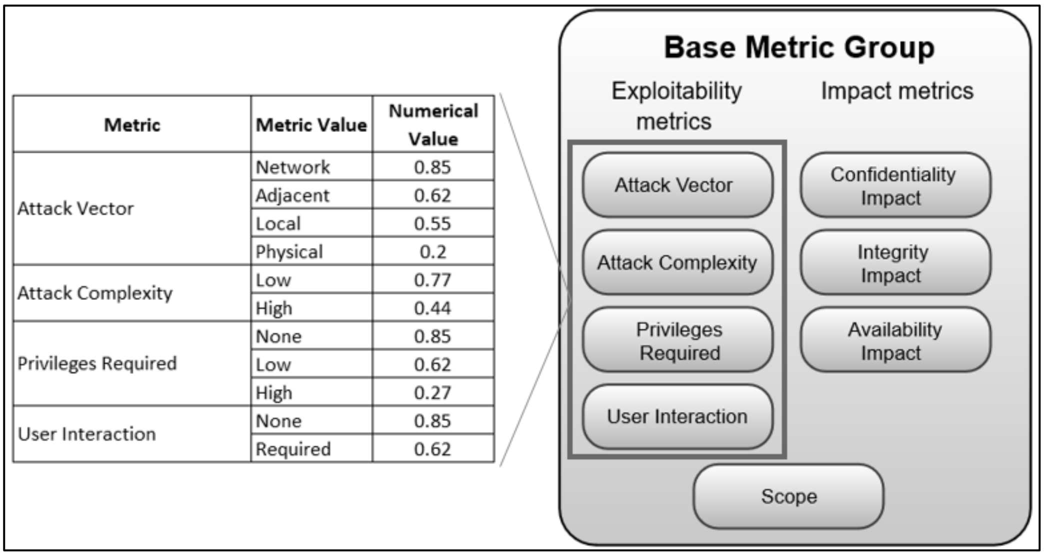


Figure 34: Metric groups of the Common Vulnerability Scoring System.
Source: Own Figure based on First.org (2022). Image source: flaticon.com (2021).

In the course of the CVSS assessment, a textual representation of the assessments according to the three metrics is also generated. It is called a vector string and contains the name of the metric as well as the set score value. For the analysis of the CVSS metric, the basic metric group in version 3.1 is used (see Figure 35).



Metric	Metric Value	Numerical Value
Attack Vector	Network	0.85
	Adjacent	0.62
	Local	0.55
	Physical	0.2
Attack Complexity	Low	0.77
	High	0.44
Privileges Required	None	0.85
	Low	0.62
	High	0.27
User Interaction	None	0.85
	Required	0.62

Figure 35: Composition of the CVSS base score.
Source: Own figure based on First.org (2022) and Ghani et al. (2013).[40]

There are exploitability metrics and impact metrics in the basic metrics. The exploitability metrics consist of the parameters (called "metrics" in CVSS) Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI). The AV defines the context of an attack: "Can an attacker attack from a distance or does he have to be physically present, for example?". The AC describes "the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. [...] such conditions may require the collection of more information about the target, or computational exceptions". (First.org, 2022). According to CVSS, PR is used to assess "the level of privileges an attacker must possess before successfully exploiting the vulnerability". UI in turn comprises "the level of privileges an attacker must possess before successfully exploiting the vulnerability" (First.org, 2022). Each of these parameters assesses different aspects of a vulnerability. The impact metrics are made up of the impact of the protection goals of confidentiality, integrity and availability. There is also the scope, which is used to map a change in scope as a result of an attack:

> The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. [...] Formally, a security authority is a mechanism (e.g., an application, an operating system, firmware, a sandbox environment) that defines and enforces access control in terms of how certain subjects/actors (e.g., human users, processes) can access certain restricted objects/resources (e.g., files, CPU, memory) in a controlled manner. (First.org, 2022).

Each of the CVSS metrics consists of descriptors, e.g. for AC "Low" and "High". These are assigned a discrete, numerical value between zero and one. These numerical values can be interpreted as contributions to exploitability, which are to be estimated by experts. In a first step, the frequency of the vulnerability scores is examined for all possible combinations. The CVSS

[40] The exploitability E is defined in CVSS v.3.1 by E = 8.22 · AV · AC · PR · UI. The scope change is not shown in the table.

does not cover the entire result space between 0 and 10 due to the possible score combinations: "The full range is not used: while the maximum score is 10.0, the minimum score ever achieved is 1.6. That means that there are 101 - 16 = 85 actual degrees in use" (Chester, 2021).

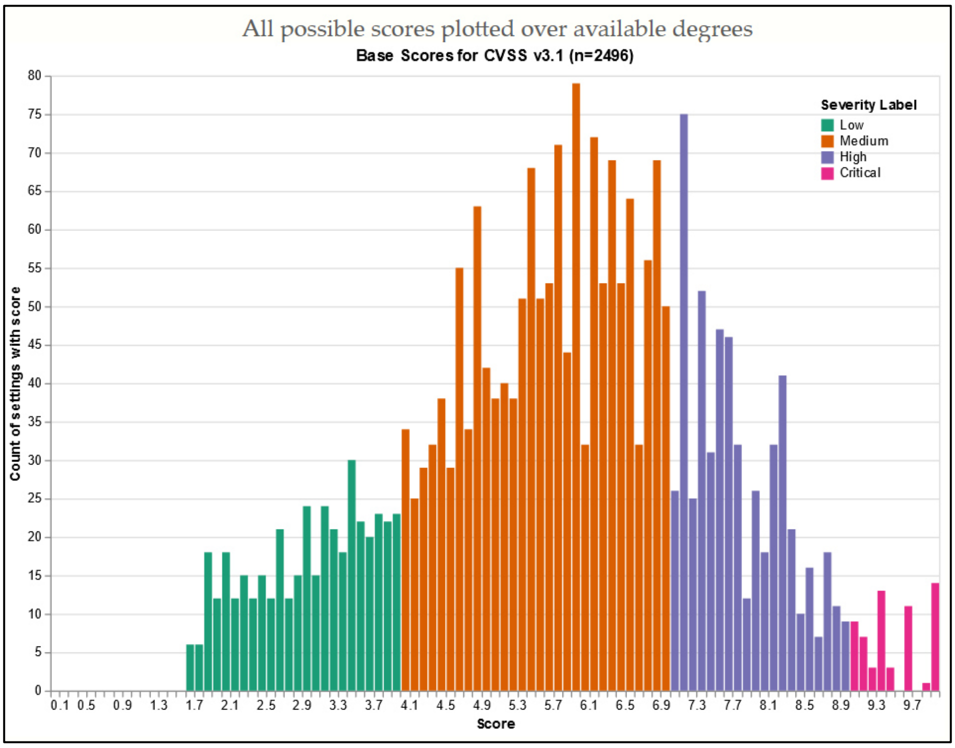
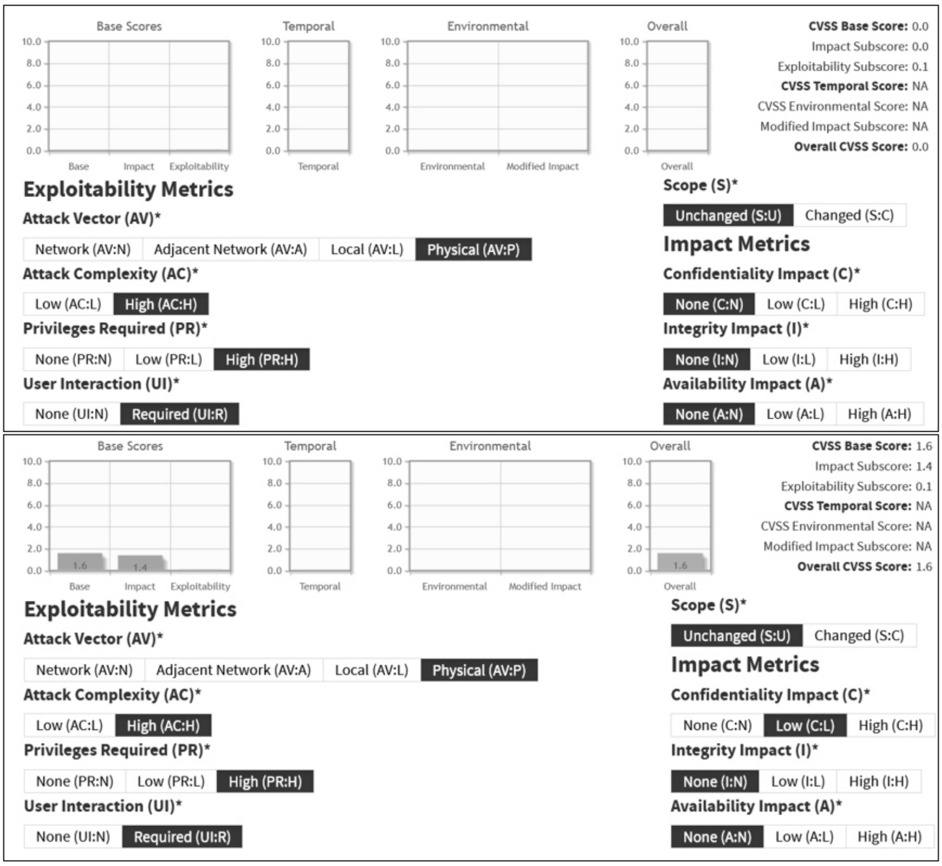


Figure 36: Plot of all possible CVSS vulnerability scores.
Source: Chester (2022).

From the presentation of the frequencies of the vulnerability scores in Figure 36, it can be seen that the next lowest score to 1.6 has the value zero (see Figure 37). This is only the case if there is no impact, i.e. confidentiality, availability and integrity are set to "None".



CVSS Base Score: 0.0
Impact Subscore: 0.0
Exploitability Subscore: 0.1
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 0.0

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | [✓ Physical (AV:P)]

Attack Complexity (AC)*
Low (AC:L) | [✓ High (AC:H)]

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | [✓ High (PR:H)]

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
[✓ Unchanged (S:U)] | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
[✓ None (C:N)] | Low (C:L) | High (C:H)

Integrity Impact (I)*
[✓ None (I:N)] | Low (I:L) | High (I:H)

Availability Impact (A)*
[✓ None (A:N)] | Low (A:L) | High (A:H)

CVSS Base Score: 1.6
Impact Subscore: 1.4
Exploitability Subscore: 0.1
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 1.6

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | [✓ Physical (AV:P)]

Attack Complexity (AC)*
Low (AC:L) | [✓ High (AC:H)]

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | [✓ High (PR:H)]

User Interaction (UI)*
None (UI:N) | [✓ Required (UI:R)]

Scope (S)*
[✓ Unchanged (S:U)] | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | [✓ Low (C:L)] | High (C:H)

Integrity Impact (I)*
[✓ None (I:N)] | Low (I:L) | High (I:H)

Availability Impact (A)*
[✓ None (A:N)] | Low (A:L) | High (A:H)

Figure 37: CVSS vulnerability scores, comparison of configurations.
Source: NIST CVSS (2022).

In addition, the CVSS shows that physical attacks can never achieve the same level of vulnerability as network attacks. One reason for this is that physical has the numerical value 0.2 and network has the numerical value 0.85. Secondly, there is no weighting of physical attacks and network attacks in the CVSS metric for determining the vulnerability score. This means that, for example, it is not possible to take into account how large the proportion of physical infrastructure and IT infrastructure is in specific use cases. The assumption "Physical = 0.2" and "Network = 0.85" requires assumptions. One such assumption can be according to Wurm (2022):

> Physical attacks are [...] no less likely [than network attacks], but they require at least time-limited access. The window of opportunity for attacks on internet connections is practically infinite and also easily scalable, as globally distributed resources (and accomplices) can be integrated. (Wurm, 2022, p. 49)

The CVSS specifications of First.org (2022) do not clearly state all the assumptions used to determine the numerical values behind the values of the assessment parameters. The assessment using the CVSS metrics to determine the vulnerability score is "not justified, either formally or empirically" (Spring et al., 2018, p. 1). For example, an infrastructure could be more physically developed than in terms of information technology. This should be reflected in CVSS, but it is not. CVSS criticism from reports by the IT community since 2007 is summarized in Spring et al. (2018, p. 3) as follows: Inadequate consideration of context (both technical and human-organizational); failure to consider the material consequences of a threat (whether life or property is threatened); problems with operational assessment (inconsistent or clustered assessments, weaknesses in algorithm design).

Braband (2004) warns against using scores on an ordinal scale in the same way as quantitative values, e.g. on a cardinal scale. Allodi et al. (2018) emphasize that the CVSS metric does not make mathematical sense because the expert data on exploitability contributions are ordinal values. On the website TheoryOf by Chester (2021), the problem is clearly explained as follows:

> CVSS v3.1 scores should be considered as rankings, which makes them an ordinal measure. Ordinal measures can't be added, multiplied or divided in a meaningful way, which rules out averaging. Imagine that there was no numerical score, only the linguistic scores of "Critical", "High", "Medium" and "Low". What's the average of "Critical" and "Medium"? Of "High" and "Low"? There isn't one. (Chester, 2021).

Krisper (2021) explains the problem in this way:

> While one would refrain from multiplying "words" like high risk and moderate impact together, doing this with arbitrarily assigned numbers suddenly seems plausible. For example, if high risk = 3 and moderate impact = 3, then the risk is 6, but what is the meaning of 6? (Krisper, 2021, p. 5).

The problem of calculating with ordinal values is also shown in Petr et al. (2022).

3.2.1 Reduction of Metric Distortions through Logarithmization

To determine exploitability, four parameters are assessed in the CVSS according to First.org (2022): Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI). Braband (2019) now proposes interpreting the CVSS exploitability parameters as barriers connected in series. This should correspond to the principle of Defense in Depth (DiD). The following classifications are used: AV stands for the location of the IT attack (physical barrier), AC for the complexity of the attack from a technical point of view (technical barrier) and PR for the required rights on the part of the user or UI for the necessity of user interaction (organizational barrier). The individual barriers are interpreted as independent of each other, which means, for example, that the PR barrier has no influence on the UI barrier. If there is independence between the barriers, the exploitability contributions of AV, AC, PR and UI can be linked multiplicatively.

In the barrier-based CVSS approach, a Likelihood of Exploitability (LoE) score is determined by adding the individual exploitability contributions and sorting them on a rating scale. To enable the addition of the exploitability contributions, Braband (2019) proposes the log transformation of the numerical CVSS values. The approach in Braband (2019) is based on the observation that a quantitative risk approach can be transformed into a semi-quantitative approach (addition of CVSS scores) by applying a logarithm to the quantitative model. The applicability of this idea is subject to the condition that the exploitability contributions must be multiplied quantitatively. This is assumed for the CVSS ($E = 8.22 \cdot AV \cdot AC \cdot PR \cdot UI$) (First.org, 2022). In addition, the log transformation can only be performed if the values to be transformed are positive. This is the case for the numerical values behind the values of the CVSS assessment parameters. The log transformation has the advantage that the individual exploitability contributions can potentially move on a scale of several orders of magnitude, e.g. over several decades (Braband, 2008). The scaling of exploitability or risk contributions cannot be represented either additively or multiplicatively with the CVSS assessment, which is why logarithmization is used.

The base b of the logarithm can be chosen according to the "resolution" of the semi-quantitative scale (Braband, 2019). In principle, however, any base b can be chosen, since the logarithm is a mathematical function that has the same mathematical properties regardless of the base: When data is logarithmized, its mathematical properties do not change, regardless of which base is chosen. The logarithm to base 10, for example, has the advantage that it is easy to understand. This is especially true in the context of measurements and scales that use a decimal system. According to Braband (2008), a log-transformed assessment approach has the following properties: continuity of the scale, rational scaling, monotonicity, comparability and sensitivity. In the following, using the example of the CVSS, it is shown analytically that logarithmizing reduces distortions within a multiplicative scoring metric:

In IT security, risk is viewed as a composite event consisting of threat, vulnerability (exploitability) and impact. The individual contributions of the risk (elementary events) are classically linked multiplicatively, so that an IT risk can be calculated assuming Eq. (1) (P(threat) = 1). It is composed of the exploitability E and the impact I (see Eq. (2)):

R = Exploitability x Impact (2)

If the events E and I do not influence each other, the IT risk can be written as a multiplication of E and I (see Eq. (3)):

$$R = E \cdot I \tag{3}$$

In IT security, risks are described using scoring-based metrics. Numbers are classified on a rating scale according to the levels of the individual contributions. If E and I were scaled linearly, IT risk scores could be calculated that are proportional to the true risk (see Eq. (4)):

$$r = e \cdot i \tag{4}$$

If the relationships between the numerical values and risk contributions are non-linear, this can lead to distortions: A risk assessment based on numerical values corresponds to different real risk values. These distortions will be demonstrated using the example of CVSS. The CVSS assessment parameters AV, AC, PR and UI have different numbers of levels:

1. AV: four levels
2. AC: three stages
3. PR: three levels
4. UI: two levels

With the help of experts, an equal number of levels can initially be defined for the assessment parameters of CVSS, according to the assumption, e.g. four levels per assessment parameter (see as an example Table 28). These levels are understood here as true contributions to exploitability, even if, strictly speaking, they are subjective expert assessments (ordinal values).

Score	AV	Score	AC	Score	PR	Score	UI
1	0.2	***1***	***0.11***	***1***	***0.11***	***1***	***0.16***
2	0.55	2	0.44	2	0.27	***2***	***0.39***
3	0.62	3	0.77	3	0.62	3	0.62
4	0.85	4	0.85	4	0.85	4	0.85

Table 28: Exploitability levels and exploitability contributions.
Source: Own table based on First.org (2022).[41]

The step values are plotted according to size. The curves are then each represented by a regression function (see Figure 38). Approximately linear relationships are assumed behind the individual exploitability contributions.

[41] Additions in italics are examples.

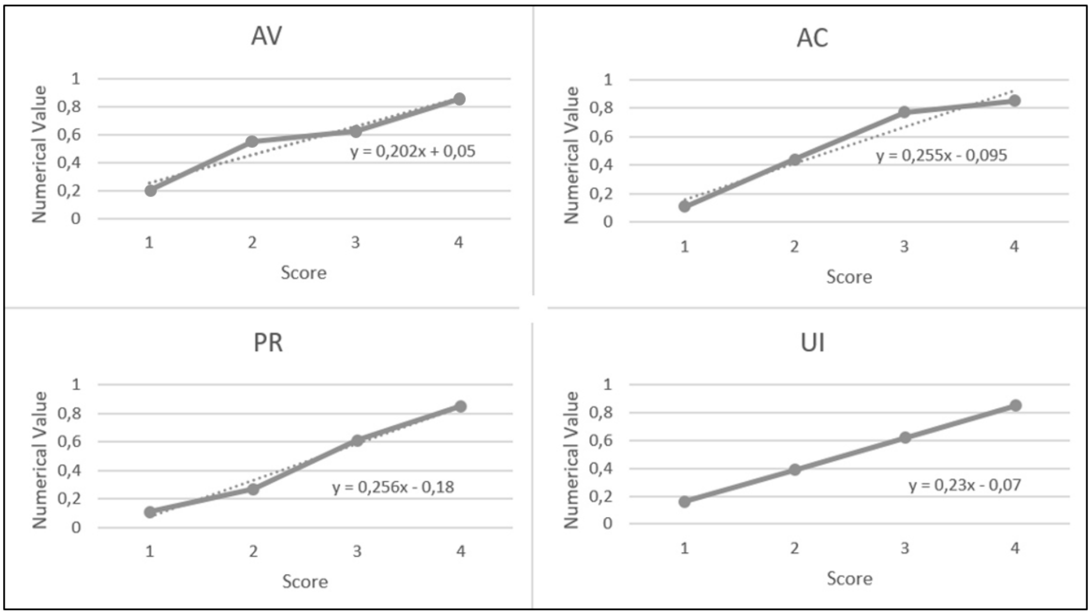


Figure 38: Plot of the exploitability contributions of CVSS.
Source: Own Figure.

The exploitability contributions AV, AC, PR and UI and Impact I are included in the risk assessment. The product of AV, AC, PR and UI is assumed to be the probability of exploitability (Lyu et al. 2020).[42] For Impact I, the correlation $I = 10^i$ [Euro] is assumed (see Table 29).

Score	Impact (Euro)	
1	10	10^1
2	100	10^2
3	1000	10^3
4	10000	10^4

Table 29: Impact levels and monetary loss values.
Source: Own Figure.

The exploitability contributions are calculated on the basis of the Table 28 and the Figure 38. The following correlations are assumed (see Eq. (5)):

1. AV = 0.202 · av + 0.05
2. AC = 0.255 · ac - 0.095
3. PR = 0.256 · pr - 0.18
4. UI = 0.23 · ui - 0.07

(5)

For the parameter combinations "av = 1, ac = 2, pr = 3, ui = 4, i = 1" and "av = 4, ac = 3, pr = 2, ui = 1, i = 1", following the semi-quantitative metric, the same risk value ($r_1 = r_2 = 24$). However, the real risk is different for both cases, as the following calculation shows (see Eq. (6)):

$$R_k = (0.202 \cdot av + 0.05) \cdot (0.255 \cdot ac - 0.095) \cdot (0.256 \cdot pr - 0.18) \cdot (0.23 \cdot ui - 0.07) \cdot 10^i$$
with av, ac, pr, ui, i = 1 ... 4

$$R_1 = (0.202 \cdot 1 + 0.05) \cdot (0.255 \cdot 2 - 0.095) \cdot (0.256 \cdot 3 - 0.18) \cdot (0.23 \cdot 4 - 0.07) \cdot 10^1 = 0.52 \text{ [Euro]} \quad (6)$$

[42] Multiplying the contributions from AV to UI makes sense if it is assumed, as in Braband (2019), for example, that AV to UI are barriers of a weak point in series connection.

$$
\begin{aligned}
&R_2\\
&= (0.202 \cdot 4 + 0.05) \cdot (0.255 \cdot 3 - 0.095) \cdot (0.256 \cdot 2 - 0.18) \cdot (0.23 \cdot 1 - 0.07) \cdot 10^1\\
&= 0.31 \text{ [Euro]}
\end{aligned}
$$

If the risk contributions are scaled differently, a proportional relationship between the level values of the risk contributions and the logarithmic risk can be established again by means of a transformation. This is illustrated using the example of the five-part IT risk assessment "$R = AV \cdot AC \cdot PR \cdot UI \cdot I$" or "$r = av \cdot ac \cdot pr \cdot ui \cdot i$". The constant (8.22), as used in the CVSS calculation formula for exploitability[43] , is omitted here as it only scales the exploitability value. The order of the risk values remains unchanged. By logarithmizing the IT risk function R with the relationship in Eq. (7):

$$\log_b x = \frac{\ln x}{\ln b} \tag{7}$$

the logarithm can be formed for the individual risk contributions AV, AC, PR, UI and I. The base 10 is selected for the impact valuation parameter (see Eq. (8)).

$$
\begin{aligned}
&\ln R\\
&= \ln AV + \ln AC + \ln PR + \ln UI + \ln 10 \frac{\ln I}{\ln 10}\\
&= \ln AV + \ln AC + \ln PR + \ln UI + \ln 10 \cdot \log_{10} I
\end{aligned} \tag{8}
$$

Inserting the numerical values for av, ac, pr, ui and i gives (see Eq. (9)):

$$
\begin{aligned}
&\ln(r)\\
&= ln(0.202 \cdot \text{ av} + 0.05) + ln(0.255 \cdot \text{ac} - 0.095)\\
&\quad + ln(0.256 \cdot \text{pr} - 0.18) + ln(0.23 \cdot \text{ui} - 0.07) + \ln(10) \cdot i
\end{aligned} \tag{9}
$$

For the parameter combinations "av = 1, ac = 2, pr = 3, ui = 4, i = 1" this leads to ln(r) = - 0.648 and for "av = 4, ac = 3, pr = 2, ui = 1, i = 1" to ln(r) = - 1.186. The real IT risk contributions result from applying the inverse function to $e^{-0.648} = 0.52$ [Euro] or $e^{-1.186} = 0.31$ [Euro]. These correspond to the risk values R_1 resp. R_2 from Eq. (6). Consequently, if the risk description contains multiplicative correlations, but the scoring is characterized by additive correlations, then the log transformation is a sensible step to reduce distortions such as those found in the multiplicative scoring metric. It should be noted that a user could also enter values such as "3.5" or "5" in the risk contribution functions. To avoid this, the strict assumption must be defined that only the scores "1", "2", "3" and "4" may be used for the function of a risk contribution in this case.

3.2.2 Analysis of the Barrier-based CVSS Approach

In Braband (2019), the numerical values of the exploitability contributions from the CVSS are transformed into log scores. The base to which logarithms are applied in Braband (2019), for example, is set to 0.6: The choice of this base is justified by the fact that the numerical values of the exploitability contributions span a value range from 0.2 to 0.85 (≈ 0.6) range. In Braband (2019), the resulting log scores are rounded up to integer values to simplify the presentation of the results.[44] As an example, in Eq. (10) the transformation is performed for the "Physical" characteristic of the AV parameter:

$$log_{0.6}(\text{AV} = \text{"Physical"}, \text{num. value} = 0.2) = log_{0.6}(0.2) = 3.15 \approx 3 \tag{10}$$

[43] Exploitability = 8.22 · Attack Vector · Attack Complexity · Privileges Required · User Interaction.

[44] Rounding rule: If the first decimal place of the digit is 0, 1, 2, 3 or 4, then it is rounded down. If the first decimal place of the digit is a 5, 6, 7, 8 or 9, round up.

All CVSS values from AV to UI can be calculated using the formula in Eq. (10). They can be transformed into new numerical values or log scores using the logarithm. The log scores associated with the values of the assessment parameters are shown in Table 30.

AV	**Physical**	**Local**	**Adjacent**	**Network**
Num. value	0.2	0.55	0.62	0.85
log score, base = 0.6	3	1	1	0

PR	**None**	**Low**	**Medium**	**High**
Num. value	0.85	0.62	Not defined	0.27
log score, base = 0.6	0	1	2	3

AC	**Low**	**Medium**	**High**
Num. value	0.77	Not defined	0.44
log score, base = 0.6	0	1	2

UI	**None**	**Required**
Num. value	0.85	0.62
log score, base = 0.6	0	1

Table 30: Log-transformed CVSS scores.
Source: Braband (2019).[45]

The choice of the base to which a data set is log-transformed influences the scaling and thus also the interpretation of the transformed values. However, it has no influence on the calculation of a true risk value. An example is shown below to illustrate this: The AV scale is logarithmized once to base 0.6 (as suggested in Braband) and once to base 3 as an example (see Eq. (11) and Eq. (12)):

$$\log - \text{Transformation from}\, AV\ to\ Basis\ 0.6 = \ln 0.6 \frac{\ln AV}{\ln 0.6} = \ ln\ 0.6 \cdot \log_{0.6} AV \tag{11}$$

For AV = Physical (0.2), Eq. (11) the value -1.6. A reverse transformation using $e^{-1.6}$ results in 0.2.

$$\log - \text{Transformation from}\, AV\ to\ Basis\ 3 = \ln 3 \frac{\ln AV}{\ln 3} = \ ln\ 3 \cdot \log_{3} AV \tag{12}$$

For inserting AV = Physical (0.2) into Eq. (12), the value -1.6 results. $e^{-1.6}$, the inverse function, gives 0.2. The result is identical in both cases. The likelihood of exploitability score (LoE) is calculated by forming the sum of the log-transformed exploitability contributions (see Eq. (13))[46] :

$$\text{LoE} \ = \ log_{0.6}(AV) + \ log_{0.6}(AC) + \ log_{0.6}(PR) + \ log_{0.6}(UI) \tag{13}$$

The result space of the LoE values is then sorted into scale categories (Braband 2019). The lowest value sum "0" corresponds to a very high probability level, the values "1-3" to a high probability level, etc. (see Table 31). A set of LoE values is thus assigned to a specific likelihood category. In addition to the log transformation of the numerical values of the exploitability contributions, it is proposed to assign the categories that can be written behind LoE score results to a series of barriers (see Table 31 third row).

[45] If attackers can carry out potential attacks remotely (context: network), this is more serious from the operator's point of view than conducting attacks with the context physical. Reasons for this may be, for example, that there are a variety of possible entry points at network level and the effort required by attackers may be less than in the case of a physical attack.

[46] The scope change is not taken into account here.

Likelihood	VL	L	P	UL	VUL
LoE score	0	1-3	4-5	6-7	8-9
Barriers	0	1	2	3	4

Table 31: LoE scale based on the CVSS barrier model.
Source: Braband (2019).[47]

In Braband (2019), instead of "$ln\ 0.6 \cdot \log_{0.6} AV$", only "$log_{0.6}(AV)$", is the obvious assumption, because "$log_{0.6}(AV)$" generates positive log values. The use of "$ln\ 0.6 \cdot \log_{0.6} AV$" results in negative log values (see Eq. (14):

$$1.\ log_{0.6}(AV = 0.2) = 3.15 \qquad (14)$$
$$2.\ ln\ 0.6 \cdot \log_{0.6}(AV = 0.2) = \text{-}1.6$$

In addition to the specific protective effect (the LoE score), the barrier depth is also included in the assessment. The addition of a further barrier would have no influence on the LoE if a score of "0" was set for the new barrier. According to the approach, there is a reduction in the LoE if a score greater than "0" is set for the new barrier. The LoE decreases with each additional barrier. Assuming, for example, that the variable "System Check" (SC) is considered as a fictitious procedural barrier with the exemplary values low (log score "0") and high (log score "1") in the barrier-based CVSS scheme, the LoE score (here LoEmod) is calculated using Eq. (15):

$$\text{LoEmod} = log_{0.6}(AV) + log_{0.6}(AC) + log_{0.6}(PR) + log_{0.6}(UI) + log_{0.6}(SC) \qquad (15)$$

Based on LoEmod, there would be a further category on the exploitability scale, e.g. "Very very unlikely := Very very unlikely (VVUL)" A reverse transformation of the LoE scores can be performed using Eq. (16) (see Table 32 fourth and fifth row). [48]

$$\text{e} = e^{\ln(0.6) \cdot LoE\ Score} \qquad (16)$$

Likelihood	VL	L	P	UL	VUL	VVUL
LoE score	0	1-3	4-5	6-7	8-9	10
Barriers	0	1	2	3	4	5
Probability Interval DiD = 4	1	0.216 - 0.6	0.078 - 0.13	0.028 - 0.047	0.01 - 0.017	/
Probability Interval DiD = 5	1	0.216 - 0.6	0.078 - 0.13	0.028 - 0.047	0.01 - 0.017	0.006

Table 32: LoE classifications based on the barrier-based CVSS metric.
Source: Own table based on Braband (2019).

If it is assumed that the numerical values of CVSS correspond to real contributions to exploitability (as interpreted, for example, in Lyu et al. (2020)), then the back-transformed log score sums can be interpreted as the probability of exploitability. As can be seen in Table 32, there are gaps in the exploitability value range from 0 % to 100 %. This is due to the integer jumps between the individual LoE scores. For example, if there were a LoE score of "3.5", the probability of exploitability would be $\text{e} = e^{\ln(0.6) \cdot 3.5} = 0.167$ result. The following points can be identified in this context:

1. An exploitability of "e = 1" can never be achieved according to the quantitative risk description of CVSS, as the largest product of "AV · AC · PR · UI" (0.85^4 =) is 0.522.

[47] "Very Likely = Very Likely (VL)", "Likely = Likely (L)", "Possible = Possible (P)", "Unlikely = Unlikely (UL)", "Very Unlikely = Very Unlikely (VUL)".

[48] The "e" on the left-hand side of the equation denotes the exploitability. The "e" on the right-hand side refers to Euler's number.

2. The smallest product that can be represented by the multiplicative relationship of CVSS is (E = 0.2 · 0.44 · 0.27 · 0.62 =) 0.0147. However, according to the barrier-based CVSS assessment, as proposed in Braband (2019), lower exploitability values can also be mapped (see Table 32).

What is the reason for this difference? In Braband (2019), the numerical values of the exploitability contributions are transformed using $log_{0.6}(Exploitability\_Beitrag)$ and then rounded to integer values: The exploitability contribution $log_{0.6}(0.85)$ = 0.318, for example, becomes $log_{0.6}(0.85) \approx$ 0. This is one of a total of four contributions that are added together. Taking into account the maximum CVSS values, the log score sum for the non-rounded log-transformed values is (0.318 + 0.318 + 0.318 + 0.318 + 0.318 =) 1.272. In contrast, following the assessment scheme in Braband (2019) results in a log score sum of (0 + 0 + 0 + 0 =) 0 for the same CVSS values. A reverse transformation results in a difference between the two variants of $|e^{\ln(0.6)\cdot 0} - e^{\ln(0.6)\cdot 1.272}$= 1 - 0.522 = 0.478(!) (see observation point one above). If the product of the exploitability contributions actually corresponded to a probability (in %), then the approach in Braband (2019) would sometimes lead to large misjudgements due to the rounding of the log scores. An important open point noted in the barrier-based CVSS approach is the assignment of LoE scale categories to probabilities (Braband 2019).

As the exploitability contributions of the quantitative CVSS metric have not yet been empirically proven (Spring et al., 2018), it is questionable to what extent the application of the LoE scale actually delivers better results than the classic CVSS approach. It is difficult to verify or falsify with the CVSS metrics whether the consideration of the barrier depth in the context of the exploitability assessment according to CVSS brings about improvements. This is different from the physical security assessment. Here, the security capability of a system can be objectively measured on the basis of the interplay between the intrusion time of an attacker and the reaction time of a defender along a path. The path itself can consist of several barriers. Consequently, a quantitative metric is needed to systematically analyze the postulated DiD effect.

Because a metric with an objective mechanism of performance for objectively assessing security capability is difficult to find in IT security assessment so that the efficiency of the CVSS path can be recalculated, Termin et al. (2022) propose emulating architectural and metric considerations from the barrier-based CVSS approach in physical security assessment.[49] In Termin et al. (2022), the problem of applying semi-quantitative metrics is highlighted from an IT perspective. In the analysis according to Termin et al. (2022), the architecture of the physical system was redesigned to emulate the postulated DiD effect as proposed in the IT security assessment. For this purpose, protection (P), observation (O) and intervention (I) are interpreted as performance-based barriers: The protection-heavy barrier, the observation-heavy barrier and the intervention-heavy barrier have properties of protection, observation and intervention respectively. One of the three assessment variables is emphasized for each barrier, while the others are less pronounced.

This means that there is a specific interaction of all three assessment parameters for each barrier. The protection-heavy barrier, for example, has an emphasized protection, but also low

[49] The emulated variant is developed in Termin et al. (2022) to quantitatively replicate the influence of the DiD effect postulated in Braband (2019). These considerations lead back to the question of whether it can be shown in physical security that better vulnerability results are generated when resources for security measures are distributed across multiple, sequentially connected barriers instead of placing all resources on a single barrier. In the classic Harnser scheme and the CVSS, no distinction is made between individual barriers and barriers in series. For this reason, neither the Harnser metric nor the CVSS can be used to map a DiD effect. This is possible with the quantitative Intervention Capability Metric.

observation and intervention components; otherwise the vulnerability at the barrier would be maximum. To illustrate the principle of performance bias, mean values and standard deviations of the normally distributed parameters are defined in the Intervention Capability Metric(ICM) according to Lichte et al. (2016) in such a way that the assumed probability interval resulting from the sum of the integral parameters protection, observation and intervention can be quantitatively recalculated. A cost function is introduced to compare the vulnerability results over the sum of the integral parameters and over the ICM. The results of the analysis in Termin et al. (2022) show that the DiD addition proposed in the barrier-based CVSS approach provides better results in the CVSS assessment for some scenarios. However, emulation did not produce clear results. In the following, distortions within the barrier-based CVSS approach are discussed and improvements are proposed.

3.2.3 Reduction of Distortions in the Barrier-based CVSS Approach

In physical security, each assessment parameter of the Harnser metric has the same level depth (score "1" to score "5"). In contrast to physical security, the barrier-based CVSS assessment scheme has different levels of depth. The significance of the different levels can be seen when comparing the barrier-based approach according to CVSS with the approach according to Harnser. For example, AV has four slots, "Physical", "Local", "Adjacent" and "Network", while UI only has two in the classic CVSS, "None" and "Required". The likelihood of exploitability scale (LoE) would therefore change depending on the barrier depth and barrier type. Assume that the "AV barrier" is activated first. AV covers a log score range from "0" to "3". The UI barrier is then set. UI ranges from log score "0" to "1". According to the DiD principle, this would mean two barriers in series. If AV is in the first position and UI in the second position, the scale division would be as follows (see Table 33):

Category:	Likely	Possible
LoE score	0-3	4
Barriers	1 (AV)	2 (UI)

Table 33: LoE for series connection of AV and UI.
Source: Own table based on Braband (2019).

If the barriers are swapped, i.e. UI is switched first and then AV, the categorization of the LoE scale may look different (see Table 34).

Category:	Likely	Possible
LoE score	0-1	2-4
Barriers	1 (UI)	2 (AV)

Table 34: LoE for series connection of UI and AV
Source: Own table based on Braband (2019).

Insofar as in the permuted variant (in Table 34) AV is substituted by AC, this results in a LoE score range of "2" to "3" in the second column. If the barriers are swapped again here, so that AC is set first and then UI is switched, the score range of the values behind the categories would change again. This in turn means that the order of the barriers can have an influence on the assessment of exploitability according to the barrier-based CVSS approach. In addition, the PR and UI barriers can each assume the value "None". However, a "None" means that there is no PR or UI barrier. PR and UI are therefore a type of binary switch. If an expert now sets the barriers to "None" when connecting PR and UI in series, a "DiD = 0" (maximum exploitability) must also be found in the LoE categorization. Although this is suggested in the approach described in Braband (2019), the other parameters, AC and AV, always have a minimum value, unlike UI and PR. There is no "None" value for AV or AC. However, if only the AV barrier were present, and assuming theoretically that there was an "AV = None" value, this would mean that

1. There is no barrier, i.e. DiD = 0. According to the barrier-based CVSS metric, this means maximum exploitability.
2. There is no context for a threat scenario. If there is no context, then there is no exploitability.

These two points contradict each other. The assessment level from AV to UI is different. Consequently, there are distortions in the CVSS assessment scheme. This CVSS assessment scheme requires that AV must always be taken into account as an assessment parameter and must not be "None". This is different from the emulated, barrier-based approach in the physical security assessment according to Termin et al. (2022). For example, if there is no protection-heavy, observation-heavy or intervention-heavy barrier in the system under consideration, the missing barrier can be removed from the assessment without this leading to distortions. In the emulated security assessment, the boundary case DiD = 0 does not exist if it is assumed that there is at least one physical barrier. This is because a certain level of performance is assumed for each physical barrier in the emulated approach. Maximum vulnerability - and therefore DiD = 0 - could only be mapped here if there are no barriers at all, i.e. neither a protection-heavy barrier, nor an observation-heavy barrier or an intervention-heavy barrier.

Applied to the barrier-based CVSS assessment scheme, the previous considerations mean that, in the sense of a good metric (see chapter 2.4), the same level of abstraction should be selected for the parameters and their values. In conclusion, it is proposed that the existing "None" values for CVSS be replaced by a descriptor that describes a concrete activation level not equal to zero. Conversely, if DiD = 0 is to be mapped for all possible permutations of IT barriers, i.e. also in the case of the series connection of AV and AC, there would have to be the values "None" for both AV and AC. However, as this can be ruled out from a logical point of view (without the AV barrier, there is no context for a threat scenario), the former variant is preferable. In addition, in the emulated approach in physical security, comparable levels are selected for all three parameters, protection, observation and intervention. There are scores from "1" to "5" for each parameter.

With regard to the assessment scheme introduced in Braband (2019), this allows a consistent scale classification with regard to the distribution of scores across the scale categories. In the barrier-based CVSS approach, however, the classification of scores into categories is different due to the different depth of the parameter values (e.g. for AV = 4 and for UI = 2) and the arrangement of the barriers. In order to meet this challenge, consideration can be given to structuring the parameters in the same way with regard to their depth of expression, so that AV to UI have comparable level depths (see for example Table 35). The proposed additions are highlighted in italics.

AV[1]	Physical	Local	Adjacent	Network
Numerical Value	0.2	0.55	0.62	0.85
Score	3	1	1	0

[1] Attack Vector

AC[2]	Low	Medium	High	***Very High***
Numerical Value	0.77	***Not defined***	0.44	***Not defined***
Score	0	***1***	2	***3***

[2] Attack Complexity

PR[3]	***Low (User)***	***Medium (Owner)***	***High (Manager)***	***Very High (Developer)***
Numerical Value	0.85	0.62	***Not defined***	***Not defined***
Score	0	1	***2***	***3***

[3] Privileges Required

UI[4]	***Low (User)***	***High (User)***	***Low (Admin)***	***High (Admin)***
Numerical Value	0.85	0.62	***Not defined***	***Not defined***
Score	0	1	***2***	***3***

[4] User Interaction

Table 35: Modification of the barrier-based CVSS scoring to adjust the LoE scale.
Source: Own table based on Braband (2019).

Applied to the definition of the characteristics of a PR barrier, this means, for example, the change from "None", "Low", "High" to "Low", "Medium", "High" and "Very High". It is assumed that there must be some form of required rights. Behind the individual levels can be roles and associated rights, for example simple user, user with administrative rights (e.g. team leader), manager and developer. For the UI barrier, it is somewhat more difficult to extend "None" and "Required" to activated levels. Here, for example, consideration can be given to dividing the level of user interaction into four levels. This means asking how many user actions a user must perform to facilitate exploitation and what type of user must perform a user action (see Table

35).[50] Exploitation is probably easier for actions by a simple user than for actions by system administrators.

A change to a metric per se generally requires a justification that the change better reflects real risks. It can first be shown that the three proposed modifications reduce distortions within the CVSS metric:

1. The log transformation reduces metric-inherent distortions if the risk description has multiplicative correlations.
2. Activation of the parameter values so that the values are not equal to zero: This modification resolves the problem of defining a DiD = 0 in the barrier-based CVSS approach compared to the physical security assessment. DiD = 0 can only exist if either UI or PR assume "None". However, there is no "None" for AV and AC. If AV and AC would now stand as barriers without UI and PR, then the assessment scale would be different than if UI or PR or both assessment variables were taken into account.
3. Each parameter has the same number of levels: This modification allows the scale division in the barrier-based CVSS approach to be normalized by defining: With each barrier added, another category is added that has the same score range in width as the previous categories.

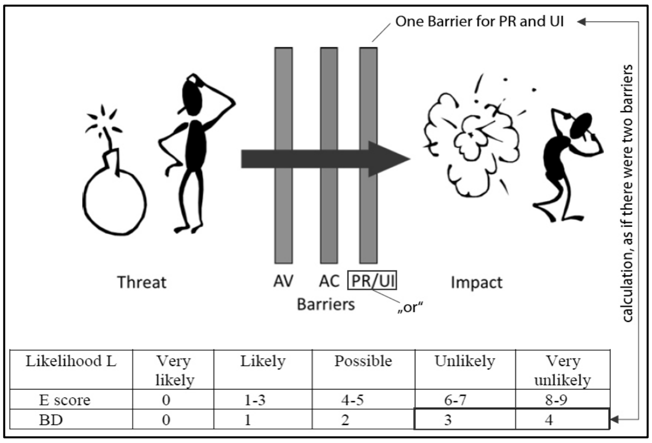
The assessment parameters from AV to UI have the following Table 35 each have four levels. In the Harnser metric, protection, observation and intervention each have five levels. Consideration can now be given to defining the same number of levels per vulnerability contribution in both the IT vulnerability assessment and the physical vulnerability assessment, e.g. five levels for each vulnerability contribution. For the CVSS, this would mean that a fifth threat context must be identified and defined for the AV. A fifth level must also be defined for the contributions from AC to UI. The expansion of the scales of the exploitability contributions should be consolidated with experts. In principle, this task presents a user of the CVSS assessment metric with challenges that are difficult to solve because this fifth level may not even exist. This approach is therefore impractical. Instead of adapting the scale levels from the CVSS to the Harnser metric, the scale levels of protection, observation and intervention can be adapted to the CVSS scales:

It is conceivable that only four levels - instead of five - could be defined for protection, observation and intervention. However, the fifth level of scoring for the contributions of physical vulnerability must not simply be deleted. Deleting it would mean disregarding a level of security capability in the security assessment. If the levels of protection, observation and intervention are compressed, then a redefinition of the meaning of these levels is necessary. The redefinition of meaning comprises two dimensions: The first dimension relates to the descriptors of the new proficiency levels. The first dimension relates to the descriptors of the new proficiency levels. The new levels are intended to provide a comparable scope of security capabilities to the previous levels. For example, does the new protection level "1" include a very low protective effect or a very low to low or even moderate protective effect? Experts should be consulted when redefining the scales. The second dimension relates to the conversion of the new scores into quantitative values that can be used as input for the quantitative ICM (see chapter 3.1). In order to make the Harnser scale quantitatively compliant with objective vulnerability levels, it is first necessary to determine mean values and standard deviations for the scores from "1" to "4". This also requires expert knowledge.

In general, the previous explanations show that the adaptation of scale levels must be carefully considered. Arbitrary compression or expansion of scales with different dimensions may not

[50] The meaningfulness of this definition is discussed in the following chapter.

be feasible or expedient. Scores are inherently uncertain. The reduction of scale levels, for example, would help to increase the information content behind a score. Alternatively, however, the harmonization of the vulnerability scales of both security domains can be pursued. For example, vulnerability scales with the same number of categories can be defined for both (see further explanations in section 3.3.3 and chapter 3.3.4). In addition, the classic CVSS uses four parameters to determine exploitability: AV, AC, PR and UI. In the barrier-based approach, as explained in Braband (2019), the organizational barrier is defined as "Privileges Required (PR) or User Interaction (UI)" (see Figure 39).


One Barrier for PR and UI
Threat
AV
AC
PR/UI
Barriers
„or"
Impact
calculation, as if there were two barriers

Likelihood L	Very likely	Likely	Possible	Unlikely	Very unlikely
E score	0	1-3	4-5	6-7	8-9
BD	0	1	2	3	4

Figure 39: Distortion in the barrier-based CVSS approach.
Source: Own Figure based on Braband (2019).

PR and UI are described as one barrier in the model, but PR and UI are calculated as if they were two separate barriers. However, if it were to be a single barrier, it would be necessary to combine the PR and UI valuation variables into one valuation variable; otherwise there would be a logical inconsistency between the model and the valuation metric. First of all, the extent to which it is possible to merge UI and PR into one valuation metric must be questioned. It must be checked whether UI and PR according to CVSS mean the same thing or describe different things that are not compatible. For this purpose, the meaning of the CVSS assessment parameters is transferred to physical security: from a physical security perspective, PR can mean that an attacker needs the rights of a manager, for example, or those of an employee in order to gain access to a certain building or room. UI would describe the extent to which an attacker needs support (from employees) to conduct their attack. In physical security, for example, this could be a porter who unlocks the computer room for an attacker. UI is used to assess which privileges an attacker must use to reach their target.

PR and UI describe the same thing from two perspectives: PR generally covers what privileges an attacker needs, while UI assesses what help they need from other (in some form) authorized persons so that an attack can be conducted. Dürrwang et al. (2021), for example, do not specify in more detail how privileges are acquired, but only what level of privilege is required to conduct an attack. This approach can be applied to the merging of PR and UI into an assessment parameter or barrier by defining Following Dürrwang et al. (2021), the new assessment parameter PR* consists, for example, of the four characteristics "Execute", "Read", "Write" and "Full Control". Each of the levels is a parameter value not equal to "None". If the exploitability is assessed according to the approach just proposed, then the following assessment scheme results, for example (see Table 36):

AV[1]	Physical	Local	Adjacent	Network
Numerical Value	0.2	0.55	0.62	0.85
Score	3	1	1	0

[1] Attack Vector

AC[2]	Low	***Medium***	High	***Very High***
Numerical Value	0.77	***Not defined***	0.44	***Not defined***
Score	0	***1***	2	***3***

[2] Attack Complexity

PR*[3]	***Full Control***	***Write***	***Read***	***Execute***
Numerical Value	0.33	0.44	***Not defined***	***Not defined***
Score	3	2	***1***	***0***

[3] Privileges Required

Table 36: Modification II of the CVSS scoring to adjust the LoE categories.
Source: Own table based on Braband (2019).[51]

In general, it must be questioned whether it makes sense to split barriers into their basic functionality in the form of AV to UI and place them one behind the other, especially as there is no objective mechanism of performance to enable a quantitative analysis in IT security. The reason for this is that AV to UI are variables that function on a different level than protection, observation and intervention. AV to UI are much more abstract as concepts than the mechanisms considered in the physical domain. AV to UI generally include more parameters and values that contribute than, for example, protection, which is a single parameter measured over time. The probability of protection is an elementary parameter in physical security, which is represented by a distribution over time (Lichte et al., 2016). An AV is initially a representation of the entire scenario (or context), which is described in general terms. This is a larger construct, behind which there is much more and potentially uncertain information than is typical for the mechanisms of protection, observation and intervention.

Despite the fact that the CVSS parameters contain much more information than the assessment parameters from physical security, only discrete exploitability contributions are defined in the CVSS metric. These are also linked multiplicatively at the level of the risk description. This assumes that the CVSS parameters are completely independent of each other, i.e. that they have no influence on each other. The AC parameter, for example, covers the conditions that must be outside the attacker's control in order for a vulnerability to be exploited. This includes the collection of information about the attack target (First.org, 2022). However, the collection of information also includes finding out what level of authorization an attacker must have before an attack in order to successfully exploit a vulnerability (PR). On the other hand, AC also includes the collection of information on whether a human user other than the attacker must be involved in the successful compromise of the vulnerable component (UI). In this regard, the CVSS specification points out: "Importantly, the assessment of this [attack complexity] metric excludes any requirements for user interaction in order to exploit the vulnerability" (First.org, 2022). Part of the AC may also be that an attacker needs to find out in which contexts there are vulnerabilities that could potentially be exploited. However, the effort estimation regarding the potential exploitability of a vulnerability is described by the AV parameter.

Overall, the risk description in the CVSS must be questioned. In physical security, the overall vulnerability of a system is determined V_{ges} is determined by the product of the vulnerability of each barrier a to z, i.e. $V_{ges} = V_a \cdot ... \cdot V_z$. The vulnerability contribution of each barrier is made up of a combination of protection, observation and intervention. In the barrier-based CVSS approach, the overall exploitability is not determined E_{ges} is determined via the product of the exploitability at the individual barriers i to k ($E_{ges} = E_i \cdot ... \cdot E_k$), but via the product of the

[51] The parameter UI in this metric summarizes the two assessment variables UI and PR of CVSS. Metric or descriptive modifications are highlighted in italics.

exploitability contributions from AV to UI. Neither AV nor AC, PR or UI are made up of an interplay of further "sub-exploitability contributions", as is the case in the physical vulnerability assessment. An exploitability contribution is interpreted as a barrier. From a physical security model perspective, this would mean interpreting protection as a barrier, for example.[52]

However, if the barrier-based CVSS approach is understood in such a way that, for example, the exploitability at the AV barrier is determined by scoring AV, then from a physical security perspective this would mean that an expert could immediately classify the vulnerability at this barrier - without first using a vulnerability metric to assess the interaction of protection, observation and intervention. From a physical security perspective, it is difficult to directly assess vulnerability without a metric. It can therefore be argued that even IT security experts cannot assess exploitability directly, i.e. without an underlying exploitability metric. An interpretation of the CVSS assessment parameters as barriers in parallel is not conclusive, as the assessment parameters do not "work in parallel". Each CVSS parameter looks at a different aspect of a vulnerability. They complement each other. A parallel connection also means that a multiplicative relationship between the exploitability contributions can no longer be represented. The meaningfulness of using the logarithm in a parallel connection from AV to UI must then be questioned. In principle, however, it can be shown analytically that the use of the logarithm can reduce distortions in multiplicative scoring metrics. The extent to which the barrier-based CVSS approach brings about an improvement in terms of a more accurate representation of objective exploitability levels cannot be confirmed due to the lack of a quantitative (effectiveness-based) IT security metric that could be used to assess the security capability of measures to reduce exploitability.

3.3 Cross-Domain Assessment

The first part of this chapter begins by explaining the extent to which security levels can be defined for physical security and IT security. It explains how cyber-physical interactions can be assessed and how the severity of an interaction can be used to align the security levels in both domains. In the second part of this chapter, measures and assumptions are developed to enable the alignment of metrics from the physical security and IT security domains. The starting point is the risk functions "Risk = Vulnerability x Impact" for physical security and "Risk = Exploitability x Impact" for IT security. The vulnerability contributions in the physical risk assessment are to be mapped using the Harnser metric, while the exploitability contributions in IT security are to be mapped using the CVSS.

For the alignment of the metrics from both domains, a standardization of the risk contributions is proposed in order to align the scale categories of the risk contributions. The dimensioning of the risk contributions from both security domains is adapted to each other by applying a log transformation. It is then examined how and under what conditions matching security levels from physical security and IT security can be defined. The Harnser metric is used for physical security. The barrier-based CVSS metric is selected for IT security. Possibilities and limitations in the harmonization of metrics from the domains of physical security and IT security as well as in the cross-domain assessment are presented.

[52] The interpretation of protection, observation and intervention as barriers is the starting point for emulating the considerations of barrier-based CVSS in physical security assessment (Termin et al., 2022).

3.3.1 Alignment of Vulnerability Descriptions

In order for the physical security and IT security domains to be successfully aligned and merged, a comparable description of vulnerability is required. To differentiate the vulnerability description in both domains, exploitability ("E") is written for IT vulnerability and "V" for physical vulnerability. If it is assumed that there can be i-barriers in IT security, then the exploitability at the i-th barrier can be described using Eq. (17):

$$E_i = P(E(B_i)) \tag{17}$$

If there are disjunctive barriers in series (see Figure 40) and assuming strict independence, the overall exploitability is the intersection of the individual exploitabilities. The overall exploitability can therefore be calculated as the product of the individual exploitabilities (E_A ... E_Z) (see Eq. (18)):

$$E_{Ges} = P(E(B_A)) \cap P(E(B_B)) \ldots \cap P(E(B_Z)) = E_A \cdot \ldots \cdot E_Z \tag{18}$$

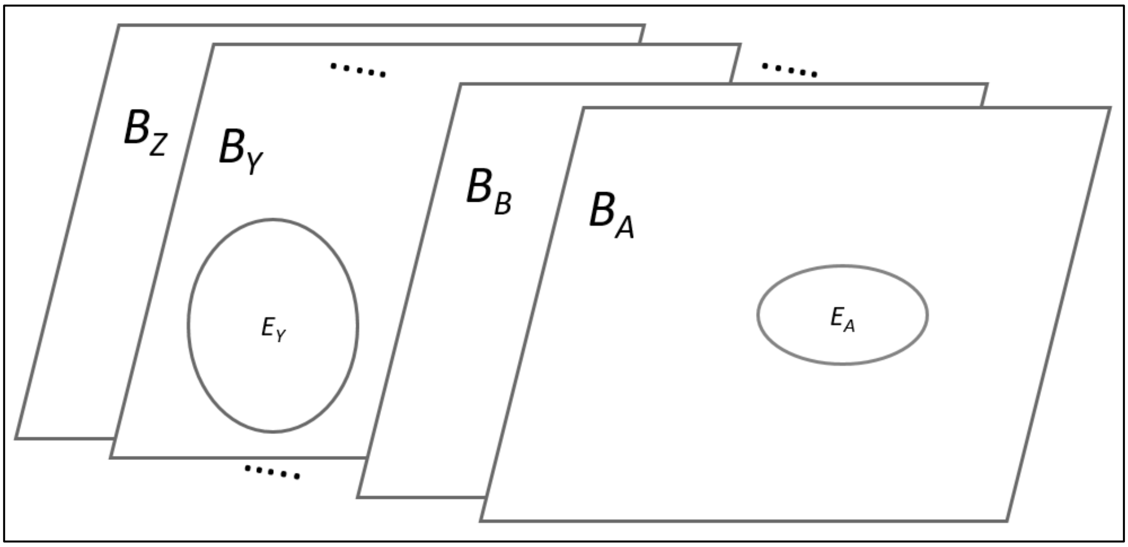


Figure 40: Series connection of disjunctive barriers in IT security.
Source: Own Figure.

In the barriers $B_A\ bis\ B_Z$ from Figure 40 there can be several weak points (see for example Figure 41). The individual vulnerabilities of a barrier make an exploitability contribution to the overall exploitability of this barrier. If $E_A = E_{a_k}$ are disjoint events, then the exploitabilities E_{a_k} at the barrier B_A can be added together. With four assumed vulnerabilities in Figure 41, E_A can be expressed by Eq. (19):

$$E_A = E_{a1} + E_{a2} + \cdots + E_{a3} + E_{a4} \tag{19}$$

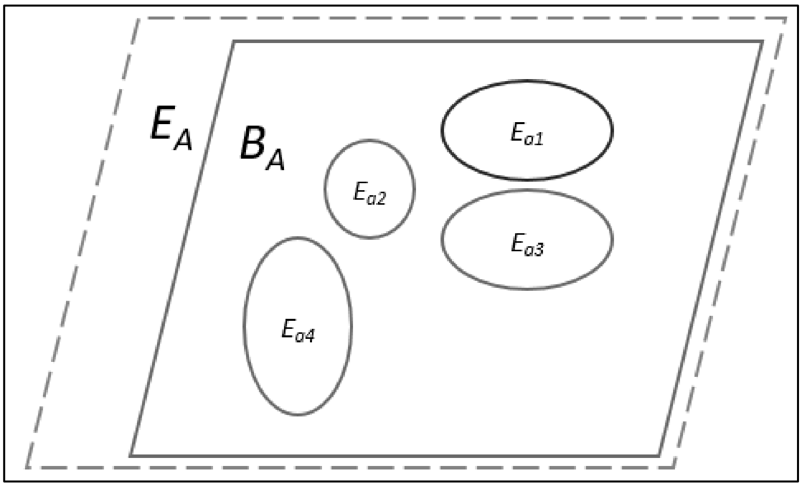


Figure 41: An IT barrier with several weak points.
Source: Own Figure.

The probability for E_A results from Eq. (20):

$$\begin{aligned} &E_A \\ &= P(E_{a1} \cup E_{a2} \dots \cup E_{a3} \cup E_{a4}) \\ &= P(E_{a1}) + P(E_{a2}) - P(E_{a1} \cap E_{a2}) + \dots + P(E_{a3}) + P(E_{a4}) \\ &= E_{a1} + E_{a2} - E_{a1} \cdot E_{a2} + \dots + E_{a3} + E_{a4} \end{aligned} \tag{20}$$

According to CVSS, the exploitability of a vulnerability can be described by four different aspects: the Attack Vector (AV), the Attack Complexity (AC), the Privileges Required (PR) and the User Interaction (UI). If these aspects are understood as disjoint barriers in series, and if strict independence is assumed for this ideal case, then for example for E_{a1} Exploitability can be written by the product of AV to UI (see Eq. (21) and Figure 42). B_J denotes the barriers AV to UI.

$$\begin{aligned} &E_{a1} \\ &= P(E(B_J)) \\ &= P(E(B_{AV})) \cap P(E(B_{AC})) \dots \cap P(E(B_{UI})) = E_{AV} \cdot \dots \cdot E_{UI} \end{aligned} \tag{21}$$

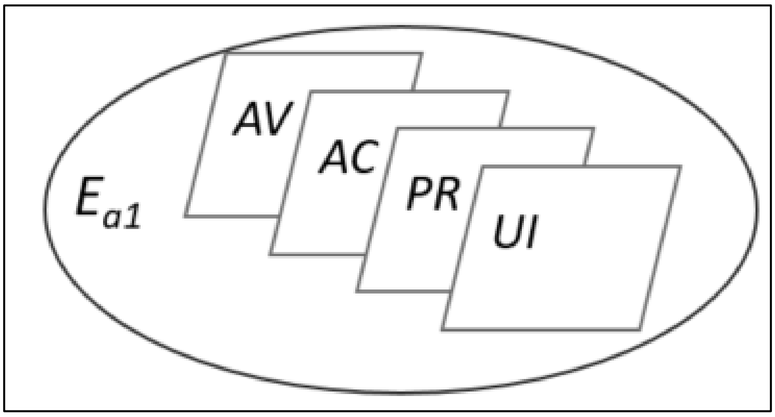
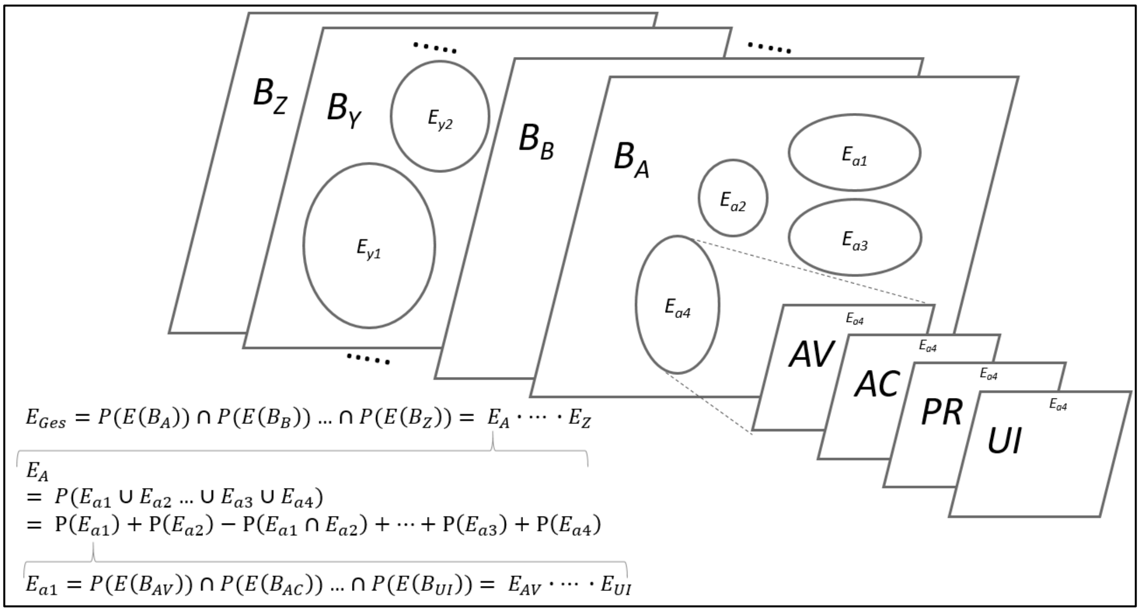


Figure 42: A weak point with several barriers.
Source: Own Figure.

Putting the individual observations together results in the correlations in Figure 43.



$$E_{Ges} = P(E(B_A)) \cap P(E(B_B)) \dots \cap P(E(B_Z)) = E_A \cdot \cdots \cdot E_Z$$

$$\begin{aligned} E_A &\\ = &\ P(E_{a1} \cup E_{a2} \dots \cup E_{a3} \cup E_{a4}) \\ = &\ \mathrm{P}(E_{a1}) + \mathrm{P}(E_{a2}) - \mathrm{P}(E_{a1} \cap E_{a2}) + \cdots + \mathrm{P}(E_{a3}) + \mathrm{P}(E_{a4}) \end{aligned}$$

$$E_{a1} = P(E(B_{AV})) \cap P(E(B_{AC})) \dots \cap P(E(B_{UI})) = E_{AV} \cdot \cdots \cdot E_{UI}$$

Figure 43: Series connection of several (disjunctive) barriers with several weak points.
Source: Own Figure.

The calculation of the exploitability for several vulnerabilities of an IT barrier by summing up the disjoint probabilities (see Eq. (20)) is not correct, however, if an attacker decides on a specific attack path. The events are then not independent of each other. Now it could be assumed that there can be several attackers who attack simultaneously. In physical security, for example, Lichte et al. (2016) assume in a scenario that an attacker decides on an attack path, i.e. a combination of barriers up to the asset. In IT security, however, the definition of the attack path from the physical security perspective can be extended by the dimension "combination of vulnerabilities". As a result, an IT attacker not only selects a combination of barriers up to an asset, but also decides which specific vulnerabilities in the selected barriers are to be exploited (see Figure 44). The principle of the weakest path, as described in Lichte et al. (2016) for vulnerability assessment in physical security, can be transferred to IT security: The weakest IT attack path is the barrier-vulnerability combination with the highest exploitability.

If a barrier has B_A in a fictitious example has two weak points with E_{a1} and $E_{a2}$the probability of exploitability at this barrier (E_A) can also be calculated for the case that the first vulnerability or the second vulnerability is exploited (see Eq. (22)) (Lyu et al., 2020).

$$P(E_A) = \mathrm{P}\,(\,E_{a1}\ \cup\ E_{a2}\,) = \mathrm{P}\,(\,E_{a1}\,) + \mathrm{P}\,(\,E_{a2}\,) - \mathrm{P}\,(E_{a1} \cap\ E_{a2}) \qquad (22)$$

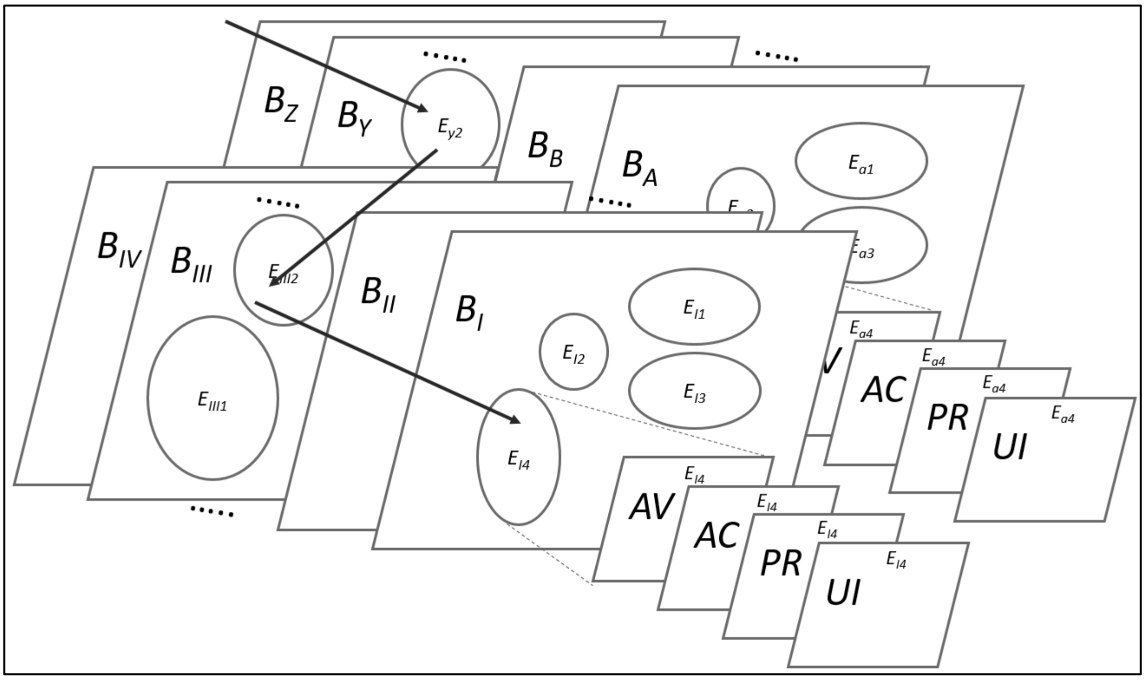


Figure 44: Attack path in IT security with multiple barriers and vulnerabilities.
Source: Own Figure.

In the physical security assessment, e.g. according to Lichte et al. (2016), it is assumed that there can be disjoint barriers in m. The vulnerability at the m-th barrier can be calculated using Eq. (23):

$$V_m = P(V(B_m)) \tag{23}$$

If there are disjoint barriers in series (see Figure 45) and assuming strict independence, the total Vulnerability is the intersection of the individual Vulnerabilities. The total Vulnerability can therefore be calculated as the product of the individual Vulnerabilities (V_A ... V_Z) (see Eq. (24)):

$$V_{Ges} = P(V(B_A)) \cap P(V(B_B)) \dots \cap P(V(B_Z)) = V_A \cdot \dots \cdot V_Z \tag{24}$$

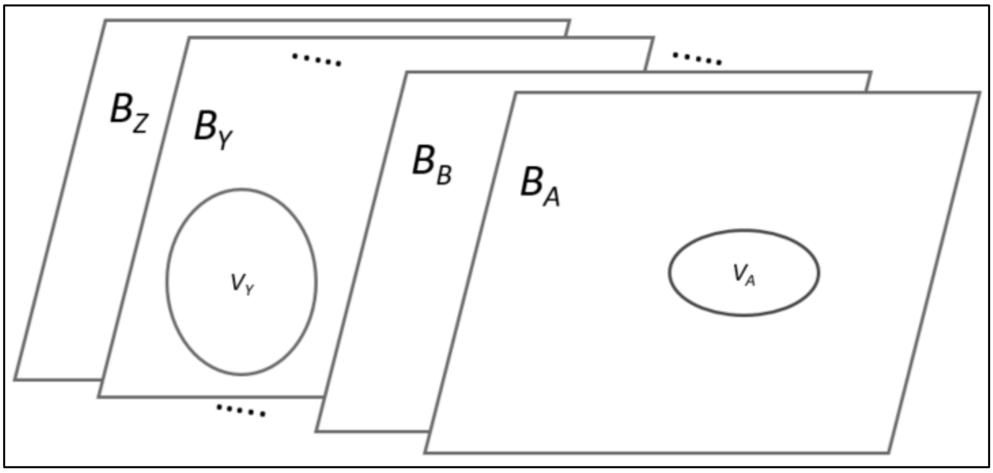


Figure 45: Series connection of disjunctive barriers in physical security.
Source: Own Figure.[53]

[53] The vulnerability assessment using the quantitative vulnerability metric (ICM) according to Lichte et al. (2016) is shown on the right.

The physical vulnerability at a barrier is determined by the interaction of protection, observation and intervention. One way of calculating vulnerability, for example, is to apply the vulnerability metric according to Lichte et al. (2016) (for a schematic representation, see Figure 46).

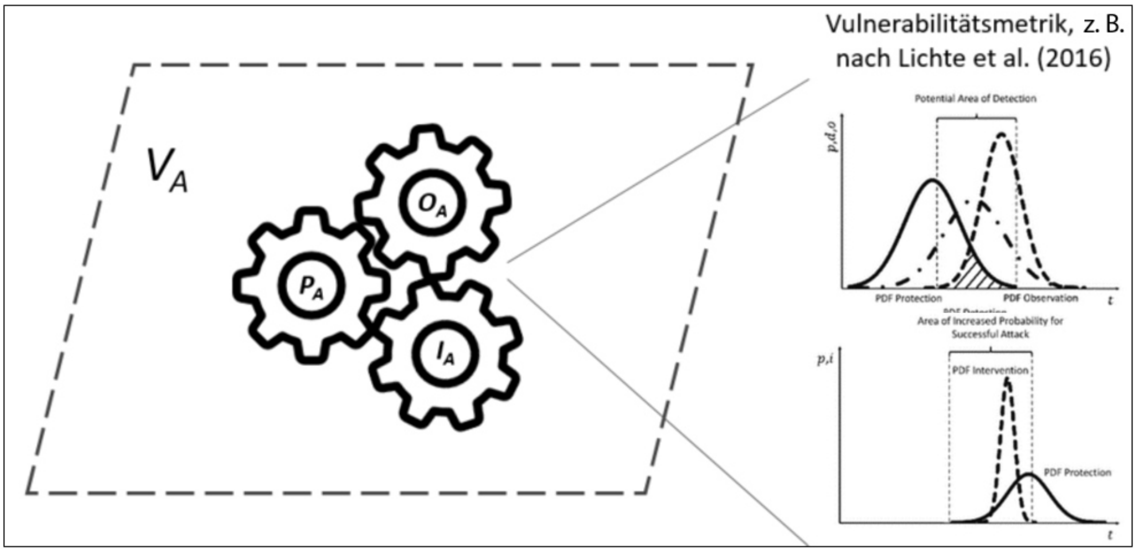

Vulnerabilitätsmetrik, z. B. nach Lichte et al. (2016)
V_A
O_A
P_A
I_A
Potential Area of Detection
p,d,o
PDF Protection
PDF Observation
PDF Detection
t
Area of Increased Probability for Successful Attack
p,i
PDF Intervention
PDF Protection
t

Figure 46: Physical vulnerability at a barrier.
Source: Own Figure based on Lichte et al. (2017).

The path model in the physical security assessment thus results in Figure 47.

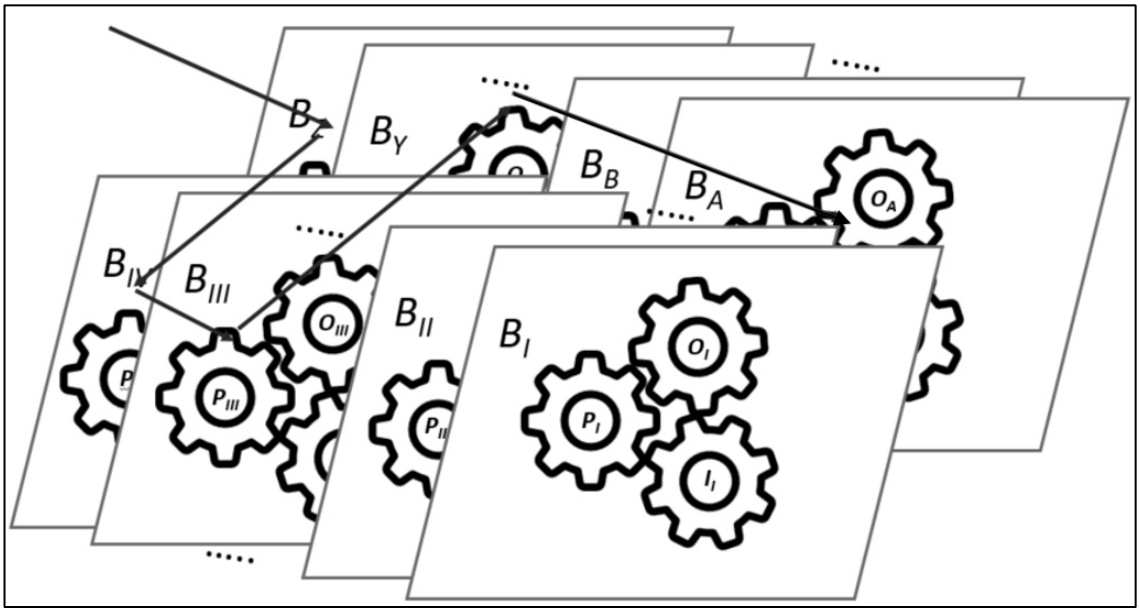


Figure 47: Path model in physical security.
Source: Own Figure.

Although there are differences in the type of attack paths in physical security and IT security, both domains share similarities in the description of attack paths.

3.3.2 Alignment of the Assessment of Impacts

In order to adapt the security assessments from physical security and IT security in a further step, a quantitative IT metric with an objective mechanism of performance to describe the protective effect of IT measures in terms of exploitability reduction must be dispensed with.

However, there are ways of making an adjustment: If the levels of risk contributions are chosen appropriately (compatible scales), the metrics described in Chapter 3.2.1 a metric can be merged with other metrics that also reflect real risks. The selection and adaptation of suitable levels of risk contributions in the physical security assessment and in the IT security assessment are explained below. The aim is to set up a multiplicative scoring-based metric for physical security and for IT security, which

a) provides quantitative values for the physical risk or IT risk.
b) comparable scales are used for the risk contributions.

In physical security, risk is viewed as a composite event. The individual contributions of the physical risk are classically linked multiplicatively, so that a physical risk is made up of the threat B, the vulnerability V and the impact I. Using the assumptions from Eq. (1) (see chapter 2.3), the following applies to the risk in this context (see Eq. (25)):

R = Vulnerability x Impact (25)

If the events V and I do not influence each other, the physical risk can be written as a multiplication of V and I (see Eq. (26)):

$$R = V \cdot I \tag{26}$$

In physical security, risks can also be described using scoring-based metrics. Numbers are assigned to the levels of the individual contributions on a rating scale. If V and I were scaled linearly, physical risk scores could be calculated which are proportional to the true physical risk (see Eq. (27)):

$$r = v \cdot i \tag{27}$$

If the relationships between the numerical values and risk contributions are non-linear, distortions may occur (see chapter 3.2.1): A physical risk assessment based on numerical values corresponds to different real physical risk values.

To combine the risk description from physical security ($R = V \cdot I$) and the risk description from IT security ($R = E \cdot I$), the impact scales from both security domains are first of all harmonized (see also the explanations in chapter 3.3.4). Experts can be used in this context to define impact levels with monetary loss values, in which both physical scenarios and IT scenarios can be found. A scale is defined for both security domains, e.g. with four levels (or scores "1" to "4"). They can be supplemented by descriptive attributes that describe the impact level (see chapter 3.3.4). The experts write a monetary loss value after each individual score (see as an example Table 37). Each level-impact pair can be interpreted as a point, e.g. $P1(1|10)$, $P2(2|100)$, etc. These points can be represented by a mathematical function. For the impact levels in Table 37 the following correlation can be assumed for the Impact I for both security ratings: $I = 10^i$ [Euro].

Score	IT Impact (Euro)		Physical Impact (Euro)	
1	10	10^1	10	10^1
2	100	10^2	100	10^2
3	1000	10^3	1000	10^3
4	10000	10^4	10000	10^4

Table 37: Impact levels and monetary loss values for both security assessments.
Source: Own table.

The risk function thus results in Eq. (28):

$$ln(r) = \cdots + \ ln\, 10 \cdot i \tag{28}$$

If, for example, score 1 is entered in the rightmost part of the equation, the result is $(ln\ 10 \cdot 1\ =)$ 2.3. A reverse transformation yields the following for the impact $(e^{2.3}\ =)$ 10 (Euro). The impact scales have been successfully merged. Scoring-based true impact classifications can be mapped. The question now arises of a suitable scoring-based mapping of the vulnerability contributions or the exploitability contributions in a multiplicative metric of the form "R = V · I" or "R = E · I". A metric is sought by means of which the impacts as well as the vulnerability and exploitability or their contributions can be scored.

3.3.3 Harmonization of the Assessment of Vulnerability

After harmonizing the impact scales for both security domains, the question of how vulnerability levels for V in the physical risk description $(R = V \cdot I)$ can be defined. In physical security, vulnerability is determined through the interplay of protection, observation and intervention. One metric that can be used to assess physical vulnerability is the scoring-based Harnser metric. Scores are not quantitative per se, which is why they cannot be calculated. Nonetheless, the idea of incorporating an objective mechanism of performance into the physical security assessment parameters to be scored means that presumed probability intervals, which are assumed to be behind the categories of the vulnerability scale, can be adapted to objective vulnerability levels. The analysis results in chapter 3.1 objectively demonstrate, using the example of physical security, that quantitative results can be mirrored using a scoring system despite different scale categories. It should be noted that quantitatively calculated results of one or more ICM variants can be found within assumed probability intervals, which are behind each scale category. As part of the investigations in this thesis, the following measures are proposed and validated, which reduce incompatibilities between the Harnser metric and the ICM:

1. Extension of the scale categories to include assumed probability intervals.
2. Adjustment of the assumed probability intervals (and scale categories, if applicable) to the course of the ICM vulnerability curve.

With the help of the Harnser metric proposed in this paper, it is possible to conduct inferential assessments whose results correspond to objective vulnerability classifications between 0 % (no vulnerability) and 100 % (maximum vulnerability). A reference model with one barrier and one asset is considered. The vulnerability results of ICM 1 are sorted according to the size of the Harnser vulnerability results and then arranged according to size within the Harnser plateaus. The Harnser plateaus of the thirteen-member scale in this case are then adjusted to the ICM 1 vulnerability values. At this point, the question arises as to how a Harnser scale could look like the impact scale from chapter 3.3.2 consists of four categories and quantitatively conforms to ICM 1. In addition, the question arises as to how Harnser scoring can be structured in such a way that log scores are used at the procedural level, as in the barrier-based CVSS approach. Arbitrary values are already added in the Harnser metric. Whether these values are the result of logarithmization or not has no decisive role with regard to the conformity of the Harnser vulnerability values to the objective vulnerability values of an ICM variant. In a first consideration, the log transformation can be applied directly to the Harnser scores from "1" to "5" (see Eq. (29)):

$$\text{log score} \\ = log_{MaxScore-MinScore}(\text{Hanser Score}) \tag{29}$$

However, this would result in the highest log value being assigned to the lowest Harnser score and the lowest log value being assigned to the highest score (see Table 38).

Harnser Score	log score, base = 4	Rounded log score
1	1.16	1
2	1	1
3	0.79	1
4	0.5	1
5	0	0

Table 38: Log-transformed Harnser scores.
Source: Own table.[54]

In the CVSS approach, as proposed in Braband (2019), a low log value means that the configuration has a major negative impact on exploitability, e.g. "Network; numerical value = 0.85; log score = "0"". Following the logic, this would mean that the Harnser score "5" represents the worst configuration when applied to physical security. However, according to the previous definition (score "1" := low; score "5" := high), this is not the case. Score "5" means a strong characteristic. The more pronounced a contribution to vulnerability, the generally more positive the effect on vulnerability reduction. In addition, there is another problem: if the log scores are rounded so that integer log scores are created, then the Harnser scores "2", "3", "4" and "5" can no longer be clearly distinguished from each other because they would be assigned the same logarithmic value (= "1"). However, the scores should be clearly distinguishable, so that an increase in a score means an increase in the security functionality.

From the point of view of a scoring user, the definition of the log values as shown in Table 38 can lead to confusion. Intuitively, it would be expected that a low Harnser score would be assigned to a low log value and a high Harnser score to a high log value. To meet this challenge, (arbitrary) numerical values between "0" and "1" are defined for each Harnser score, similar to the CVSS: The smallest Harnser score is assigned the largest numerical value. The largest Harnser score is assigned the smallest numerical value. The numerical values are defined "equidistantly". As shown in Table 39 low Harnser scores have low numerical values and high Harnser scores have high numerical values. This is necessary in order to obtain scores after logarithmization that are arranged in ascending order like the Harnser scores. Applying the logarithm to the numerical values of the Harnser scores with a base of 0.6, as conducted in Braband (2019), results in the assignments in Table 40.

P	O	I	Numerical Value
1	1	1	0.83
2	2	2	0.66
3	3	3	0.5
4	4	4	0.33
5	5	5	0.16

Table 39; Harnser score levels with corresponding numerical values.
Source: Own table based on Harnser (2010).[55]

[54] The order of the log scores is inverse to the Harnser scores. The rounding rule also applies here: If the first decimal place of the digit is a 0, 1, 2, 3 or 4, then it is rounded down. If the first decimal place of the digit is a 5, 6, 7, 8 or 9, then it is rounded up.

[55] P := Protection, O := Observation and I := Intervention. The conversion of descriptive levels into numerical values is similar to the principle of the Common Vulnerability Scoring System (CVSS) (First.org, 2022): Scores that are worse are assigned high numerical values, while scores that are better are assigned low numerical values. Although the assessment parameters in physical security are on a much more concrete level than the threat scenario-describing parameters in CVSS, they could be substituted here in the same way.

P/O/I Score	Numerical Value	log score, base = 0.6
1	0.83	0
2	0.66	1
3	0.5	2
4	0.33	3
5	0.16	5

Table 40: Formation of log scores from Harnser scores.
Source: Own table.

To summarize, in this Harnser scoring variant, the scores for protection (P), observation (O) and intervention (I) are logarithmized, each scored between "0" and "5" and added together. This results in a Likelihood of Vulnerability (LoV) score - analogous to the Likelihood of Exploitability (LoE) in the barrier-based CVSS approach. The LoV can be calculated using Eq. (30). As a result, a score range from "0" to "15" is possible.

$$\text{LoV} = log_{0.6}(P) + log_{0.6}(O) + log_{0.6}(I) \tag{30}$$

A four-item Harnser scale can be created by means of the 3.1 that all vulnerability values of an ICM variant lie within the vulnerability plateaus of the scoring. Table 41 shows an exemplary classification of such a four-tier Harnser scale. Figure 48 shows that all ICM 1 vulnerability values lie within the plateaus.

Category		High	Medium	Low	Very Low
Score Range		"0-5"	"6-8"	"9-11"	"12-15"
Estimated Probability	Lower Interval Limit (LIL)	0.98	0.64	0.2	0.024
	Upper Interval Limit (UIL)	1	0.99	0.8	0.257
	Mean of Interval (MI)	0.99	0.815	0.5035	0.1405

Table 41: Four-item Harnser log scale adapted to ICM 1
Source: Own table.

The probability intervals behind the four scale categories cover a wider range of ICM 1 values than is the case with the 13-point scale. Vulnerability values of ICM 1 can lie on the interval boundaries of a plateau or in between. If the scale category "Low" is present, for example, a high range of suspected vulnerability values is assumed. The difference between the highest and lowest probability values in this category is over 60 %. If, assuming a worst-case scenario, the Harnser scoring results in the "Low" category and the "upper limit" of the associated probability interval for vulnerability is selected, the true vulnerability value (of ICM 1) could be 20%. Consequently, the security margin in this case is high. In terms of cost-effectiveness, the use of a physical vulnerability rating scale with thirteen categories makes more sense than a rating scale with four categories.

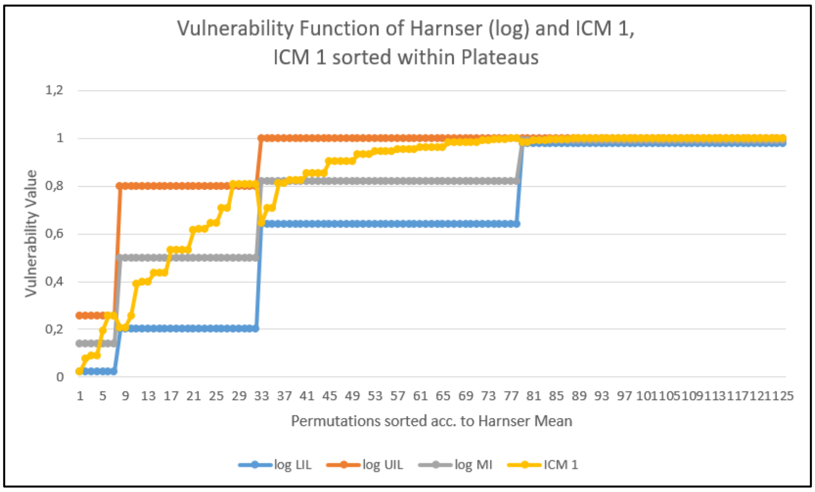


Figure 48: Plot of vulnerability values (Harnser log) and ICM 1
Source: Own Figure.

Each category of the four-point Harnser scale can be assigned a vulnerability score for the multiplicative scoring metric. Behind each of these levels are quantitative probability values for vulnerability (see Table 42 third and fourth columns).

Harnser V Scale	V Score (for multiplicative scoring metric)	Vulnerability LIL of Harnser Intervals	Vulnerability UIL of Harnser Intervals
Very Low	1	0.024	0.257
Low	2	0.2	0.8
Medium	3	0.64	0.99
High	4	0.98	1

Table 42: ICM 1 vulnerability values on a four-point scale.
Source: Own table.[56]

Based on the third and fourth columns in Table 42 the following correlations result (see Figure 49):

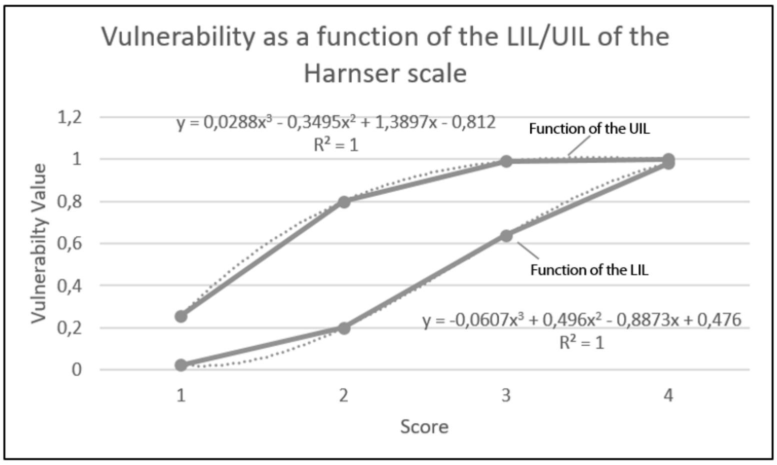


Figure 49: Vulnerability functions according to the interval limits of the four-part Harnser scale categories incl. regression function.
Source: Own Figure.

[56] UIL := Upper Interval Limit. LIL := Lower Interval Limit.

The vulnerability curves (LIL and UIL) can each be determined by a third-degree polynomial function (see Eq. (31)):

$$\begin{aligned} V_{LIL} &= -0.0607 v_{LIL}^3 + 0.4965 v_{LIL}^2 - 0.8873\, v_{UIL} + 0.476 \\ V_{UIL} &= 0.0338 v_{UIL}^3 - 0.3845 v_{UIL}^2 + 1.4597\, v_{UIL} - 0.852 \end{aligned} \tag{31}$$

For the assessment parameter Impact ($I = 10^i$) of the risk function (R = V · I), the base 10 is selected here, and for the vulnerability functions, Eq. (31) is chosen. The physical risk results in Eq. (32):

$$\begin{aligned} \ln(r_{LIL}) &= \ln 0.6 \cdot \log_{0.6}(-0.0607 v_{LIL}^3 + 0.4965 v_{LIL}^2 - 0.8873\, v_{UIL} + 0.476) + \ln 10 \cdot i \\ \ln(r_{UIL}) &= \ln 0.6 \cdot \log_{0.6}(0.0338 v_{UIL}^3 - 0.3845 v_{UIL}^2 + 1.4597\, v_{UIL} - 0.852) + \ln 10 \cdot i \end{aligned} \tag{32}$$

According to the approach outlined, physical vulnerability is determined using the following steps:

1. Experts score protection, observation and intervention.
2. The score sum is sorted into a category on a four-point Harnser scale, which is quantitatively consistent with an ICM variant.
3. Each scale category is assigned a vulnerability score (for the multiplicative scoring metric). For example, if the vulnerability is "High", the vulnerability score "4" is selected.
4. The vulnerability score is used as input for the vulnerability contribution in Eq. (32) as input for the vulnerability contribution.
5. Experts score the extent of damage (score "1" to "4").
6. The impact score is used as input for the impact contribution in Eq. (32) as input for the impact contribution.
7. The risk is calculated once for the cases LIL and UIL with Eq. (32) is calculated.

For the assessment of IT vulnerability, Eq. (8) can be used. The reference model consists of a barrier, a vulnerability and an asset. For the assessment of physical vulnerability, Eq. (32) is used for the risk assessment on the reference model of a barrier and an asset. This results in the following risk descriptions (see Eq. (33)):[57]

IT risk:

$$\begin{aligned} &\ln(r) \\ &= \ln 0.6 \cdot \log_{0.6}(0.202 \cdot \mathrm{av} + 0.05) + \ln 0.6 \cdot \log_{0.6}(0.255 \cdot \mathrm{ac} - 0.095) \\ &\quad + \ln 0.6 \cdot \log_{0.6}(0.256 \cdot \mathrm{pr} - 0.18) + \ln 0.6 \cdot \log_{0.6}(0.23 \cdot \mathrm{ui} - 0.07) + \ln 10 \cdot i \end{aligned} \tag{33}$$

Physical risk:

$$\begin{aligned} \ln(r_{LIL}) &= \ln 0.6 \cdot \log_{0.6}(-0.0607 v_{LIL}^3 + 0.4965 v_{LIL}^2 - 0.8873\, v_{UIL} + 0.476) + \ln 10 \cdot i \\ \ln(r_{UIL}) &= \ln 0.6 \cdot \log_{0.6}(0.0338 v_{UIL}^3 - 0.3845 v_{UIL}^2 + 1.4597\, v_{UIL} - 0.852) + \ln 10 \cdot i \end{aligned}$$

Assuming the barrier-based CVSS approach from chapter 3.2.2, a four-tier exploitability scale can be defined whose categories can be assigned to objective exploitability levels by back-transforming the log score sums from AV to UI (see for example Table 43).

[57] For IT security, the following is assumed: a barrier with a vulnerability and an asset. For physical security, the following is assumed: one barrier and one asset.

Likelihood	High	Medium	Low	Very Low
LoE score	0	1-3	4-5	6-9
Estimated Probability Interval (LIL)	1	0.216	0.078	0.01
Estimated Probability Interval (UIL)	1	0.6	0.13	0.047

Table 43: LoE scale with assumed probability intervals.
Source: Own table.[58]

If the allocations in Table 43 are adopted, four levels can also be defined for exploitability in the IT risk description (see ($R = E \cdot I$) (see Table 44)).

Exploitability Scale (CVSS)	E Score (for multiplicative scoring metric)	Exploitability LIL	Exploitability UIL
Very Low	1	0.01	0.047
Low	2	0.078	0.13
Medium	3	0.216	0.6
High	4	1	1

Table 44: "Quantitative" exploitability values on a four-point scale.
Source: Own table.[59]

For the exploitability, the third and fourth columns in Table 44 result in the following correlations (see Figure 50):

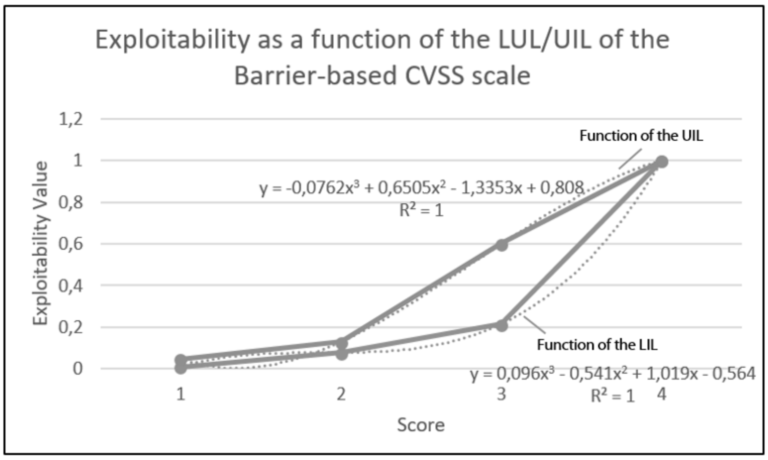


Figure 50: Exploitability functions according to the interval limits of the four-part CVSS scale categories incl. regression function.
Source: Own Figure.

The exploitability curves can each be determined by a third-degree polynomial function (see Eq. (34)):

$$E_{LIL} = 0.096e_{LIL}^3 - 0.541e_{LIL}^2 + 1.019e_{UIL} - 0.564 \qquad (34)$$
$$E_{UIL} = -0.0762e_{UIL}^3 + 0.6505e_{UIL}^2 - 1.3353e_{UIL} + 0.808$$

For the assessment parameter Impact ($I = 10^i$) of the risk function (R = E · I), the base 10 is selected here, and the base 0.6 for the exploitability functions. For the IT risk, the formulas in Eq. (35) result:

[58] The interval limits are determined as follows:
$e_{LIL} = e^{\ln(0.6) \cdot LoE\ Score\ min}$ resp. $e_{UIL} = e^{\ln(0.6) \cdot LoE\ Score\ max}$.

[59] UIL := Upper Interval Limit. LIL := Lower Interval Limit.

$$
\begin{aligned}
\ln(r_{LIL}) &= \ln 0.6 \cdot \log_{0.6}(0.096e_{LIL}^3 \; - \; 0.541e_{LIL}^2 \; + \; 1.019e_{UIL} - \; 0.564) + \; \ln 10 \cdot i \\
\ln(r_{UIL}) &= \ln 0.6 \cdot \log_{0.6}(-0.0762e_{UIL}^3 + \; 0.6505e_{UIL}^2 - \; 1.3353e_{UIL}) + \; \ln 10 \cdot i
\end{aligned}
\tag{35}
$$

According to the approach outlined, exploitability is determined using the following steps:

1. Experts score the CVSS assessment parameters AV, AC, PR and UI.
2. The score sum is calculated on a four-point scale (as shown in Table 43) and it is sorted into a category.
3. Each scale category is assigned an exploitability score (for the multiplicative scoring metric). If the exploitability is "Very Low", for example, the exploitability score "1" is selected.
4. The exploitability score is used as input for the exploitability contribution in Eq. (35).
5. Experts score the extent of damage (score "1" to "4").
6. The impact score is used as input for the impact contribution in Eq. (35).
7. The risk is calculated once for the cases LIL and UIL with Eq. (35).

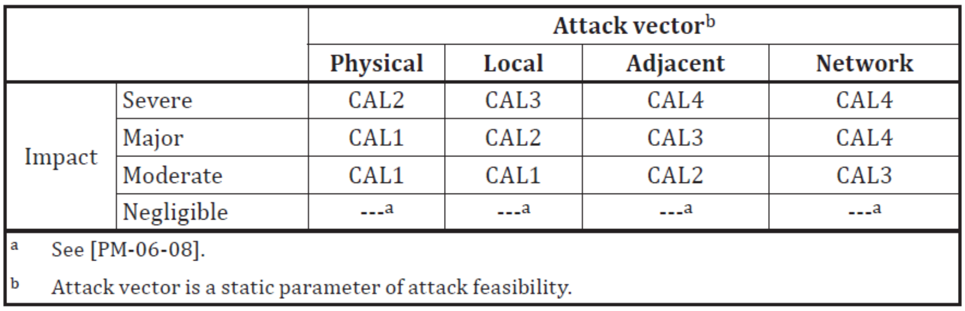
It is important to note the strict assumption that only the scores defined in the scales (here: score "1", "2", "3" and "4") are used in the mathematical functions of the risk contributions. Both the physical risk description and the IT risk description can be adapted to each other using the options presented (see Eq. (33) and Eq. (35)). When aligning both security metrics, it is generally possible to consider logarithmizing the risk contributions to the same base, e.g. to a base of ten. In chapter 3.2.2, it is shown in Eq. (11) and Eq. (12) that the base to which logarithmization is performed has no influence on the calculation of true risk values. However, it should be noted that the choice of base has an influence on the scaling of the data: very large values are reduced by the log transformation, and very small values are increased. Consequently, the choice of a particular base can influence the interpretation of the transformed data. Data transformed to a base of ten can be interpreted more easily than data transformed to a base of 0.6, for example, due to the underlying power of ten.

The application of the log-transformation approach can demonstrably help to reduce metrics-inherent distortions in scoring-based assessment systems. At the same time, the metrics from the physical security assessment and from the IT security assessment can be merged via a compatibility of the scales of the risk contributions. The following requirements must be met for a merger:

- The metrics from both security domains are used to assess the same thing, e.g. risk by linking threat (assumption = 100%), vulnerability and impact.
- True risk contributions must be known.
- The scales of the risk premiums are structured in the same way with regard to the level classification, insofar as possible, e.g. four levels per risk premium.
- Insofar as a multiplicative relationship is assumed (disjointness between the risk contributions and strict independence assumed): The base to which the risk contributions in both domains are logarithmized is chosen to be the same in each case. For example, this can be 10 for the impact and 0.6 for the vulnerability, as demonstrated in the examples in this paper. However, it is also generally possible to use the same basis for the log transformation of all risk contributions.
- The epistemic threat component is excluded from the risk assessment by assuming a case of attack (threat = 100 %).

3.3.4 Determination of Security Levels

In functional safety, qualitative risk analyses are used to determine the required Automotive Safety Integrity Level (ASIL) (Krisper, 2021) (see e.g. ISO 26262-3:2018, p. 19-26). In the context of IT security, qualitative risk analyses are also used to determine the Cybersecurity Assurance Level (CAL) (see e.g. ISO/SAE 21434, p. 59). In IT security, threat scenarios (described by the attack vector) and impact components are combined in a table to determine the CAL (see Table 45). The CAL from "1" to "4" is associated with development requirements (see Table 46). "---" means that it is not necessary to take further risk mitigation measures beyond the accepted quality system within the organization.[60] In the case of "---", ISO/SAE 21434 suggests developing the IT system or component according to the V-model (ISO/SAE, 2021b, p. 15).



		Attack vector[b]			
		Physical	Local	Adjacent	Network
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	---[a]	---[a]	---[a]	---[a]

[a] See [PM-06-08].

[b] Attack vector is a static parameter of attack feasibility.

Table 45: Determination of the CAL according to ISO/SAE 21434.
Source: ISO/SAE (2021b, p. 59).

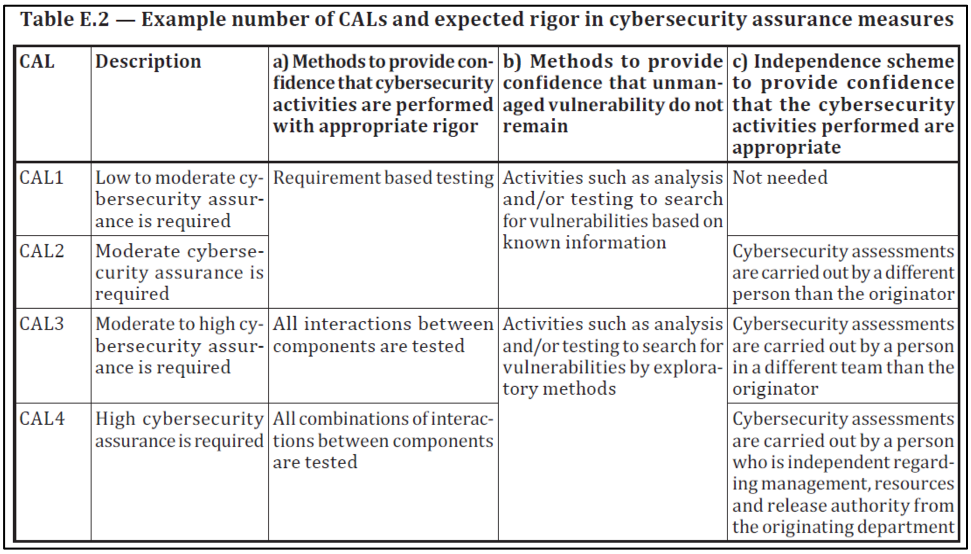


Table E.2 — Example number of CALs and expected rigor in cybersecurity assurance measures

CAL	Description	a) Methods to provide confidence that cybersecurity activities are performed with appropriate rigor	b) Methods to provide confidence that unmanaged vulnerability do not remain	c) Independence scheme to provide confidence that the cybersecurity activities performed are appropriate
CAL1	Low to moderate cybersecurity assurance is required	Requirement based testing	Activities such as analysis and/or testing to search for vulnerabilities based on known information	Not needed
CAL2	Moderate cybersecurity assurance is required			Cybersecurity assessments are carried out by a different person than the originator
CAL3	Moderate to high cybersecurity assurance is required	All interactions between components are tested	Activities such as analysis and/or testing to search for vulnerabilities by exploratory methods	Cybersecurity assessments are carried out by a person in a different team than the originator
CAL4	High cybersecurity assurance is required	All combinations of interactions between components are tested		Cybersecurity assessments are carried out by a person who is independent regarding management, resources and release authority from the originating department

Table 46: Cybersecurity measures corresponding to the CAL according to ISO/SAE 21434.
Source: ISO/SAE (2021b, p. 60).

The CAL from ISO/SAE 21434 is comparable to the theoretical security profile according to Schwerdtfeger, which sets requirements for the auditor in the form of guiding questions to be answered (2018, pp. 53-54), or to the Assessment Assurance Levels (EAL) "1" to "7" according to the Common Criteria (CC, 2021). A high EAL means that the claimed security guarantee of the system under consideration is checked more comprehensively than with a lower EAL. The same principle underlies the CAL, which results from an impact/attack vector pair. The Attack Vector is part of the Attack Feasibility Rating according to ISO/SAE 21434 (ISO/SAE, 2021b,

[60] After the risk assessment, risk treatment decisions (accept, remove, sharing, reduction) can be made. The "Reduction" option aims to reduce the CAL.

pp. 76-77) and consists of the "Physical", "Local", "Adjacent" and "Network" characteristics according to CVSS (ISO/SAE, 2021b, p. 59). The CAL categorization can be transferred to physical security as an initial idea.[61] However, a transfer would lead to restrictions in the PAL categorization because "Local", "Adjacent" and "Network" are IT threat vectors that are not considered in the physical domain. All combinations that contain these three attack vector attributes are not defined in physical security. Only the "Physical" column is occupied here (see italicized marking in Table 47). If the scheme for linking attack vector and impact from ISO/SAE 21434 is followed, then only PAL "1" and PAL "2" are defined. PAL "3" and PAL "4" remain undefined.

Impact	Attack Vector			
	Physical	Local	Adjacent	Network
Severe	***CAL 2 = PAL 2***	CAL 3 = PAL 3	CAL 4 = PAL 4	CAL 4 = PAL 4
Major	***CAL 1 = PAL 1***	CAL 2 = PAL 2	CAL 3 = PAL 3	CAL 4 = PAL 4
Moderate	***CAL 1 = PAL 1***	CAL 1 = PAL 1	CAL 2 = PAL 2	CAL 3 = PAL 3
Negligible	**---**	---	---	---

Table 47: Restrictions on mapping from CAL to PAL.
Source: Own table based on ISO/SAE (2021b, p. 59).[62]

The mapping from CAL to PAL could be modified as follows to obtain PAL "1" to PAL "4": The attack vector/impact pair "Physical-Severe" is assigned the highest PAL. The attack vector/impact pair "Physical-Negligible", on the other hand, is assigned the lowest PAL (see Table 48). In this case, it can be seen that CAL "1" is assigned to two different PALs ("2" and "3") (see grey marking in the Table 48). However, the security levels should be clearly distinguishable in pairs. This means that a CAL (e.g.: "1") also only corresponds to one PAL, e.g. only "1" and not "1" and "2".

Impact	Attack Vector
	Physical
Severe	CAL 2 = PAL 4
Major	*CAL 1 = PAL 3*
Moderate	*CAL 1 = PAL 2*
Negligible	--- = PAL 1

Table 48: Modification of the mapping from CAL to PAL.
Source: Own table based on ISO/SAE (2021b, p. 59).[63]

In this context, it is also necessary to define what specifically lies behind the impact categories. From a physical perspective, worst-case scenarios are assessed. In the context of MAS, this could be the successful theft of a vehicle. According to this assumption, every physical attack would be classified as "Severe" or PAL "4". However, from the perspective of a system operator that owns several fleets and operates them via a mobile access service, the purely financial loss of a vehicle would be lower than the loss of an entire fleet (reputational damage excluded). IT attacks can therefore scale differently to physical attacks.[64] If an operator now de-

[61] PAL is not defined in ISO/SAE 21434.

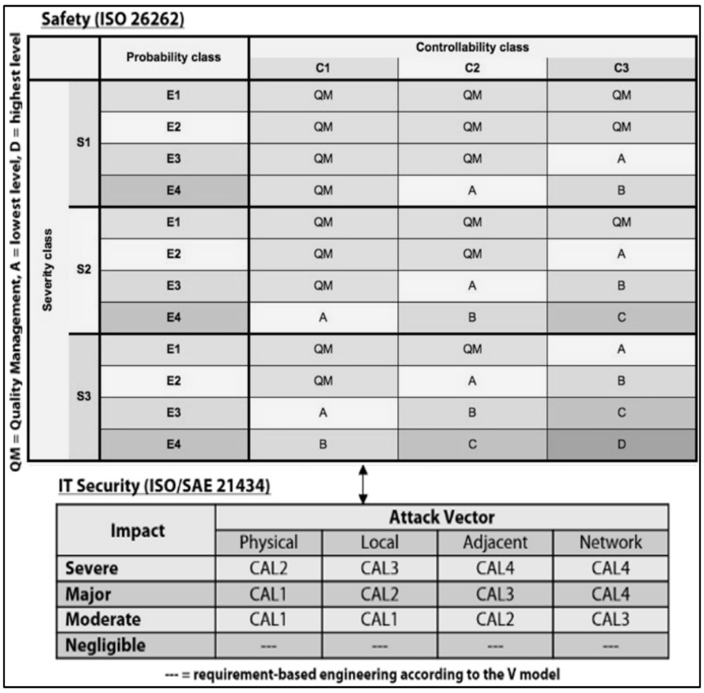
[62] The light gray marking indicates that these columns cannot be used to derive the physical security level. The green marking indicates the permissible assignments for physical security.

[63] The fact that a CAL ("1)" is assigned to two different PALs ("2" and "3") is highlighted in gray italics.

[64] Local, physical attacks can also have similar effects. For example, if supply nodes in energy supply systems are affected, the impact does not remain local (Lichte et al., 2020b). Another example can be drone attacks. They can be conducted from any distance, but an attacker still has to physically reach the facility (Schneider et al., 2021).

fines that the impact categories are to be understood as "Severe = all fleet customers or vehicles affected, Major = all fleets or vehicles of a customer affected, Moderate = fleet vehicles of a customer's fleet affected, Negligible = one vehicle affected", then each successful physical attack would be defined as PAL "1" according to the above table.

It is assumed that physical attacks only have a local impact, i.e. only one vehicle can be stolen. A physical theft is not facilitated by a previous theft. For product development, this could generally correspond to minimum development requirements. This in turn would lead to a minimal design of the physical representative of the mobile access product and thus potentially to an increase in attractiveness for an attacker. This would not be a bad thing if the impact is actually low. However, if, for example, a master key can be stolen and the expected impact is greater, then a possible scenario could lead to interactions between IT security and physical security. The requirements for the design of physical barriers must then be carefully considered. The previous explanations suggest the importance of establishing a uniform impact scale for both domains. When determining an ASIL in accordance with ISO 26262, the variables "severity", "probability class" ("frequency") and "controllability" are linked together in a matrix - unlike in ISO/SAE 21434 (see Figure 51).



Safety (ISO 26262)

QM = Quality Management, A = lowest level, D = highest level

Severity class	Probability class	Controllability class C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

IT Security (ISO/SAE 21434)

Impact	Attack Vector			
	Physical	Local	Adjacent	Network
Severe	CAL2	CAL3	CAL4	CAL4
Major	CAL1	CAL2	CAL3	CAL4
Moderate	CAL1	CAL1	CAL2	CAL3
Negligible	---	---	---	---

--- = requirement-based engineering according to the V model

Figure 51: Comparison of ASIL and CAL.
Source: Embitel.com (2018) (top); ISO/SAE (2021b, p. 59) (bottom).

In security, the "frequency" assessment parameter could be described by the threat percentage. However, this is difficult to estimate, even with the help of experts, because it is epistemic. In this context, Witte et al. (2020), for example, are working on models to describe scenario probabilities. The basic idea behind the considerations in Witte et al. (2020) is that an absolute frequency statement cannot be depicted due to a lack of evidence. However, a networked representation would make it possible to check threat scenarios for logical consistency: Using a combination of attacker characteristics (e.g. skills, tools, publicly available information), experts can make a statement as to whether certain scenarios are more plausible than others. If the Frequency column of the ASIL matrix is now replaced by the Attack Feasibility (vulnerability) and the Severity column by the Impact, CAL can be determined according to the same scheme as ASIL: The impact is linked to the vulnerability and controllability in a table (see Table 49).

Impact	Attack Feasibility	Controllability		
		Simple	Normal	Difficult
Negligible	Very Low	QM	QM	QM
	Low	QM	QM	QM
	Medium	QM	QM	QM
	High	QM	QM	QM
Moderate	Very Low	QM	QM	QM
	Low	QM	QM	QM
	Medium	QM	QM	CAL 1
	High	QM	CAL 1	CAL 2
Major	Very Low	QM	QM	QM
	Low	QM	QM	CAL 1
	Medium	QM	CAL 1	CAL 2
	High	CAL 1	CAL 2	CAL 3
Severe	Very Low	QM	QM	CAL 1
	Low	QM	CAL 1	CAL 2
	Medium	CAL 1	CAL 2	CAL 3
	High	CAL 2	CAL 3	CAL 4

Table 49: Consideration of the recategorization of CAL according to ISO 26262
Source: Own table based on Embitel.com (2018)[65]

In IT security, "controllability" describes, for example, the extent to which an operator is able to reduce damage by reacting appropriately once an asset has been reached if the affected system is compromised. This could include, for example, the possibility of deactivating the mobile access service remotely or activating a fallback plan. In contrast to the IT security assessment, the physical security assessment (e.g. according to Lichte et al. (2016)) only considers the period from the start of an attack until the asset is reached, not beyond. From a purely physical perspective, reactive measures are difficult to implement after asset recovery, as it is expected that the vehicle will be stolen. Now it could be argued that reactive measures could be initiated for all products still in the field, such as recalls or the physical retrofitting of mobile access products in the field. A controllability scale could look as follows for physical security and IT security (see Table 50):

Controllability	Description
Difficult	Further impact can only be inadequately prevented by postventive measures.
Normal	There are options for limiting further impact through postventive measures.
Simple	Further damage can be limited as far as possible by postventive measures.

Table 50: Controllability Category Description.
Source: Own table.[66]

Unlike the CAL, however, the ASIL refers to requirements for a very specific safety function of a component: Depending on the ASIL, the component must be equipped with suitable measures in such a way that a certain failure rate of this component is not exceeded. In physical security, for example, the security assessment takes place at system level. This is because vulnerability depends on the interaction between the vulnerability components of protection, observation and intervention. A system is therefore vulnerable if the interaction of protection,

[65] The security classifications "Quality Managed" (QM, ISO 26262) and "---" (ISO/SAE 21434) are comparable. QM means that the development process should follow a standardized and repeatable methodology for the development of the product (ISO 26262). An example of this could be Automotive SPICE. According to Automotive SPICE, the product must be developed according to the V-model. ISO/SAE 21434 suggests developing the product according to the V-model for the classification "---" (SAE, 2022, p. 15). Accordingly, "QM" and "---" can be used synonymously.

[66] Postventive refers to the time after a successful attack.

observation and intervention along a path under consideration is insufficient. If one component fails, e.g. the protection at barrier one (of a total of three barriers), this is not a sufficient condition for the overall system to be 100% vulnerable. ASIL is developed according to a specific failure rate. In the proposed CAL matrix, however, the attack feasibility (vulnerability), according to which development would have to be conducted for a specific CAL, is part of the CAL matrix.

In physical security, on the other hand, a certain PAL would have to be developed according to a vulnerability level. Consequently, a CAL must not depend on attack feasibility and a PAL must not depend on vulnerability. One solution could be to remove vulnerability from the CAL or PAL matrix as a first step and define a security level that results from the combination of impact and controllability. In a second step, a vulnerability level can be written behind each impact/controllability pair, according to which the system under consideration is to be developed. When using a four-point scale for vulnerability ("Very Low" - "Low" - "Medium" - "High"), the combination of impact and controllability can look as follows (see Table 51):

Assigned PAL/CAL to Impact-Controllability Pair				Assigned Vulnerability Category to Impact-Controllability Pair			
Impact	**Controllability**			**Impact**	**Controllability**		
	Simple	**Normal**	**Difficult**		**Simple**	**Normal**	**Difficult**
Negligible	---	---	PAL/CAL 1	**Negligible**	---	---	High
Moderate	---	PAL/CAL 1	PAL/CAL 2	**Moderate**	---	High	Medium
Major	PAL/CAL 1	PAL/CAL 2	PAL/CAL 3	**Major**	High	Medium	Low
Severe	PAL/CAL 2	PAL/CAL 3	PAL/CAL 4	**Severe**	Medium	Low	Very Low

Table 51: Approach to deriving CAL and PAL.
Source: Own table.

The correlations in Table 51 must be checked for plausibility in a third step. The entry "---" means that no further risk mitigation measures are required and that it is recommended to develop according to the V-model. Insofar as the impact scale is set up as "Severe = all fleet customers or vehicles affected, Major = all fleets or vehicles of a customer affected, Moderate = fleet vehicles of a customer's fleet affected, Negligible = one vehicle affected", there is a problem from a physical security perspective: if it is assumed that physical attacks scale less than IT attacks and consequently only one vehicle can be stolen with a vehicle break-in, then only one vehicle can be stolen according to Table 51. Table 51 only the impact controllability classifications "Negligible-Simple" ("---"), "Negligible-Normal" ("---") and "Negligible-Difficult" (PAL "1") can apply. According to this classification, minimum vulnerability requirements would apply in all three cases in terms of physical security.

The maximum physical impact is a stolen vehicle. It was previously defined as the lowest impact level. From an IT security perspective, however, the physical impact of "one vehicle theft" is low in relation to the impact of "entire vehicle fleets can be stolen". To solve the problem, the impact scale can be reconsidered and redefined. ISO/SAE 21434 distinguishes between four impact types: Financial, Privacy, Operational and Safety (ISO/SAE, 2021b, pp. 63-64). Each impact rating has four levels: "Severe", "Major", "Moderate" and "Negligible" (see for example Table 52).

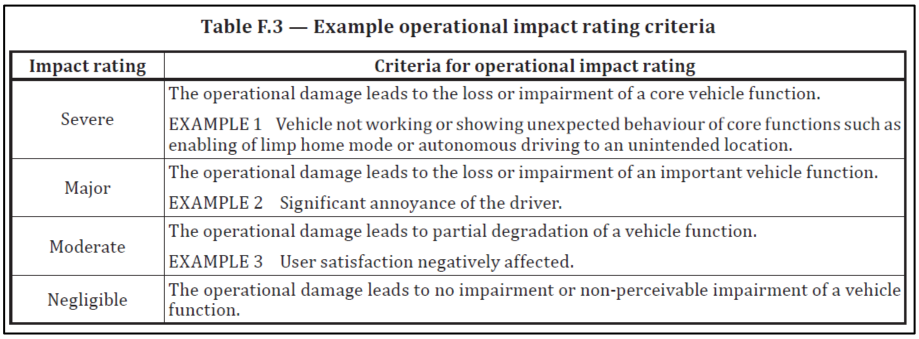


Table F.3 — Example operational impact rating criteria

Impact rating	Criteria for operational impact rating
Severe	The operational damage leads to the loss or impairment of a core vehicle function. EXAMPLE 1 Vehicle not working or showing unexpected behaviour of core functions such as enabling of limp home mode or autonomous driving to an unintended location.
Major	The operational damage leads to the loss or impairment of an important vehicle function. EXAMPLE 2 Significant annoyance of the driver.
Moderate	The operational damage leads to partial degradation of a vehicle function. EXAMPLE 3 User satisfaction negatively affected.
Negligible	The operational damage leads to no impairment or non-perceivable impairment of a vehicle function.

Table 52: Operational impact rating according to ISO/SAE 21434
Source: ISO/SAE (2021b, p. 64).

The criteria used in ISO/SAE 21434 are similar to those used by Harnser (2010, B3 p. 42) for physical security. In contrast to the impact types Financial, Privacy, Operational and Safety in ISO/SAE 21434, Harnser uses the classifications "Loss of Life/Health", "Loss of Production" and "Loss of Containment". "Loss of Life/Health" corresponds roughly to the "Safety" impact type. "Loss of Production" (impact scale according to Harnser (2010)) corresponds to the "Operational" impact type. "Loss of Containment", on the other hand, consists of "Safety", "Operational" and "Controllability". This deals with secondary consequences after a successful attack, e.g. due to the release of toxic gases, etc. Instead of a rating using descriptive levels, Harnser uses numerical values between "10" (no significant consequences) and "100" (major monetary or health damage). Harnser's dimensioning is obviously different from the impact rating according to ISO/SAE 21434. Harnser considers entire critical infrastructures (KRITIS). ISO/SAE 21434 is concerned with a vehicle. With MAS, however, it is not only the impact on a vehicle that must be taken into account, but also on entire vehicle fleets. The criteria from Table 52 a new impact rating can look as follows, taking into account the fleet perspective (see Table 53):

Impact Rating	Criteria
Severe	The functional damage leads to the loss of several vehicles or to a blackout of the MAS service. Example: Compromised cloud, theft of several vehicles.
Major	The functional damage leads to the loss of the vehicle or the MAS service for a vehicle. Example: Theft of the vehicle, user cannot get the vehicle locked or unlocked.
Moderate	The functional damage leads to partial impairment of the MAS service. Example: User satisfaction is impaired.
Negligible	The functional damage leads to no or imperceptible impairment of the MAS service.

Table 53: Operational impact rating and criteria for MAS.
Source: Own table based on ISO/SAE (2021b, pp. 63-64).[67]

The goal of a potential attacker is defined as the achievement of functional damage through a physical attack or an IT attack. According to the impact criteria, all impact categories include degrees of compromise by physical or IT means. In addition, the categories can also be assigned monetary loss values by experts (see chapter 3.3.1). The "Major" and "Severe" categories include the loss of physical assets. The procedure of bringing the impact contributions to a comparable scale so that the impact scales in physical security and IT security represent a common range is also referred to as "min-max normalization" (Al Shalabi & Shaaban, 2006). With this definition, the derivation of CAL and PAL according to the matrix from Table 51 can be conducted. Furthermore, in the course of the risk assessment of CPS, scenarios with cross-domain interaction should also be able to be assigned a security level for both domains. Experts must assess the extent to which, for example, an IT scenario can have a cross-domain impact on a physical scenario. The first step is to clarify how experts can assess the IT Impact on Physical Vulnerability (ITIPV). It is assumed that an interaction is accompanied by a change

[67] A scale that is structured in the same way for two domains can facilitate the interpretation and comparability of levels (Newsome, 2013, pp. 102, 104).

in the functionality of security measures. This means that an IT scenario can be used to reduce the three variables of protection, observation and intervention. The reduction of protection, observation and intervention results in a deterioration of the protective effect. The deterioration of the protective effect due to an interaction means an increase in vulnerability. Experts can estimate the impairment of the security functions.

One option may be to conduct a total of two scorings. In a first step, protection, observation and intervention are scored assuming a barrier and a quantitatively compliant, four-tier Harnser scale (e.g. for ICM 1) for the case that only one physical scenario materializes. The score sum is then sorted on the four-point vulnerability scale. The result is a vulnerability category that corresponds to an assumed probability interval for vulnerability. In a second step, the vulnerability is determined as in the first run, but it is assumed that an IT-side compromise was successful before the physical scenario. The physical vulnerability is therefore determined taking into account an interaction. The result is either a vulnerability classification that is at the same level as in the first run or at a higher, i.e. worse, level. The relative change in the vulnerability level due to an interaction can be used as a measure of the severity of a compromise, the ITIPV. A rating scale with four categories provides the following options for classifying the ITIPV (see Table 54).

If at least one of the three assessment variables is completely canceled out at a barrier, then it can be defined that the ITIPV is set as "High". This definition is based on the fact that vulnerability is maximized if at least one of the three assessment variables fails at a barrier. If there is an interaction, it is necessary to ask what requirements should be placed on the development. It is not expedient to increase the physical security level in the case of an ITIPV. Adding further barriers, for example, does not reduce the IT impact on the affected physical assessment parameters. In contrast, it is more promising to harden the system against the realization of the IT scenario that has an impact on physical security mechanisms. Let's assume that PAL "2" is used to determine a fictitious physical scenario (without taking an interaction into account). If experts estimate that there is an interaction, the IT scenario, which has an ITIPV, can also be attributed an IT security level that is considered at least equivalent to PAL 2. In this example, this is a CAL "2" or higher.

Vulnerability Category (Physical Scenario)	**Vulnerability Category (Physical Scenario with previous IT Scenario)**	**ITIPV**
Very Low	Very Low	Very Low
Very Low	Low	Low
Very Low	Medium	Medium
Very Low	High	High
Low	Low	Very Low
Low	Medium	Low
Low	High	Medium
Medium	Medium	Very Low
Medium	High	Low
High	High	Very Low

Table 54: Determination of the ITIPV.
Source: Own table.[68]

From the operator's point of view, there is a fundamental problem in having only scarce resources available (Sowa, 2011, p. 8). It should be possible to justify the classification of a CAL

[68] The Harnser scoring in this case is quantitatively consistent with the ICM 1 variant.

to the company management. Placing all CAL on the fourth level in a scenario with cross-domain impact is uneconomical. The introduction of a rule can help to attribute the IT scenario with an impact on physical vulnerability with an appropriate CAL. Here is an example: PAL 4 is to be developed against the lowest vulnerability category, "Very Low". If the vulnerability is in this category, a CAL can be assigned according to Table 54 an ITIPV can potentially assume the compromise levels "Very Low", "Low", "Medium" and "High". If at least one of the three assessment parameters is completely neutralized, the ITIPV category is set to "High" in accordance with the above definition. Because PAL "4" is defined as the highest security level, CAL "4", for example, is also selected for all potential levels of compromise for all ITIPV categories that may occur.

PAL "2" is to be developed according to the "Medium" vulnerability level. According to Table 54 there can be the potential compromise levels "Very Low" and "Low". A compromise level of "Medium" is undefined. Furthermore, it is assumed that the ITIPV applies to "High" if at least one mechanism of performance is completely undermined. Consequently, the question arises as to which CAL should be set, taking into account the ITIPV classification. The minimum CAL for the IT scenario is CAL "2", as PAL "2" is assumed for the physical scenario. It can then be generally agreed, for example, that an ITIPV of "Very Low" is developed to CAL "2", an ITIPV of "Low" to CAL "3" and an ITIPV of "High" to CAL "4". The same principle can be used to assign CAL for PAL "1" and PAL "3" (see Table 55).

PAL 1, assigned Vulnerability = High		**PAL 2, assigned Vulnerability = Medium**		**PAL 3, assigned Vulnerability = Low**		**PAL 4, assigned Vulnerability = Very Low**	
ITIPV	**CAL**	**ITIPV**	**CAL**	**ITIPV**	**CAL**	**ITIPV**	**CAL**
Very Low	1	Very Low	2	Very Low	3	Very Low	4
Low	x	Low	3	Low	3	Low	4
Medium	x	Medium	x	Medium	4	Medium	4
High	x	High	x	High	x	High	4

Table 55: Proposal for determining CAL in the event of an interaction.
Source: Own table. [69]

Table 55 can be used to deduce security levels in physical security and IT security depending on the degree of interaction. This generally applies regardless of the direction of impact, i.e. instead of PAL "1" to "4" in the first column of Table 55, there could also be CAL "1" to "4". In this case, the PAL would then be determined depending on the severity of an interaction. However, as there is no way to quantitatively prove vulnerability in IT security using a metric with an objective impact mechanism that could be used to assess the effectiveness of measures to reduce vulnerability, the Physical Impact on IT Vulnerability (PIITV) should not be considered.

[69] "x" stands for undefined.

4 Structure of the Risk Analysis

This chapter develops a procedure for cross-domain threat analysis and risk assessment of MAS. As an example, a reference model consisting of a barrier and an asset is used for the physical security assessment. For IT security, a reference model with a barrier with a vulnerability and an asset is considered. The cross-domain threat analysis and risk assessment is developed under the assumption that it is not possible to adjust the IT exploitability levels, which are determined based on scoring via the CVSS, to objective exploitability levels. This assumption is based on the lack of an effectiveness-based, quantitative metric for IT exploitability. The assumptions from Eq. (1) (see chapter 2.3) are assumed in this chapter.

4.1 Assessment (Profiling) of Assets

A first essential step in the risk assessment of the system under consideration is the examination of physical and IT security-relevant structures. For this purpose, Harnser (2010, B1, pp. 4-13) proposes profiling the system under consideration. Profiling describes the transparent and structured processing of intrinsic properties and functions of a system and its technological artifacts. The results of the analysis provide an overview of the elements and functions to be protected, so-called assets. They also provide an indication of

1. how the individual physical components and IT components relate to each other.
2. the various ways in which the objective can be achieved, e.g. in the case of MAS the undesired triggering of a trigger event.
3. the possible effects of an attack.

For the definition and classification of assets, Lyu et al. (2020) demonstrate the listing of all assets in the form of a table. The asset table is structured in Lyu et al. (2020) according to the following criteria: Asset type, designation, and location of the asset (e.g. physical and IT). A similar approach is followed in Harnser (2010, B1, pp. 4-13) using the so-called what-if technique. This technique can help to find assets (Termin et al., 2020). Scenarios are set up to identify system-relevant elements: "What happens if unit x no longer fulfills its function or is removed?". Lyu et al. (2020) and Harnser (2010) propose almost identical steps for identifying assets:

- **Step 1:** Collection and analysis of design documents and conducting expert interviews.
- **Step 2:** Classification of the assets of the system under consideration, e.g. according to Lyu et al. (2020) by material/immaterial, data, software, hardware, etc. or according to Harnser (2010, B1, p. 6) by name, role, key dependency on other units, level of service provision of the unit in the overall context, etc.
- **Step 3:** Summary and creation of a list of assets, whereby these can be assessed in terms of their value, e.g. according to Harnser (2010, A4, p. 42; B1, p. 4) via criticality scoring.

To support the identification of assets, Termin et al. (2020) suggest classifying the system to be analyzed in a morphological box (for MAS). The asset analysis in Harnser (2010, B1, p. 4) is function-based. This analysis also includes processes, sub-processes and the assessment of the criticality of sub-components. In Harnser (2010, B1, p. 4), assets are scored in terms of their criticality between "1" (low) and "5" (high). Assets with scores of less than or equal to "2" are not considered further in the analysis. The (sub) processes associated with an asset are then considered, the results are filtered again according to the most critical processes[70] , and so on. According to Harnser (2010, B1, p. 4), the aim is for risk analysts to focus on the most important assets and exclude the less important ones. This is due to the fact that only scarce resources

[70] This refers to the most important operational activities.

(time and money) are available (Sowa, 2011, p. 8). In addition, Harnser (2010) considers a critical infrastructure consisting of several sub-systems. The scope of possible assets is generally larger when considering entire infrastructures than when considering a vehicle or a system that is installed in the vehicle, for example.

Asset profiling is fundamentally use case-specific (Harnser, 2010, B1, p. 4), i.e. an asset register - the overview of all considered and prioritized assets - of a product in use case A can have different assets and criticality ratings than an asset register in use case B. According to ISO/SAE 21434, an answer to a question that is asked in the course of applying the what-if technique corresponds to one or more damage scenarios. A damage scenario is associated with a potential breach of confidentiality (Confidentiality, C), availability (Availability, A) and integrity (Integrity, I) (ISO/SAE, 2021b, pp. 73-74) (see as an example Table 56). The approach to assessing assets, as proposed in ISO/SAE 21434, can be applied to both physical and IT security. This is used to develop an approach for cross-domain threat analysis and risk assessment.

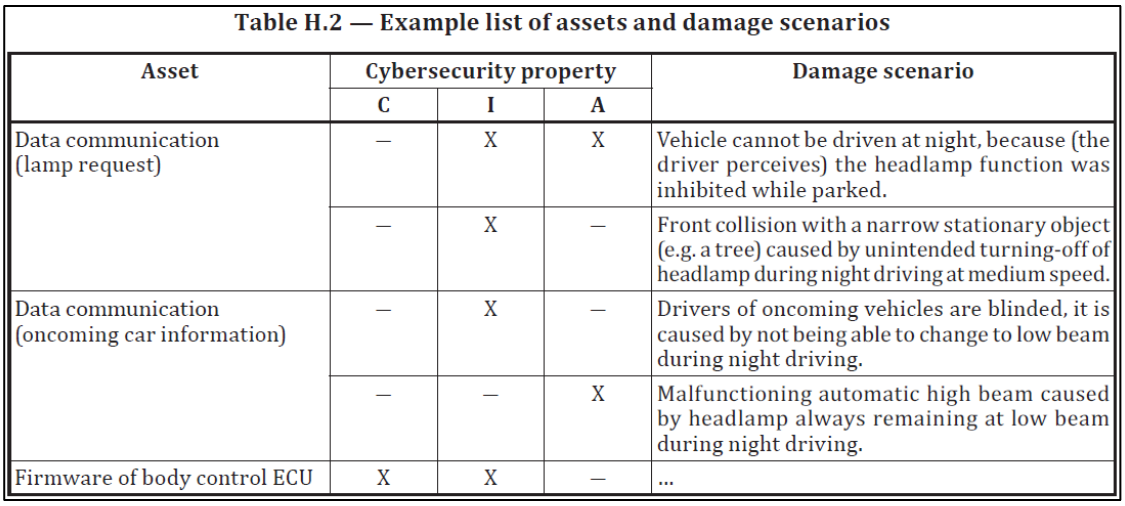


Table H.2 — Example list of assets and damage scenarios

Asset	Cybersecurity property			Damage scenario
	C	I	A	
Data communication (lamp request)	–	X	X	Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.
	–	X	–	Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.
Data communication (oncoming car information)	–	X	–	Drivers of oncoming vehicles are blinded, it is caused by not being able to change to low beam during night driving.
	–	–	X	Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.
Firmware of body control ECU	X	X	–	...

Table 56: Example asset analysis according to ISO/SAE 21434
Source: Source: ISO/SAE (2021b, p. 74).

4.2 Assessment (Profiling) of Threats

According to PRISM according to Harnser (2010) and TARA according to ISO/SAE 21434, asset profiling is followed by threat profiling (Harnser, 2010, B2, p. 15; ISO/SAE, 2021b, p. 74). In this step, threat scenarios are assigned to the assets or damage scenarios (see as an example Table 57).

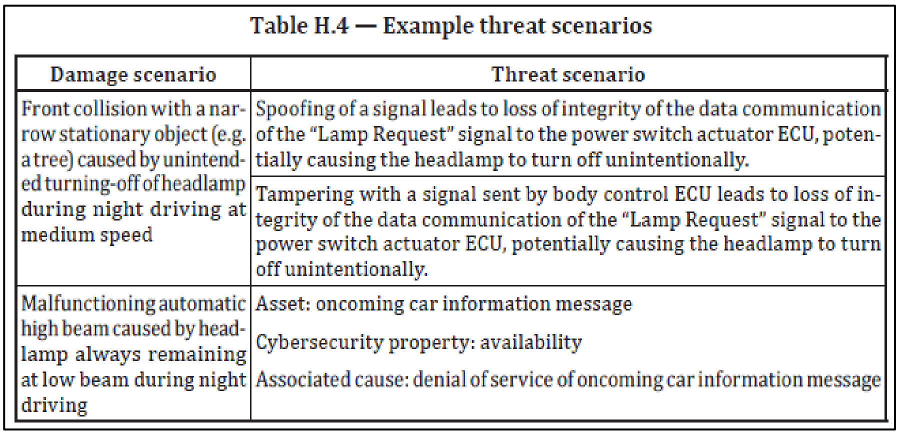


Table H.4 — Example threat scenarios

Damage scenario	Threat scenario
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed	Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
	Tampering with a signal sent by body control ECU leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving	Asset: oncoming car information message Cybersecurity property: availability Associated cause: denial of service of oncoming car information message

Table 57: Exemplary damage scenario - threat scenario mapping according to ISO/SAE 21434. Source: ISO/SAE (2021b, p. 74).

Termin et al. (2020) suggest developing use case diagrams and using misuse case diagrams to identify and localize attack vectors. In addition, possible attack paths must be investigated to determine how an asset can be successfully compromised. In Termin et al. (2020), the implementation of an attack tree analysis (ATA) or attack graph analysis (AGA) is proposed using the example of MAS. The results from the ATA or AGA provide possible physical attack paths and IT attack paths. ISO/SAE 21434 also suggests conducting such an attack path analysis (APA) (ISO/SAE, 2021b, pp. 75-76). Attack paths are assigned to a threat scenario in tabular form in accordance with ISO/SAE 21434 (see for example Table 58). The APA can be applied both in the IT domain and in the physical domain.

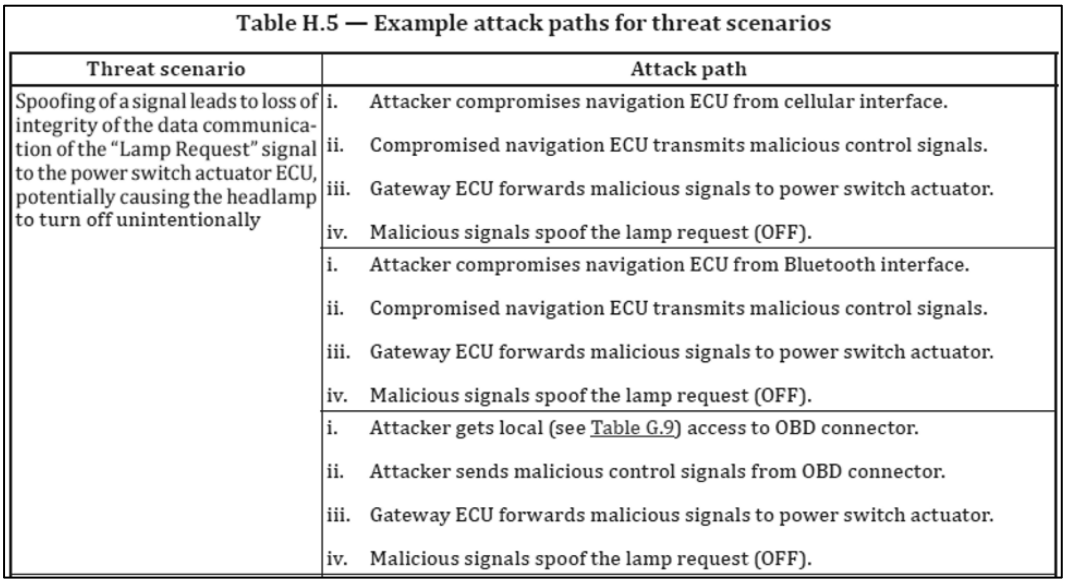


Table H.5 — Example attack paths for threat scenarios

Threat scenario	Attack path
Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker compromises navigation ECU from Bluetooth interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker gets local (see Table G.9) access to OBD connector. ii. Attacker sends malicious control signals from OBD connector. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).

Table 58: Example attack path analysis according to ISO/SAE 21434. Source: ISO/SAE (2021b, p. 75).

4.3 Assessment (Profiling) of Attack Paths

Once threat scenarios have been assigned to damage scenarios and an APA has been conducted, it is necessary to assess the attack paths. The assessment parameter is vulnerability. A distinction is made between vulnerability for the physical security assessment and exploitability or attack feasibility for the IT security assessment. The severity of an interaction is described by the IT Impact on Physical Vulnerability (ITIPV). The vulnerability assessment is based on expert assessments. The considerations from chapters 3.3.1 the attack feasibility can be assessed using the Attack Vector (AV), Attack Complexity (AC) and Privileges Required (PR*) assessment variables. According to CVSS (First.org, 2022), the levels of each assessment parameter have an assigned numerical value between zero and one. Each of these numerical values is assigned according to chapter 3.3.4 logarithmized to the base 0.6. Each characteristic of an assessment parameter is described by a logarithmic score value (see for example Table 59).

AV	Physical	Local	Adjacent	Network
Numerical Value	0.2	0.55	0.62	0.85
log score	3	2	1	0
AC	Low	Medium	High	Very High
Numerical Value	0.77	0.66	0.44	0.33
log score	0	1	2	3
PR*	Full Control	Write	Read	Execute
Numerical Value	0.33	0.44	0.62	0.85
log score	3	2	1	0

Table 59: Assessment parameters of the IT vulnerability metric.
Source: Own table.

In order to determine the attack feasibility or LoE, the severity levels from AV to PR* are determined by experts for each attack path of an existing IT threat scenario. The log scores are then added together. The result is then sorted on a four-point scale. The result is a LoE or Attack Feasibility category associated with an attack path (see Table 60).

Category		High	Medium	Low	Very Low
Score Range		"0-2"	"3-4"	"5-7"	"8-9"
Estimated Probability	Lower Interval Limit (LIL)	0.75	0.5	0.24	0
	Upper Interval Limit (UIL)	1	0.75	0.5	0.25
	Mean of Interval (MI)	0.975	0.625	0.375	0.125

Table 60: LoE scale for assessing IT vulnerability.
Source: Own table.[71]

The Attack Feasibility Scale has a total of four classifications: "Very Low", "Low", "Medium" and "High". According to ISO/SAE 21434 (ISO/SAE, 2021b, p. 47), these can be interpreted as follows (see Table 61):

[71] The assumed probability intervals are set here as examples and distributed equally across the categories of the scale. Due to the lack of an objective mechanism of performance, the CVSS scale cannot yet be made quantitatively compliant.

Likelihood of Exploitability (Attack Feasibility)	Description
High	The attack path can be implemented with very little effort.
Medium	The attack path can be conducted with little effort.
Low	The attack path can be conducted with moderate effort.
Very Low	The attack path can be conducted with great effort.

Table 61: Description of the attack feasibility categories.
Source: Own table based on ISO/SAE (2021b, p. 47).

Vulnerability is also assessed using a scoring-based approach. Harnser scoring is proposed as an example here, which quantitatively conforms to variant ICM 1. This means that moderate scatter is assumed for the assessment variables. Depending on the existing use case, experts must estimate the assumption about the underlying mean values and scatter, which are assigned to the Harnser score levels "1" to "5". Once these have been determined, a Harnser scale can be developed that is quantitatively consistent with the assumed mean values and scatter. Defining specific times for a MAS use case is always a challenge. This is due to the dynamic boundary conditions in the use case. The assessment variables of protection, observation and intervention can be subject to greater uncertainties than critical infrastructures, where static boundary conditions prevail (Möller et al. 2019, p. 307). The specific designation of what observation and intervention in particular represent in the MAS use case must be consolidated with experts.

The definition of criteria can help experts to classify security functionalities in terms of their characteristics (Harnser, 2010, B4, p. 51) (see as an example Table 62):

P-Score	**log score, base = 0.6**	**Criteria for classification**	**ICM 1 Values (sec)**

1	0	Slightly pronounced ability to inhibit overcoming.	μ = 15
			σ = 30

2	1	Limited ability to overcome inhibition.	μ = 45
			σ = 30

3	2	Moderate ability to overcome inhibition.	μ = 75
			σ = 30

4	3	Highly developed skills for overcoming inhibition.	μ = 105
			σ = 30

5	5	Very highly developed ability to overcome inhibition.	μ = 135
			σ = 30

O-Score	**log score, base = 0.6**	**Criteria for classification**	**ICM 1 Values (sec)**

1	0	No technical means of controlling access, minimal human observation of access.	μ = 135
			σ = 30

2	1	Limited technical possibilities for controlling access options, temporary observation of access options by humans.	μ = 105
			σ = 30

3	2	Moderate technical possibilities for controlling access options, moderate observation of access options by humans.	μ = 75
			σ = 30

4	3	High technical possibilities for controlling access options, frequent observation of access options by humans.	μ = 45
			σ = 30

5	5	Very high degree of possibilities to control access at any time and any place through technical measures and/or people.	μ = 15
			σ = 30

I-Score	**log score, base = 0.6**	**Criteria for classification**	**ICM 1 Values (sec)**

1	0	Minor technical and/or human intervention skills.	μ = 135
			σ = 30

2	1	Limited technical and/or human intervention capabilities.	μ = 105
			σ = 30

3	2	Moderate technical and/or human intervention skills.	μ = 75
			σ = 30

4	3	Highly developed technical and/or human intervention skills.	$\mu = 45$ $\sigma = 30$
5	5	Very high level of technical and/or human intervention skills.	$\mu = 15$ $\sigma = 30$

Table 62: Criteria for determining Harnser scores for a MAS Use Case.
Source: Own table based on Harnser (2010, B4, p. 51).[72]

In the same way as when determining the attack feasibility, the numerical values belonging to the protection, observation and intervention scores are logarithmized to a base of 0.6. The log values are set for a physical attack path and the sum of the log scores is calculated to obtain the Likelihood of Vulnerability (LoV) score. If it is assumed that a MAS consists of only one product barrier and the assumptions for ICM variant one apply, then the scoring can be calculated using the assumed probability intervals from Table 41 can be used. The LoV score is sorted accordingly on the four-level Harnser scale (see Table 63).

Category		High	Medium	Low	Very Low
Score Range		"0-5"	"6-8"	"9-11"	"12-15"
Estimated Probability	Lower Interval Limit (LIL)	0.98	0.64	0.2	0.024
	Upper Interval Limit (UIL)	1	0.99	0.8	0.257
	Mean of Interval (MI)	0.99	0.815	0.5035	0.1405
Harnser Score	1	2	3	4	5
log score	0	1	2	3	5

Table 63: LoV scale for classifying physical vulnerability.
Source: Own table.

Similar to Table 61, it is possible to describe the levels using descriptors (see Table 64).

Likelihood of Vulnerability (Attack Feasibility)	Description
High	The asset is very likely to be achieved. The protective effect is low.
Medium	The asset is achieved with moderate probability. The protective effect is medium.
Low	The asset is achieved with a low probability. The protective effect is good.
Very Low	The asset is achieved with a very low probability. The protective effect is very pronounced.

Table 64: LoV Category Description.
Source: Own table based on ISO/SAE (2021b, p. 47).

The choice of protection, observation and intervention scores depends on the existing attack path and the attacker. In IT, the variables AV, AC and UI are assessed along an entire path, regardless of the path length (ISO/SAE, 2021b, p. 76). In physical security, however, "attack path" means that an attacker must overcome a certain combination of barriers to reach the asset (Lichte et al., 2016). In the approach proposed in this paper, experts score protection, observation and intervention for one barrier each. This is because the Harnser scale is made quantitatively compliant with an ICM variant that assesses the vulnerability of a single barrier. For example, if a product has several comparable barriers, the overall vulnerability can be determined as follows:

1. The assessment parameters for the individual barriers are scored by experts.

[72] However, a quantitative level is written behind each criterion, assumed here on the basis of ICM 1.

2. The vulnerability score is determined for each barrier.
3. The vulnerability scores for barrier one and two are sorted into a category on the four-point Harnser scale, which conforms quantitatively to ICM 1.
4. Since each category on the vulnerability scale is followed by a presumed probability interval, a vulnerability level can be determined for each barrier.
5. To obtain the total vulnerability, one option may be to perform the following steps:
    1. For each barrier, the upper interval limit of the assumed probability interval is selected assuming a worst case, e.g. barrier one, "Medium" = 0.98, barrier two, "Very Low" = 0.2.
    2. The two probabilities are multiplied together.
    3. The result is sorted into the categories of the four-point Harnser scale that conforms quantitatively to ICM 1, i.e. here total vulnerability = 0.196 (≙"Very Low"). If the overall vulnerability is 0.8, for example (upper interval limit of the "Low" category and lower interval limit of the "Medium" category), then the category with the higher vulnerability is selected.

For the example of two barriers that are comparable in terms of their security properties, the following are shown in Table 65 shows the values and classifications of the overall Vulnerability for all possible permutations.

Vulnerability Category		Estimated Probability		Vulnerability total	"Vulnerability Path" Category
Barrier 1	Barrier 2	Barrier 1	Barrier 2		Barrier 1 - Barrier 2
Very Low	Very Low	0.2	0.2	0.04	Very Low
Very Low	Low	0.2	0.8	0.16	Very Low
Very Low	Medium	0.2	0.98	0.196	Very Low
Very Low	High	0.2	1	0.2	Low
Low	Very Low	0.8	0.2	0.16	Very Low
Low	Low	0.8	0.8	0.64	Low
Low	Medium	0.8	0.98	0.784	Low
Low	High	0.8	1	0.8	Medium
Medium	Very Low	0.98	0.2	0.196	Very Low
Medium	Low	0.98	0.8	0.784	Low
Medium	Medium	0.98	0.98	0.9604	Medium
Medium	High	0.98	1	0.98	High
High	Very Low	1	0.2	0.2	Low
High	Low	1	0.8	0.8	Medium
High	Medium	1	0.98	0.98	High
High	High	1	1	1	High

Table 65: Scoring-based determination of overall physical vulnerability in the presence of two barriers. Source: Own table.

After the assessment of physical attack paths and IT attack paths, the IT Impact on Physical Vulnerability (ITIPV) is assessed by experts for scenarios with cross-domain interaction (see chapter 3.3.4). The ITIPV scale, like the physical vulnerability assessment and IT exploitability assessment scale, has four categories. The categories can be described as follows (see Table 66).

IT Impact on Physical Vulnerability	Description
High	The protective effect is massively reduced. The LoV is increased by three categories.
Medium	The protective effect is greatly reduced. The LoV is increased by two categories.
Low	The protective effect is moderately reduced. The LoV is increased by one category.
Very Low	The protective effect is slightly reduced. The LoV category remains the same.

Table 66: IT Impact on Physical Vulnerability Category Description.
Source: Own table based on ISO/SAE (2021b, p. 47).

4.4 Assessment (Profiling) of Impacts

If assets, threats and exploitability or vulnerability are assessed, then the impact must also be assessed in order to enable a holistic risk assessment. The effects of successful attacks must therefore be reflected in the risk assessment. The impact can scale differently depending on the type of attack (Termin et al., 2020). CPS is based on the principle "from physical to digital to physical" (Hoffmeister, 2017, pp. 136, 193; Sinha et al., 2015). There are therefore three perspectives for assessing impacts: the physical view (impacts of physical attacks), the IT view (impacts of IT attacks) and the cyber-physical view (impacts of IT attacks on physical scenarios and vice versa). Impacts can primarily be determined on the asset or a component of the asset that is reached by an attacker (Harnser 2010, B6, p. 64). As assets are assessed on a functionality basis in the context of this research work, there is a functionality impact on a component, a unit or entire systems in the event of a successful attack. Physical scenarios with an impact on IT scenarios are not considered below, as the impairment of IT security functions by physical attacks is difficult to quantify.

In principle, there can be different components within a system that are arranged hierarchically in any number of complex ways. The question is how these relationships can be used to classify effects using scale categories. In IT, there is a standard concept called the server-client model (SCM) (DIN SPEC 27070). The SCM describes the relationship between system units and the distribution of tasks between these units. For example, a server provides services for a client. Due to this clear hierarchical structure, it can be assumed that if the server is hacked, the subordinate components can also be hacked. Assume that a component C1 can be attacked via two attack modes. In addition, C1 has the higher-level component C2. C1 can be successfully compromised if C2 is successfully hacked or one of the threat scenarios is successful or if all possibilities occur. The successful compromise of an entity or component is accompanied by an impact that manifests itself in the physical world. For MAS, the impact scale, as described in chapter 3.3.4, is used.

4.5 Assessment (Profiling) of Risks

Risk is determined in accordance with ISO/SAE 21434 using a risk matrix. According to Hubbard et al. (2016), the use of a risk matrix is a proven approach in the industry. "These scales represent both likelihood and impact, not in probabilistic or monetary terms, but in ordinal scales", according to Hubbard et al. (2016, p. 84). According to ISO/SAE 21434, the impact is linked in tabular form with the attack feasibility, e.g. according to CVSS (ISO/SAE, 2021b, pp. 76-77). Each impact/attack feasibility pair is given a score value from "1" (= low) to "5" (= high). The higher the impact and the higher the attack visibility category, the higher the risk score. Attack feasibility is used to assess whether an attack will be successful. This requires a threat on the one hand and vulnerability (exploitability) on the other.

However, the threat probability is not included in the attack feasibility assessment. One reason for this may be the (possible) underlying assumption that a vulnerability can theoretically also be exploited by an attacker if it is present. Nayak et al. (2014) state: "[...] some vulnerabilities are never exploited in the wild, partly due to security technologies that make exploiting them difficult" (Nayak et al., 2014, p. 1). However, Interagency Report 7628 "Guidelines for Smart Grid Cyber Security" published by the National Institute of Standards and Technology (NIST) in 2010 emphasizes in this context: "Software could have vulnerabilities in it at any time [...]. Once a new vulnerability becomes publicly known, risk usually increases because attackers are more likely to develop exploits that target the vulnerable software" (NIST 2010, p. 3). Identified vulnerabilities must therefore be closed by default. In principle, it is not known when an attacker will exploit a vulnerability. However, a threat analysis and risk assessment can be used to determine where vulnerabilities exist in the system and how they could be exploited. Foreman (2019) also clarifies: "The operational and engineering successes of any organization depend on the ability to identify and remediate a vulnerability that a would-be attacker might seek to exploit" (Foreman 2019, p. XV). Building on the considerations from chapter 3.3.4 the risk matrix from ISO/SAE 21434 for the physical risk is as follows Table 67 and for the IT risk Table 68. Based on this scoring, physical and IT risks can be sorted and prioritized according to size.

		Likelihood of Vulnerability (LoV)			
Impact		Very Low	Low	Medium	High
	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Table 67: Physical risk matrix.
Source: Own table based on ISO/SAE (2021b, p. 78).

		Likelihood of Exploitability (LoE)			
Impact		Very Low	Low	Medium	High
	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Table 68: IT risk matrix.
Source: Own table based on ISO/SAE (2021b, p. 78).

One way to focus on major risks is to define a risk acceptance threshold. This means, for example, that experts determine that all risks with a score of less than or equal to "2" are accepted. For all other risks, treatment in the form of a measure implementation is necessary. As both risk matrices have the same classification, they can also be combined in a matrix (see Table 69).

		LoE/LoV			
Impact		Very Low	Low	Medium	High
	Severe	2	3	4	5
	Major	1	2	3	4
	Moderate	1	2	2	3
	Negligible	1	1	1	1

Table 69: Matrix for determining risk scores.
Source: Own table based on ISO/SAE (2021b, p. 78).

4.6 Modeling in Bayesian Networks

After the steps for conducting a threat analysis and risk assessment for CPS have been presented in the previous chapters, the question arises as to a possibility for probabilistically consistent merging. The Bayesian networks method is one option for linking properties from the physical domain and properties from the IT domain in a probabilistically consistent manner. Bayesian networks are already being applied to risk assessment problems involving two domains, for example in Lichte et al. (2019) to assess the impact of cybersecurity on safety using the example of an "x-by-wire system". In Lyu et al. (2020), a "cyber-to-physical" risk analysis model for assessing functional safety taking cyber threats into account is proposed and assessed using the example of an attacked water tank system. The detection and determination of anomalies in CPS is modeled by Bayesian networks in Chockalingam et al. (2017). In Chockalingam et al. (2017), an approach is shown for differentiating between an anomaly caused by a physical fault or by a cyber-attack in order to be able to initiate appropriate measures depending on the cause. Wang et al. (2017) show how Bayesian networks can be used to map the interactions of exploited vulnerabilities within an IT network.

The Bayesian network method is also used in IT security, for example in Xie et al. (2010) and Wu et al. (2017). The method is also used in physical security, for example in Fakhravar et al. (2017) and Argentini et al. (2018). While the vulnerability of physical protection systems (PPS) is modeled and assessed using the example of a gas pipeline in Fakhravar et al. (2017), a chemical plant is considered in Argentini et al. (2018). Bayesian networks are therefore a common method in IT security assessment and physical security assessment. The method is also used to answer questions regarding the interaction of safety and IT security. The advantage of using the Bayesian network method is that the available knowledge and assumptions made can be mapped in a probabilistically consistent manner, i.e. the approach is compatible with probability theory (Koch, 2013). Prokain (2008, p. 74) compares the Bayesian network method with other methods[73] using the criteria of risk sensitivity, subdivision of total losses into expected and unexpected losses, data material requirements, consideration of qualitative and quantitative factors and implementation costs. The aim of the comparison is to find out which approach is particularly suitable for quantifying risks in a deployed IT infrastructure and associated business processes. The results of Prokain's investigations show that Bayesian networks are well suited in this context. The following advantages and disadvantages are named for the use of Bayesian networks (Prokain, 2008, p. 78):

- **Advantages:** Transparent mapping of causal chains, consideration of qualitative and quantitative factors, quantification of losses, subdivision into expected/unexpected losses at different confidence levels possible.
- **Disadvantages:** High demands on the data material, high costs involved in setting up the network.

Based on the aforementioned application potential, it can therefore be assumed that the transfer of expert knowledge into conditional probabilities based on Bayesian networks can also combine the metrics from physical and IT security, resulting in an overall assessment that can also map interactions. Bayesian networks are versatile in terms of their applicability for risk assessment because expert knowledge and causalities can be described by conditional probabilities and actual processes can be represented mathematically (Lyu et al., 2020). In the absence of evidence, expert knowledge is used in security to estimate the probability of certain attack scenarios for a specific use case (Harnser, 2010, A4, p. 42). It must be possible to convert

[73] These are: Key value method, modified basic indicator approach/standardized approach in accordance with Basel II, internal assessment approach, score card approaches, capital asset pricing model, scenario analysis, full conversion and Monte Carlo simulation.

expert knowledge into subjective probabilities (Expert Knowledge Allocation, (Nevo et al., 2012)) in a cross-domain assessment for the physical domain and for the IT domain. As a result, the Bayesian network could, according to the hypothesis, on the one hand represent the knowledge and assumptions about the system components in physical security, and on the other hand represent the knowledge and assumptions about the system components in IT security. This idea also raises the question of how a metric can be transferred into a corresponding network and brought together with another metric or another network.

This chapter explains how TARA for CPS can be successfully transferred to a Bayesian network. The GeNIe Academic software tool is used for modeling (Bayesfusion, 2021). In a Bayesian network in GeNIe, a general distinction is made between "chance nodes" and "deterministic nodes". Chance nodes are mapped as ovals in the GeNIe software and describe uncertain variables. N states can be defined, and these states are assigned probabilities. If nodes are linked together so that a distinction can be made between parent and child nodes, this results in conditional probabilities for the child node. The cause-effect relationship between two nodes is defined by the direction of the arrow. It indicates the direction of influence "from (cause, arrow origin) - to (effect, arrow end)". In GeNIe, probabilities are mapped in probability tables. Deterministic nodes are represented as double circles or double ovals. These are either constantly defined values or values that result (algebraically) from the respective states of the parent nodes, i.e. if the value of a parent node is known, then the value of the deterministic child node is also known with certainty (p = 1).[74]

In contrast to random nodes, the stored probability tables of deterministic nodes only consist of zeros and ones. Deterministic nodes therefore represent a purely binary view. Value nodes can also be represented in GeNIe. Value nodes are represented in the form of hexagons and generally show the expected result of all combinations of the decision alternatives represented in the model, e.g. in the form of a monetary loss value. Submodels can also be mapped in GeNIe. They combine several nodes into units and promote the clarity of models. If a double arrow points from a submodel to a node, this means that there are at least two nodes in the submodel that are parent nodes of the node in the effective direction. If, on the other hand, the arrow only has a single point, there is only one parent node.

4.7 Transfer of the Risk Analysis into a Bayesian Network

The risk analysis begins with profiling the assets. Possible breaches of protection objectives (confidentiality, availability and integrity) are defined for the assets. Damage scenarios are then assigned to these assets. In the next step, threat scenarios are assigned to these damage scenarios and the effects (impacts) of a damage scenario are assessed. Once threat scenarios have been identified, attack paths (implementation options with and without interaction) are analyzed. From an IT perspective, the exploitability of these attack paths is assessed. Vulnerability is assessed from a physical security perspective. For scenarios with cyber-physical interaction, the IT Impact in Physical Vulnerability is used. The risk score is determined using a risk matrix that links the impact with the assessment of the attack paths.[75]

To determine the required CAL and PAL, the impact is linked to the controllability in a table. Measures can be defined to reduce the assurance levels, for example. However, the risk treatment decision step is not considered further here. A clear structure is recognizable in the risk analysis, where a selective connection of assessment variables takes place in the individual

[74] p stands for "probability".

[75] Physical security: Likelihood of Vulnerability (LoV), IT security: Likelihood of Exploitability (LoE).

sub-steps. The risk score, for example, results from a combination of the impact and the assessment of the attack paths. It is therefore determined by these two variables. The idea is now to represent these causal relationships in a Bayesian network. The backward planning approach from classic project management is used for this purpose (Friedrich et al., 2009, pp. 47-87). The output variables at the end of an assessment should be the risk value and the security assurance level (PAL or CAL). The security assurance level is determined by the impact and controllability. For the transfer to a Bayesian network, this means that there are the following nodes: The assurance level node is a child node of controllability and impact. The child nodes of the risk score include the parent nodes Impact and Assessment of the attack path (see Figure 52). The nodes are deterministic here, as a value is assigned to the child node for each combination of the values of the parent nodes.

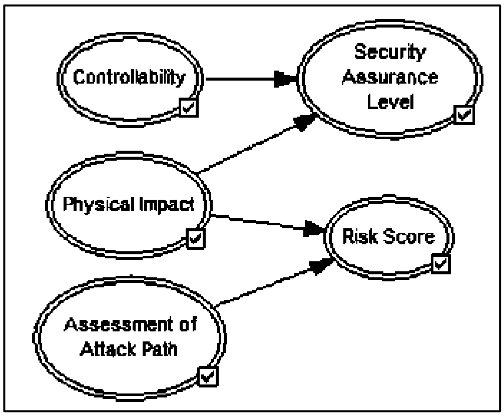
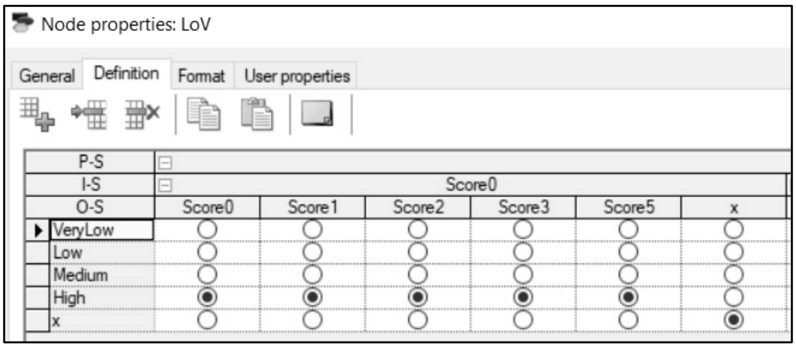


Figure 52: Bayesian network for determining the risk score and the assurance level.
Source: Own Figure.

In physical security, for example, the attack path is assessed using the Harnser scale for physical vulnerability (LoV). The LoV category is determined by the existing combination of the logarithmized Harnser scores of Protection (P), Observation (O) and Intervention (I). The LoV node is thus determined by the three nodes that each describe the log scores (in short: P-S, O-S and I-S). Using the probability table stored with the LoV node, all permutations can be assigned to a LoV category according to the vulnerability scales developed (see Figure 53). All nodes are also defined as deterministic here.



Node properties: LoV

General | Definition | Format | User properties

P-S	⊟					
I-S	⊟ Score0					
O-S	Score0	Score1	Score2	Score3	Score5	x
VeryLow	○	○	○	○	○	○
Low	○	○	○	○	○	○
Medium	○	○	○	○	○	○
High	●	●	●	●	●	○
x	○	○	○	○	○	●

Figure 53: Extract from the LoV probability table.
Source: Own Figure.

A logarithmized Harnser score depends on the Harnser score from "1" to "5" (as descriptor "Very Low" to "Very High"). The nodes of the Harnser scores, P, O and I, are therefore parent nodes of P-S, O-S and I-S. There is a 1:1 mapping from Harnser scores to logarithmized scores. Overall, this results in the following representation (see Figure 54):

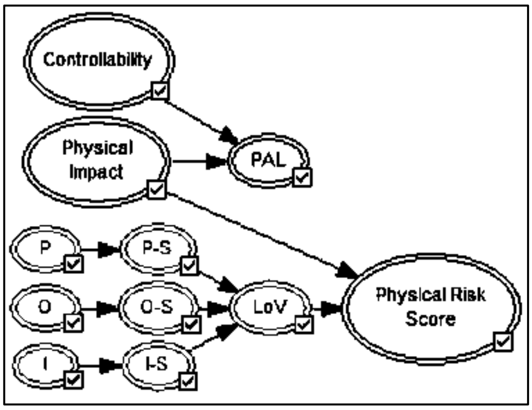


Figure 54: Bayesian network for physical risk assessment.
Source: Own Figure.

The Bayesian network for IT risk assessment can be set up in the same way (see Figure 55). Instead of the assessment variables protection, observation and intervention for physical vulnerability, the CVSS metric is used here to assess the likelihood of exploitability. The assessment variables are the Attack Vector (AV), the Attack Complexity (AC) and the Privileges Required* (PR*). PR* is an assessment parameter proposed in this work, which is made up of the variables Privileges Required (PR) and User Interaction (UI).

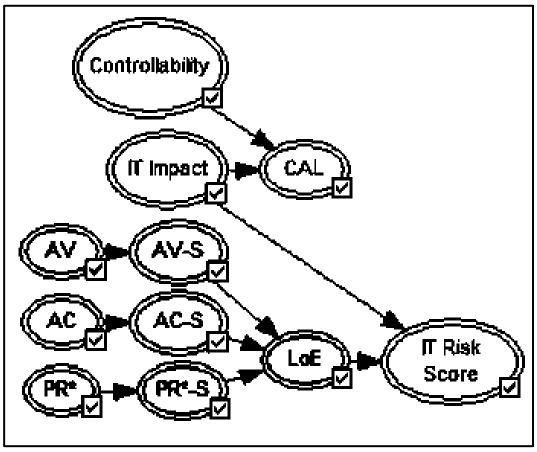


Figure 55: Bayesian network for IT risk assessment.
Source: Own Figure.

Both the scores in physical security and the scores in IT security depend on the attack path under consideration. As two outputs must always be defined for random and deterministic nodes in Bayesian networks to ensure probabilistic consistency, the question arises as to which entry is made for P, O and I if the attack path is not set to "Yes = given" but to "No = not given". A workaround solution, the "undefined" characteristic "x", can be introduced for P, O and I here. For "x", a value "x" is also defined for the log score nodes. If there is at least one log score node with the characteristic "x", the LoV and consequently the assurance level and the risk score are "x". According to TARA in accordance with ISO/SAE 21434, attack paths are determined by a threat scenario (TS) (ISO/SAE, 2021b, pp. 75-77). The fact that an attack path (AP) is possible can be expressed as follows (see Eq. (36)):

$$P(AP|TS) = \begin{cases} 1 & if\ TS = 1 \\ 0 & else \end{cases} \tag{36}$$

For each attack path there is a rating according to Figure 54 and Figure 55 depending on the domain. The controllability depends on the threat scenario. Using the example of physical risk assessment, this results in the network in Figure 56. The designations are shown as examples. The IT security network can be structured according to the same scheme.

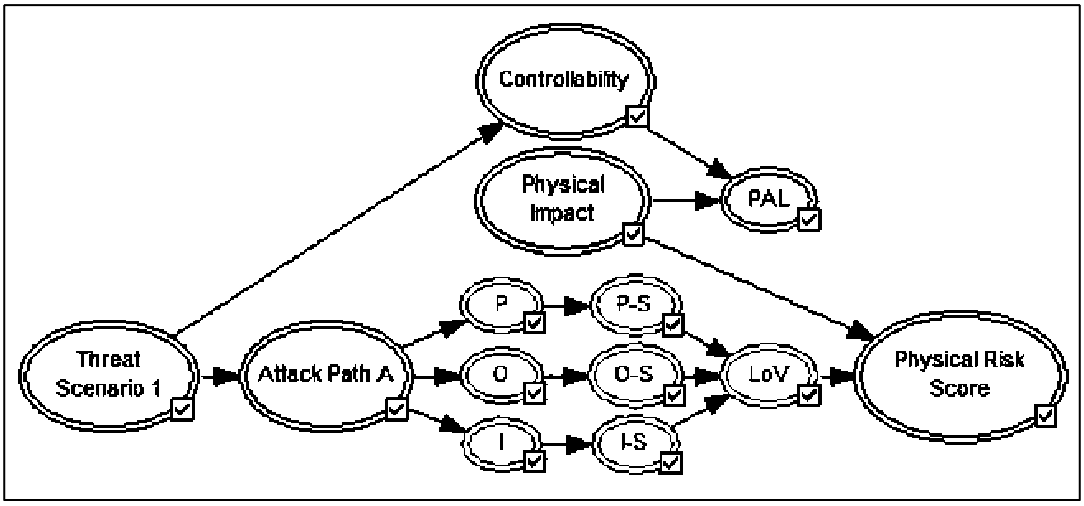


Figure 56: Bayesian network for physical risk assessment with attack path and threat scenario. Source: Own Figure.

The network of Figure 56 can also have a different cause-effect direction between the attack-path and threat-scenario nodes. Instead of defining "The attack path is caused by a single threat scenario", it is also possible to define: "A threat scenario is given under the condition that one or more specific attack paths (AP_i)" (see eq. (37)).

$$P(TS|AP_i) = \begin{cases} 1 & if \ \exists \mathrm{i} \ (AP_i = 1) \\ 0 & else \end{cases} \tag{37}$$

It can be argued here that an attack can only be launched via an attack path if there is a corresponding threat. According to ISO/SAE 21434, several threat scenarios can also be assigned to a damage scenario (ISO/SAE, 2021b, p. 74). The "Physical Impact" node is in the network of Figure 56 because it depends on the respective damage scenario.

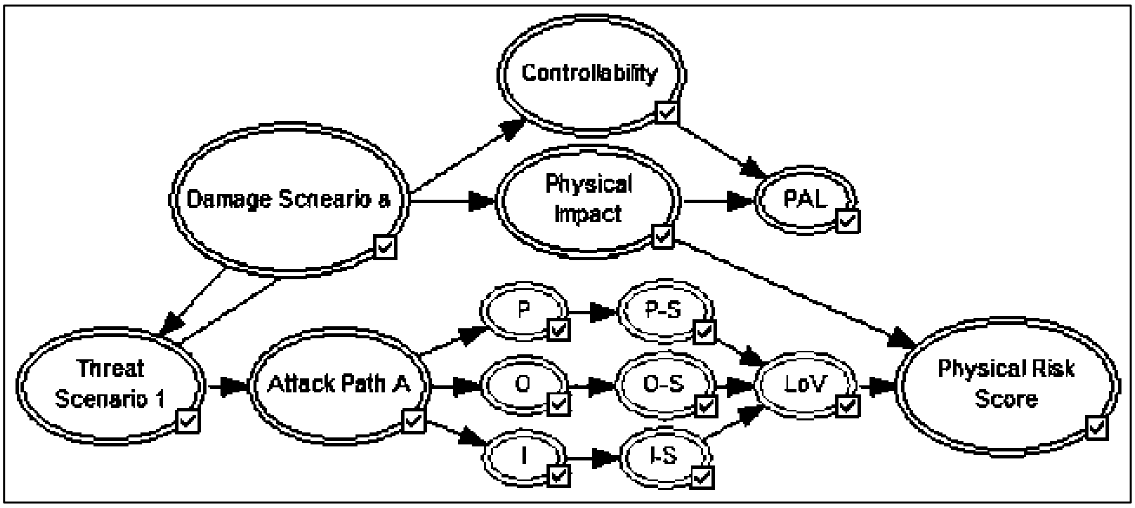


Figure 57: Bayesian network for physical risk assessment including damage scenarios. Source: Own Figure.

A damage scenario depends on the asset in question. It therefore occurs if the asset is present, otherwise not. A damage scenario can also be associated with the possibility of a breach of confidentiality, availability and integrity. The damage scenario node is therefore the parent node of the node that describes the protection goal violation (see Figure 58).

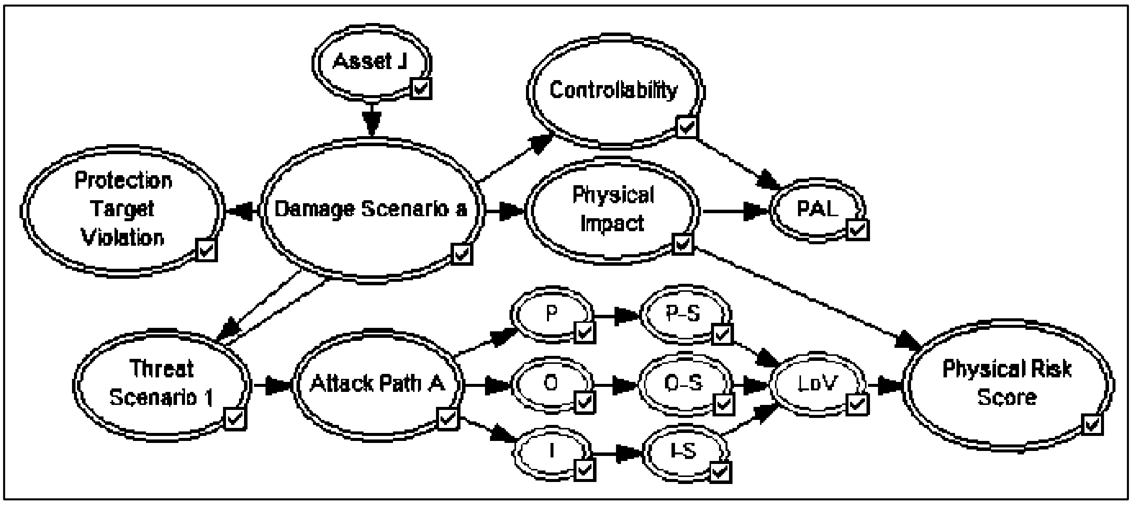


Figure 58: Bayesian network for physical risk assessment according to the risk analysis.
Source: Own Figure.

The Bayesian network of Figure 58 can be transferred to the modeling of IT security (see Figure 59).

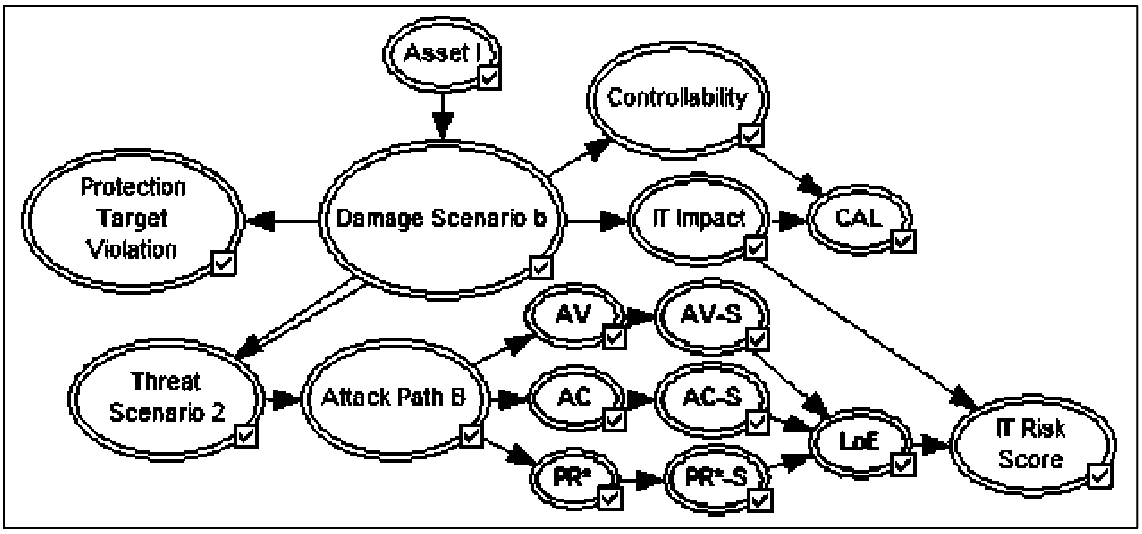


Figure 59: Bayesian network for IT risk assessment according to the risk analysis.
Source: Own Figure.

In a final step, cyber-physical interactions in the Bayesian network are to be depicted. Assume that an interaction is associated with Attack Path B that has an impact on the characteristics of physical security mechanisms. The IT Impact on Physical Vulnerability node is introduced to map this interaction. The IT Impact on Vulnerability is used to assess the severity of the compromise of physical security functions by a successful IT attack. This value depends on the physical vulnerability assessment without taking an IT scenario into account and the physical vulnerability assessment taking an IT scenario into account. If there is an IT impact on physical vulnerability, the affected scenario from the physical domain must be assessed again (see P, O and I nodes in the middle of the Figure 60).

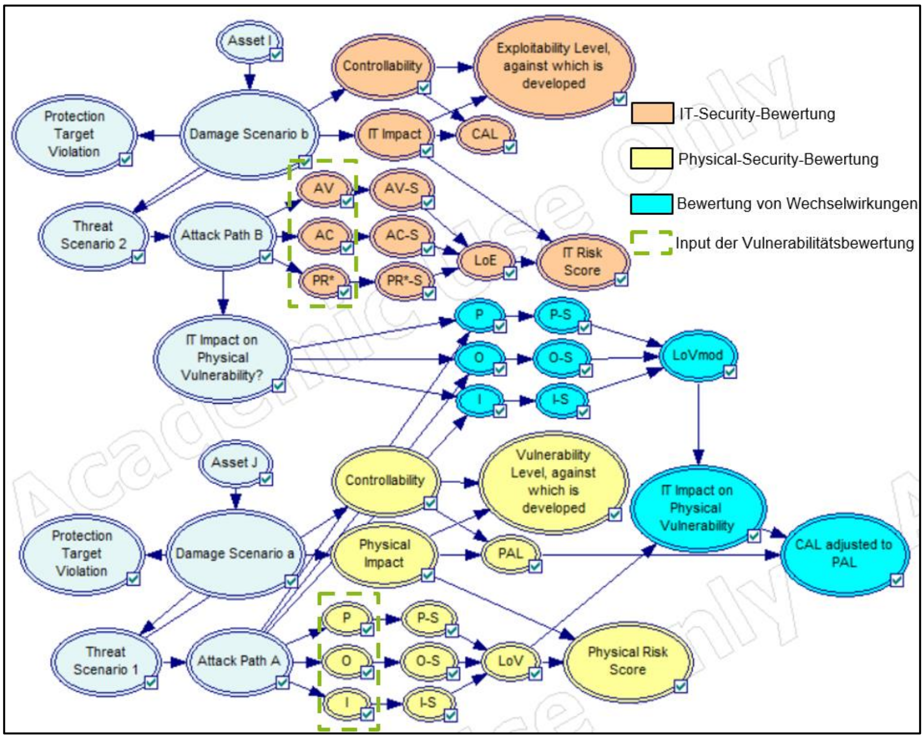
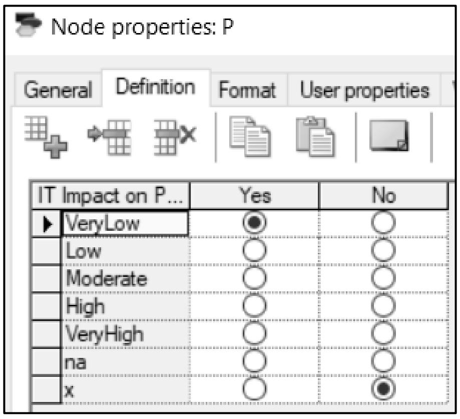

Asset I
Controllability
Exploitability Level, against which is developed
Protection Target Violation
Damage Scenario b
IT Impact
CAL
IT-Security-Bewertung
Physical-Security-Bewertung
Bewertung von Wechselwirkungen
Input der Vulnerabilitätsbewertung
AV
AV-S
Threat Scenario 2
Attack Path B
AC
AC-S
LoE
IT Risk Score
PR*
PR*-S
P
P-S
IT Impact on Physical Vulnerability?
O
O-S
LoVmod
I
I-S
Asset J
Controllability
Vulnerability Level, against which is developed
IT Impact on Physical Vulnerability
Protection Target Violation
Damage Scenario a
Physical Impact
PAL
CAL adjusted to PAL
P
P-S
Threat Scenario 1
Attack Path A
O
O-S
LoV
Physical Risk Score
I
I-S

Figure 60: Bayesian network for cyber-physical risk assessment.
Source: Own Figure.

The IT Impact on Physical Vulnerability node is a child node of attack path B. However, when reassessing physical vulnerability, a special feature applies to the Protection, Observation and Intervention nodes of the Bayesian network: The consideration of the complete elimination of the assessment variables (see example in Figure 61).

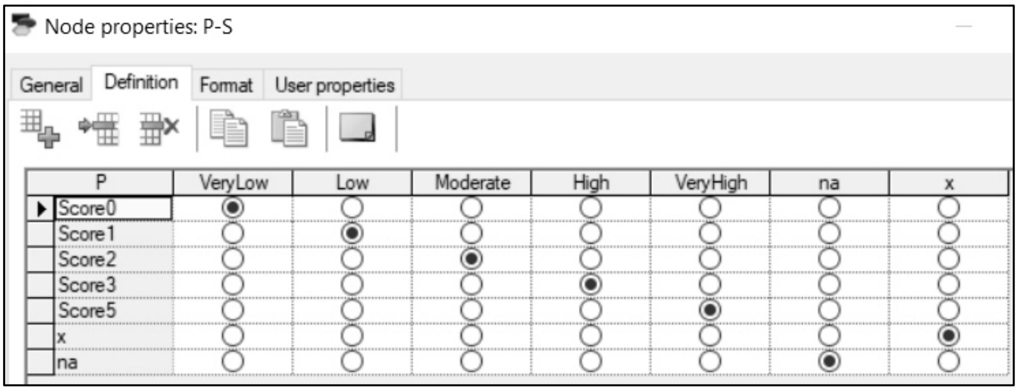


IT Impact on P...	Yes	No
VeryLow	●	○
Low	○	○
Moderate	○	○
High	○	○
VeryHigh	○	○
na	○	○
x	○	●

Figure 61: Characteristics of the protection node including IT Impact on Vulnerability.
Source: Own Figure.

The combination of controllability and impact can also be used, as described in this thesis in chapter 3.3.4 the vulnerability level or the exploitability level according to which product developers should develop can also be determined. Controllability and Impact are parent nodes of "Exploitability Level, against which is developed" (IT security assessment) and "Vulnerability Level, against which is developed" (physical security assessment). The "Physical security level" and "IT impact on vulnerability" nodes are parent nodes of the "CAL adjusted to PAL" node. The CAL of the IT scenario that has an impact on a physical scenario is adjusted depending on the severity of the compromise of physical security functions using the rule from chapter 3.3.4

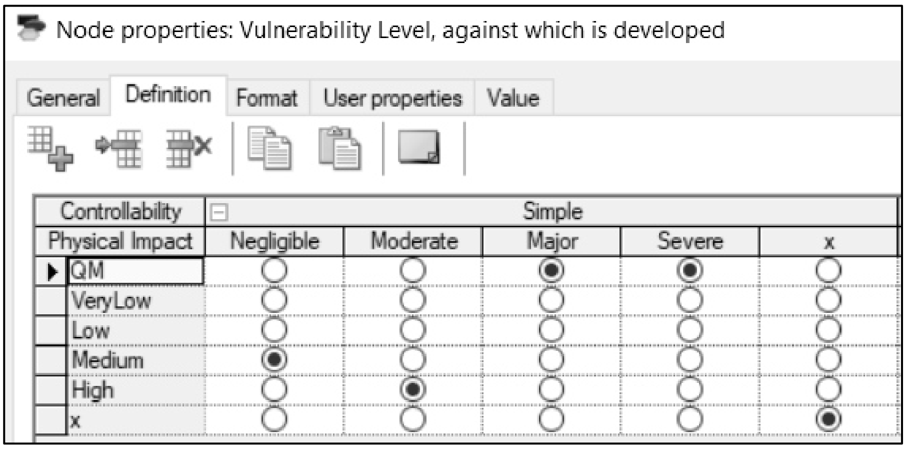
is determined. In addition to the previous specifications, the specification "n. a." (not applicable) is introduced. If this occurs, the IT Impact on Physical Vulnerability is generally rated as "High". For the Observation and Intervention nodes, the "n. a." attribute is also added and included (see Figure 62). When converting the descriptors "High", "Medium", etc. into a score, "n.a." is also added as a characteristic. The "n. a." are linked in the probability table: If the parent node P assumes the characteristic "n. a.", "n. a." occurs in the child node P-S.



P	VeryLow	Low	Moderate	High	VeryHigh	na	x
Score0	●	○	○	○	○	○	○
Score1	○	●	○	○	○	○	○
Score2	○	○	●	○	○	○	○
Score3	○	○	○	●	○	○	○
Score5	○	○	○	○	●	○	○
x	○	○	○	○	○	○	●
na	○	○	○	○	○	●	○

Figure 62: Mapping of characteristics of the protection node to protection scores.
Source: Own Figure.

The result of the score sum of P, O and I is described here by "LoVmod"[76] . The value "n. a." is also added accordingly in the LoVmod node. In a further step, the IT Impact on Physical Vulnerability is determined. For this purpose, the impairment of vulnerability is divided into four degrees of compromise, as described in chapter 3.3.4 is presented. Finally, the CAL to be determined for the IT scenario with an IT Impact on Physical Vulnerability can be determined in accordance with the rules proposed in Chapter 3.3.4. In addition, a vulnerability category can be written for each PAL and each CAL, according to which development is to be conducted. The assignment is made as described in the chapter (see Figure 63).


Node properties: Vulnerability Level, against which is developed
General
Definition
Format
User properties
Value

Controllability	Simple				
Physical Impact	Negligible	Moderate	Major	Severe	x
QM	○	○	●	●	○
VeryLow	○	○	○	○	○
Low	○	○	○	○	○
Medium	●	○	○	○	○
High	○	●	○	○	○
x	○	○	○	○	●

Figure 63: Mapping from controllability and impacts to vulnerability levels.
Source: Own Figure.

Overall, it can be seen that a Bayesian network can be used to combine expert knowledge in a probabilistically consistent manner. However, the size and complexity of the Bayesian network is challenging in this context. In the example from Figure 60 only two assets, two damage scenarios, two threat scenarios and two attack paths are considered. However, as can be seen in the TARA of ISO/SAE 21434, a risk assessment can be much more extensive. This makes it

[76] LoVmod = Likelihood of Vulnerability modified

difficult for industrial users to access and use. To conduct a risk analysis, a tabular presentation, such as that suggested in ISO/SAE 21434, promotes clarity. In addition to a risk register for the physical risk, as outlined in Harnser (2010, B6, p. 66), an IT risk register or a cyber-physical risk register can be set up in accordance with the steps outlined for conducting a risk analysis (see Figure 64). The creation of a risk register is also common practice in IT (Ahmed et al., 2019).

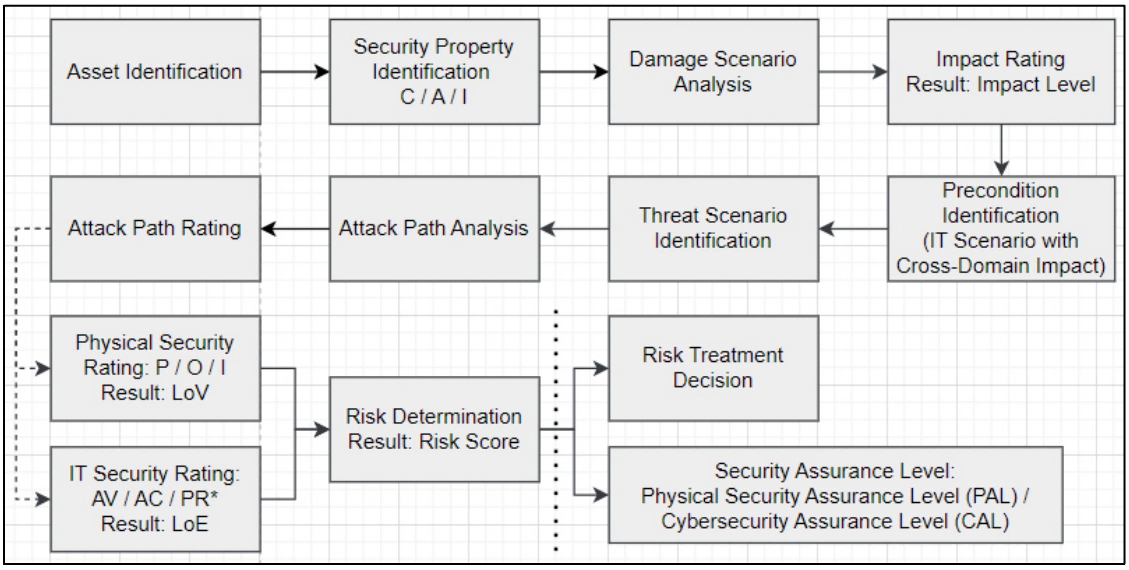

Asset Identification
Security Property Identification C / A / I
Damage Scenario Analysis
Impact Rating Result: Impact Level
Precondition Identification (IT Scenario with Cross-Domain Impact)
Threat Scenario Identification
Attack Path Analysis
Attack Path Rating
Physical Security Rating: P / O / I Result: LoV
IT Security Rating: AV / AC / PR* Result: LoE
Risk Determination Result: Risk Score
Risk Treatment Decision
Security Assurance Level: Physical Security Assurance Level (PAL) / Cybersecurity Assurance Level (CAL)

Figure 64: Work steps for creating a risk register.
Source: Own Figure based on ISO/SAE (2021b).[77]

4.8 Synthesis of Model Input Variables

When analyzing risk using Bayesian networks, the question of how to map uncertainties arises. This requires experts to define the probability values of the model parameters. Expert knowledge can be used in Bayesian networks to either modify the structure of the model, e.g. by adding new nodes and depicting causal relationships in more detail, or to assign probability distributions to the states of the nodes. Random nodes can be used instead of the deterministic nodes for protection, observation and intervention in physical security and the deterministic nodes for the assessment variables Attack Vector, Attack Complexity and User Interaction in IT security. This means that the sum of the probabilities of all states of a node must equal 100 %. Expert knowledge can be interpreted as a subjective degree of conviction (see chapter 2.6.1). For example, a probability of 0.5 means that the variable of interest is located there according to the personal degree of conviction of an expert. A statement can vary from expert to expert (ESFA, 2021, p. 26), because not all experts have the same knowledge about an issue:

> One knowledgeable expert will argue, for example, that a particular framework based on qualitative scores improves decisions, builds consensus, and avoids the problems of more quantitative methods. Another equally qualified expert will argue this is an illusion and that such methods simply do the math wrong. (Hubbard et al., 2016, p. 55).

The transfer of expert knowledge into a security metric is a fundamental prerequisite for the utilization of TARA's Bayesian network. The website Bayesia.com (2021) proposes a combination of the Cooke and Delphi methods to systematically collect expert knowledge for nodes of

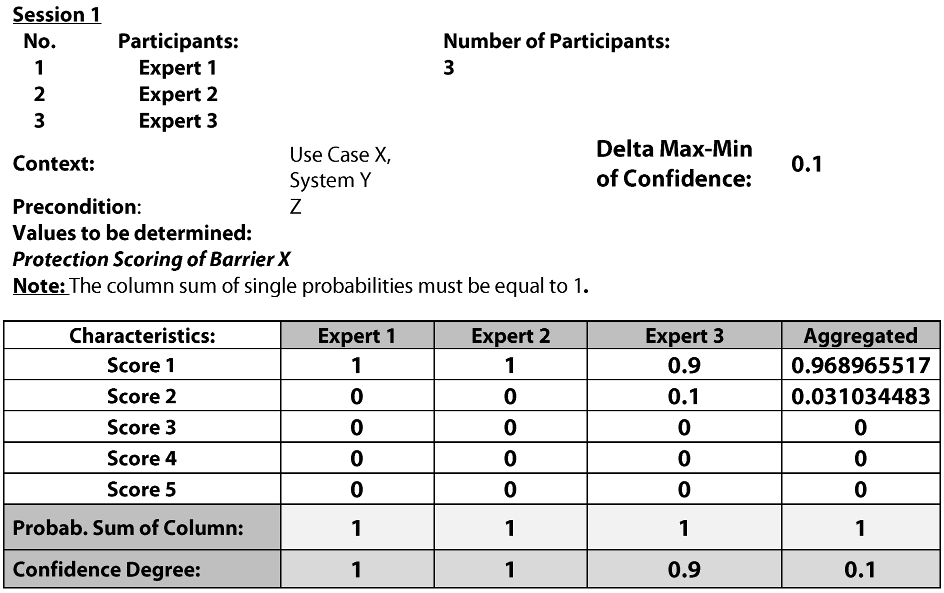
[77] LoE = Likelihood of Exploitability, LoV = Likelihood of Vulnerability, A = Availability, C = Confidentiality, I = Integrity.

a Bayesian network. The approach involves a two-stage survey of several experts by a moderator. The following steps are recommended for preparation (BayesiaLab, 2012): Conducting brainstorming sessions to obtain a clear definition of the objective of the Bayesian network; Identification of the conceptual dimensions associated with the objective; If required: probabilistic training (see also EFSA (2014, p. 8)). The expert survey is divided into two parts. In the first part, the context is presented to the participating experts and the (preconditions) linked to the characteristics of the node under consideration are named. These can be assets, damage scenarios, threat scenarios and the associated attack path assessments.

The participants are then asked to give their personal assessment - their subjective probability distribution - whereby the probability of occurrence of the states under consideration is to be estimated between zero (0 %, low) and one (100 %, high). In addition, the experts must indicate how confident they are with their statement, i.e. they state their personal confidence in the statement made - their confidence - between zero (0 %, low confidence) and one (100 %, high confidence). This approach is adapted in this paper for risk analysis using Bayesian networks. The confidence is used as a means of weighting the expert statements, i.e. if probabilistic statements $x_1, \dots, x_i$ $(0 \leq x_1, \dots, x_i \leq 1)$ from experts with the confidences $c_1, \dots, c_i$ $(0 \leq c_1, \dots, c_i \leq 1)$ are made, then the weighted mean value is calculated using Eq. (38)[78]:

$$m = \frac{\sum_i x_i \times c_i}{\sum_i c_i} = \frac{x_1 \times c_1 + x_2 \times c_2 + \cdots + x_i \times c_i}{c_i + c_2 + \cdots + c_i} \tag{38}$$

The higher the confidence, the greater the weighting of the respective expert statement. This means that expert statements that are uncertain are considered less in the overall assessment due to the weighting (see as an example Table 70).



Session 1

No.	Participants:	Number of Participants:
1	Expert 1	3
2	Expert 2	
3	Expert 3	

Context: Use Case X, System Y — **Delta Max-Min of Confidence:** **0.1**

Precondition: Z

Values to be determined:

Protection Scoring of Barrier X

Note: The column sum of single probabilities must be equal to 1.

Characteristics:	Expert 1	Expert 2	Expert 3	Aggregated
Score 1	1	1	0.9	0.968965517
Score 2	0	0	0.1	0.031034483
Score 3	0	0	0	0
Score 4	0	0	0	0
Score 5	0	0	0	0
Probab. Sum of Column:	1	1	1	1
Confidence Degree:	1	1	0.9	0.1

Table 70: Completed template for eliciting expert knowledge using the example of protection scoring at barrier X.
Source: Own table based on Bayesia.com (2021).

In principle, results are disclosed and discussed in plenary after the first session. In a second session, the request to state subjective probabilities for the same facts is repeated. The purpose of this step is to allow experts to sharpen their opinions again after reviewing the results, if necessary, so that the confidence in the expert statement is increased. The approach does

[78] The approach of weighting an expert statement is also used, for example, in Lichte et al. (2018): Scores are weighted and converted into a quantitative expression.

not involve qualifying experts through calibration questions from the moderator, as is traditionally recommended in the classic Cooke approach (BayesiaLab, 2012) (see chapter 2.6.1).[79] In this approach, the experts assess the confidence in their assessment themselves. On the one hand, this reduces the effort for the moderator to qualify or disqualify experts, while at the same time the moderator must trust that the experts are competent and honest enough to assess the confidence in their assessment.

The formulation of the context and the description of the target values to be defined by the moderator can support experts in specifying a confidence value. The more precisely a specific target variable is described and the more concretely the framework conditions that influence the target variable are named, the more conducive this is to the distillation of the desired expert knowledge. The choice of experts who can make a well-founded statement on a particular issue lies with the moderator. As a result, the moderator's discretion in selecting experts indirectly influences the validity of the result. Assuming that the risk assessment and thus the collection of expert knowledge is conducted by a qualified assessor, the weighting approach is a scalable, simple way of interviewing several experts in order to aggregate expert information quantitatively by weighting subjective probabilities with the associated confidence statements. For this reason, this approach is proposed for the application of TARA's Bayesian network. In order to make the target values sought as accessible as possible to the experts, one option may be to use guiding questions based on the what-if technique, as described in chapter 4.1 "Assuming that the system [...] - how likely is it that the protection has characteristic x?".

Causal relationships that are important for the assessment of the facts should be articulated as simply as possible by the moderator. The key questions are prepared by the moderator before the survey. This type of expert knowledge survey is therefore a "mixed methods" approach, in which a question is first formulated (qualitative part) and then answered by experts in quantitative form (Vogl, 2017). This is then transferred to the model as input. The mixed-method approach can also be used to assess the impact of successful IT attacks on physical security functions. By applying the proposed survey approach to the TARA, different expert assessments can be taken into account. Using the mixed-method approach, it is possible to uncover a spread of vulnerability results. This can occur when different experts rank, for example, protection, observation and intervention or the attack vector, attack complexity or privileges required* differently. The use of different expert opinions can help the operator of a MAS to reconsider the investment in security measures if a defined risk acceptance threshold is not reached, for example: "at least 95 % of risk level "2" must be present".

[79] Methods for improving calibration are presented, for example, in Hubbard et al. (2016, pp.137-154).

5 Discussion

This paper proposes a methodological approach for conducting a cross-domain security assessment of CPS using the example of MAS in mobility applications. Using the methodological approach, it is possible to assess the impact of successful IT attacks on physical security mechanisms. The analysis of previous approaches to cross-domain security assessment shows that the effects of successful IT attacks on physical security have so far hardly been taken into account in threat analyses and risk assessments. In existing security standards for motor vehicles, such as ISO 26262 or ISO/SAE 21434, there are few quantitative methods for cross-domain security assessment that can incorporate uncertainties in the description of security capability. Following on from existing approaches to vulnerability assessment, the properties of a physical system can be described on the basis of effectiveness through protection, observation and intervention. For the description of the characteristics of an IT system, there is no objective mechanism of performance for the representation of protective measures to reduce vulnerability, which is why the security characteristics can only be expressed at an abstract level. Scenario-describing characteristics, such as complexity, the need for privileges and the need for user interactions, are used to describe the security capability of IT systems.

There are challenges in the cross-domain assessment of physical security and IT security due to incompatible metrics for assessing the vulnerability of a system. In physical security, semi-quantitative approaches to vulnerability assessment are used, such as in Harnser (2010). However, there are also quantitative approaches to vulnerability assessment, such as Lichte et al. (2016). In IT security, on the other hand, qualitative and semi-quantitative approaches are mainly used. One example of a semi-quantitative approach is CVSS (First.org, 2022). Because IT security assessment lacks an objective impact mechanism to describe security capability (Jacobs et al., 2019), it is not possible to combine physical security and IT security at the impact-based level and thus at the model level. This is a problem that still needs to be solved.

The differences between the assessment systems from the domains of physical security and IT security lead to the first research question: How can a cross-domain assessment work? To answer this research question, further research questions are formulated in order to break down the problem of cross-domain assessment into individual components. From a scientific point of view, the first question is whether it is possible to compare metrics. This question is posed because the example of physical security assessment can be used to show that although physical vulnerability can be determined using both the Hanser metric according to Harnser (2010) and the vulnerability metric according to Lichte et al. (2016), the results differ greatly in parts. This leads to the research question: How can incompatibilities between two metrics from physical security assessment be quantified and mitigated through measures or requirements?

In this paper, a structured analysis of the Harnser metric (2010) and the vulnerability assessment according to Lichte et al. (2016) from the physical security assessment is conducted to answer this question. For the vulnerability assessment according to Lichte et al. (2016), the term Intervention Capability Metric (ICM) was chosen in line with Garcia (2005). In the Harnser metric, protection, detection and intervention are scored between "1" and "5" and added together. The ICM is used to quantitatively map the time lag between the penetration time of an attacker and the reaction time of a defender. The assessment variables are protection, observation and intervention. First of all, it is noticeable that Lichte et al. (2016) choose a different term for the second assessment parameter than Harnser (2016). According to the argumentation in Lichte et al. (2016), detection is an event that is made up of protection and observation components; consequently, according to this assumption, protection would be included twice in the vulnerability assessment according to Harnser (2010): Once via the scoring of protection and once via the scoring of detection. In addition, the question arises as to what extent experts are able to assess composite events. The following justification is put forward as a basis for argumentation: An expert must first determine the input parameters of a vulnerability metric and feed them into a vulnerability metric in order to be able to make a statement about the vulnerability level. A direct statement of vulnerability by an expert without prior application of a vulnerability metric is therefore difficult. This reasoning is the starting point for the proposal to replace the "detection" assessment parameter in the Harnser metric with the "observation" assessment parameter, so that protection, observation and intervention are now scored in the Harnser metric.

In order to compare the Harnser scoring with the quantitative ICM, it is proposed that the vulnerability scores according to Harnser be sorted into categories on a scale and that these categories be assigned presumed probability intervals. In addition, corresponding time stages are defined in the ICM for the scores "1" to "5". In the ICM, protection, observation and intervention are stored with probabilistic density functions so that uncertainties can be taken into account in the description of security measures. A normal distribution is used in the ICM for protection, observation and intervention, i.e. each of the levels "1" to "5" is assigned a mean value and a standard deviation for the three assessment variables. It is assumed that only one barrier is assessed with the properties of protection, observation and intervention. From the user's point of view, the question arises as to what a meaningful level definition for the ICM might look like. Depending on the application, a definition of "small time jumps" from level to level may be impracticable, and it may also be more appropriate to assume other distributions instead of the normal distribution. In this paper, the normal distribution is used as an example and it is explained that experts can set the levels in the ICM arbitrarily depending on the use case at hand.

Taking into account different metric boundary conditions, such as different types of score aggregation on the part of the Harnser metric and the variation of scatter on the part of the ICM metric, vulnerability levels are determined with both metrics and compared. The vulnerability results are compared according to the total of (5 x 5 x 5 =) 125 permutations considered. The vulnerability values are presented in sorted form, in particular according to the Harnser mean values or ICM values within the Harnser plateaus, which are formed due to the same score totals for different permutations. As a result, objective vulnerability functions are derived from the plotted vulnerability values for both metrics. After assessing the results, measures are identified so that comparable vulnerability levels can be generated with both metrics.

In this paper, the alignment of vulnerability levels is referred to as quantitative conformity. The measures include increasing the dispersion of the quantitative metric and adapting the Harnser vulnerability scale to the curve of the ICM function. It can be seen that the assessment variables for describing the impact mechanism can be converted into consistent scores, so that the different assessments according to Harnser (2010) and Lichte et al. (2016) can be made compatible with regard to the vulnerability classification. It should be noted that the Harnser scoring is only adapted to certain ICM variants, behind which there are clearly defined time steps (assumed mean values and standard deviations for protection, observation and intervention).

To summarize, the quality of the Harnser metric for physical security can be sharpened and verified by adapting it to the vulnerability results of the ICM. This is possible because it is assumed that the quantitative assessment based on the ICM according to Lichte et al. (2016) can be used to represent real vulnerability levels. The quantitative assessment metric is not adapted in such a way that it can be used to depict the scoring-based results according to Harnser (2010). According to the considerations in Gigerenzer (2014, pp. 44-47, 130-131), it should rather be possible to assess reality using a simplified algorithm (a "good, simplifying rule of thumb"). In the context of physical security assessment, for example, this means the results of the ICM ("reality") should be represented by a scoring ("rule of thumb"). Instead of adapting the parameters of the quantitative ICM to a flawed scoring, it is necessary to define requirements for the scoring so that the same vulnerability levels can be generated with the different assessment metrics according to Harnser (2010) and Lichte et al. (2016). An approach to metric analysis is therefore developed so that it is possible to quantify how good a non-quantitative metric is and to what extent certain measures lead to fewer incompatibilities between the scoring and the quantitative metric. Based on this, it is possible to compare metric versions, as proposed for example in Harnser (2010) and Lichte et al. (2016), and to make a statement about the conditions under which one specific way of combining expert knowledge in a scoring is better than another.

In this paper, the Harnser scoring is adapted to specific ICM variants using different scales. It is shown that the interval widths per scale category generally increase the fewer scale categories there are. This means that if, for example, a four-item Harnser scale is made quantitatively compliant with an ICM variant, the assumed probability intervals behind these four categories are significantly wider than in the case of, for example, a thirteen-item Harnser scale that is made quantitatively compliant with the same ICM variant. If a Harnser scale is adapted to several ICM variants, the assumed probability intervals per scale category also become larger. In addition, the interval limits per scale category increasingly overlap. As a result, the Harnser scoring suggests a sometimes large range of vulnerability. The question here is to what extent it helps product developers who carry out a physical security assessment if the result suggests a vulnerability of 0.2 to 0.8, for example. The larger the assumed probability intervals behind the scale categories, the more difficult the decision becomes regarding the investment of scarce resources in security measures to reduce physical vulnerability. This is a disadvantage of using Harnser scales, which have few scale categories and are adapted to several ICM variants. In this context, it is a challenge to find a balance between practicability (number of scale categories used) and the usability of scoring results (related to the interval width of the suspected vulnerability level).

Scoring-based approaches are widely used in IT security assessments. In simplified terms, it is said that "1" is bad and "5" is good. Assessment variables are scenario-describing parameters, such as attack vector, attack complexity, etc. In the case of CVSS (First.org, 2022), they are linked via a metric without a stored objective mechanism of performance to describe the effect of measures on vulnerability reduction, resulting in a vulnerability classification that cannot be quantitatively verified. This means that in IT security, the kind of metric refinement demonstrated by the Harnser metric and Intervention Capability Metric is difficult to implement. The latest considerations take the approach of interpreting the assessment variables in the CVSS as consecutive barriers and logarithmizing the associated scores. The transformation is proposed because the calculation of the CVSS parameters involves a multiplicative link. At the same time, logarithmization solves problems with quantitative scales of different magnitudes, to which the assessment parameters are assigned on a uniform scale, e.g. "1" to "4". To solve the problem of calculating ordinal values, the scoring system must be adapted to vulnerability values of a quantitative metric with an objective mechanism of performance, as shown in the example of the Harnser metric and the ICM, with regard to the assumed probability intervals behind the scale categories. Since a quantitative metric with an objective mechanism of performance is missing for the CVSS, the paper raises the question of how to assess whether proposals for changing the CVSS assessment metrics will bring improvements.

Now, on the one hand, there are the classical scoring approaches, e.g. CVSS, and on the other hand barrier-based scoring approaches, e.g. Braband (2019), in which the transformation of exploitability contributions (according to CVSS) to log scores is proposed. In this work, it can be shown analytically that the application of a log transformation to a multiplicative scoring metric reduces distortions. However, this assumes that true risk contributions and the scaling between the numerical values of the true risk contributions are known. In order to be able to test the quality of metric or model modifications, a quantitative metric is required that can be used to transfer and recalculate the considerations made in Braband (2019). However, the CVSS of IT security does not provide this because it lacks the ability to quantify correctly and assess based on effectiveness. As part of the analysis in Termin et al. (2022), the considerations from IT security are mimicked in physical security in order to examine the plausibility of the considerations made in the IT security assessment. However, the results were inconclusive.

In addition, it is explained that, for example, the barrier of the attack vector to describe the context of an attack must always have a value for logical reasons. It must not be zero: without an attack vector, there is no threat context and therefore no possibility of exploiting a vulnerability in a system. In contrast to the other assessment variables, the User Interaction and Privileges Required barriers have the value "None". If User Interaction and Privileges Required have this value, there are essentially no barriers. The assessment parameters also have different levels of severity: The Attack Vector has four, the Attack Complexity two, the Privileges Required three and the User Interaction two. The levels of the assessment parameters within the CVSS are therefore different. Efforts are being made in this work to adapt the levels so that, firstly, they always describe an activation state and, secondly, that each CVSS parameter has the same number of levels.

Finally, based on the considerations in Braband (2019), it is discussed how the assessment variables Privileges Required (PR) and User Interaction (UI) can be transferred into one assessment variable. This is done because PR and UI describe the same thing from different perspectives: Privileges are required in some form to perform a particular attack. Following Dürrwang et al. (2021), it is proposed to merge the PR and UI assessment variables into one assessment variable PR*, which has the four characteristics "Execute", "Read", "Write" and "Full Control". The merging of PR and UI is done to resolve the incompatibility between the barrier-based CVSS model and the CVSS metric as introduced in Braband (2019). At the same time, the combination offers the advantage that three assessment parameters are assessed in both the IT security assessment and the physical security assessment. The disadvantage, however, is that the proposed specification of the PR* assessment parameter cannot be confirmed quantitatively because, unlike in the physical security assessment, there is no quantitative metric for adjusting the PR* exploitability contributions.

Based on the approaches developed in this thesis for aligning a semi-quantitative vulnerability metric (Harnser metric) with a quantitative vulnerability metric (ICM) and for assessing suggestions for improving a semi-quantitative metric without an underlying, objective mechanism of performance (barrier-based CVSS approach), the first research question is taken up again: How can a cross-domain assessment work? In this paper, vulnerability descriptions and vulnerability assessments in physical security and IT security are analyzed in more detail. The analysis shows that a path-based vulnerability model can be mapped in both security domains: In physical security, an attack path (scenario) can be described by a combination of (disjoint) physical barriers in series up to the asset. In IT security, an attack path is also a combination of (disjunctive) barriers in series that an attacker has to overcome to reach an asset. However, these barriers can have exploitable vulnerabilities. A physical attacker can choose from a combination of barriers to gain access to a physical asset. An IT attacker, on the other hand, can choose from a combination of barriers and vulnerabilities to reach an IT asset.

In both security domains, risk can be described by the product of threat, vulnerability and impact. This tripartite division can be reduced to a bipartite division, vulnerability multiplied by impact, if two conditions are present:

1. The contributions of threat, vulnerability and impact are completely disjoint from each other. In addition, this idealization assumes strict independence between the three contributions.
2. The threat probability is assumed to be 100 % (p = 1.00). This means that the security capability of a system is considered in the event of an attack.

The physical risk can thus be described by "R = V · I", while the IT risk can be described by "R = E · I" (E := Exploitability, IT vulnerability). To combine the physical and IT impacts, this paper proposes defining a harmonized scale, e.g. with scores from "1" to "4". It is assumed that each score level is described by a descriptor in such a way that both physical impacts and IT impacts can be found. Experts then provide monetary loss values for each score level from "1" to "4". Each score/loss value pair can be transferred to a coordinate system as a point. The scores from "1" to "4" on the abscissa are assigned to the loss values on the ordinate. The points entered can be described by a mathematical function. If an impact score is fed into the mathematical function, the corresponding monetary impact results as a functional value. The mathematical function of the impact is required at a later stage when merging the risk assessments in physical security and IT security.

In addition to the impact, vulnerability (physical security) and exploitability (IT security) must also be assessed. If a barrier and an asset are assumed as a reference model in physical security, then the physical vulnerability can be assessed through the interaction of protection, observation and intervention at this barrier. If a barrier with a vulnerability is assumed as a reference model in IT security, then IT vulnerability (exploitability) can be assessed, for example, by the exploitability-describing aspects of the CVSS, Attack Vector, Attack Complexity, Privileges Required and User Interaction. Braband (2019) suggests logarithmizing the CVSS scores and sorting them into categories on an exploitability scale. In order to first of all enable an alignment of the scores from physical security using the Harnser example and IT security using the CVSS example, it is proposed to conduct the log transformation of the scores for the vulnerability and exploitability contributions. The dimensioning in both scorings is standardized using a common basis. For the quantitative conformity of the Harnser scale to specific ICM variants, it is irrelevant how the already arbitrary Harnser scores are arrived at. Based on ISO/SAE 21434, a four-part rating scale for vulnerability is developed, which can be described, for example, using the descriptors "Very Low", "Low", "Medium" and "High" (ISO/SAE, 2021b, p. 78). This offers the advantage that the vulnerability assessment in physical security and the assessment in IT security are structured in the same way at a procedural level. Both the physical vulnerability and the IT vulnerability are determined on the basis of log scoring. The result is sorted on a four-point scale.

A Harnser scale for assessing physical vulnerability is developed, which consists of four categories and is quantitatively compliant with ICM 1. For each scale category, a vulnerability score can be written for the semi-quantitative scoring metric from "1" to "4". The assumed probability intervals behind the categories of the Harnser scale consist of a Lower Interval Limit (LIL) and an Upper Interval Limit (UIL). Consequently, a vulnerability score consists of two parts, LIL and UIL. Each vulnerability score/LIL value pair and vulnerability score/UIL value pair can be interpreted as a point and entered in a coordinate system. These points can be mapped for the LIL values and UIL values using a mathematical function for vulnerability. These mathematical functions are used in this paper to describe vulnerability.

A four-tier scale is also developed for the exploitability assessment, which is based on the CVSS-based approach in Braband (2019). Insofar as it is assumed that the back-transformation of the score sums corresponds to true exploitability contributions, assumed probability values (LIL and UIL) can also be written behind the categories of the exploitability scale. The quantitative exploitability value belonging to the lowest score of a category can be defined as the lower presumed probability of exploitability (LIL), while the highest score can be defined as the upper presumed probability of exploitability (UIL). For each scale category, an exploitability score can be written for the semi-quantitative scoring metric from "1" to "4". The exploitability score also consists of two parts, LIL and UIL. Each exploitability score/LIL value pair and exploitability score/UIL value pair can be interpreted as a point and entered in a coordinate system. These points can be mapped for the LIL values and UIL values using a mathematical function for the exploitability. These mathematical functions are used in this work to describe the exploitability.

In a final step, the mathematical functions for vulnerability or exploitability and the effects are integrated into the risk equations ("R = V · I" and "R = E · I") and then logarithmized. The base to which the impact contribution is logarithmized is chosen as 10 for both assessments, for example. The base to which the vulnerability contribution and the exploitability contribution are each logarithmized is set to 0.6 for both assessments in line with Braband (2019) The result is two risk functions each for the physical risk and for the IT risk, R_{LIL} and R_{UIL}. For example, the first risk function is used to calculate the physical risk assuming the LIL values for vulnerability. The second risk function is then used to calculate the physical risk, assuming the UIL values for vulnerability. For example, if vulnerability scores and impact scores are used in the first risk function (R_{LIL}) and the result is then back-transformed using the inverse function of the logarithm, a quantitative value for the risk is obtained. This value corresponds to a true risk level.

In this work, it can be shown that distortions within multiplicative scoring metrics can be reduced by (skillful) logarithmization. Overall, it can be shown that it is possible to align the risk assessments by harmonizing the scales of the risk contributions. However, this only works if the true values of the risk contributions are actually known. It is also assumed that the exploitability scores or vulnerability scores for the multiplicative risk scoring metric cannot be directly specified by experts. Rather, the application of a vulnerability metric in the physical security assessment and the application of an exploitability metric in the IT security assessment are required to determine a vulnerability level or exploitability level. The proposed approach works if the assumed probability intervals behind the scale categories can be adapted to objective vulnerability or exploitability levels. In both security domains, this requires a quantitative metric that can be used to determine objective vulnerability or exploitability values. In IT security, however, such a metric is difficult to find.

For a cross-domain security assessment to be successful, there needs to be a way of assessing scenarios from physical security and IT security, between which there may be interactions. The IT Impact on Physical Vulnerability (ITIPV) assessment parameter is introduced to assess the severity of an interaction between IT scenarios and physical scenarios. The ITIPV describes the impairment of physical security functions by an IT scenario. This impairment results in an increase in physical vulnerability. To determine the IT impact on physical vulnerability, two calculations are proposed. The physical scenario is assessed once without and once with consideration of an interaction by experts in order to measure the severity of the interaction via the ITIPV. In both cases, the vulnerability scores are sorted on the four-point rating scale and the categories for both scenarios are compared with each other. This approach is considered sensible because neither the Harnser metric nor the ICM takes IT threats into account. Because the scale of the Harnser metric is made quantitatively compliant by means of concrete ICM variants, a real vulnerability level can be inferred from the assessment of the impairment of physical security functions via the scoring.

In addition, it shows how security levels can be derived so that product development can be based on a vulnerability level behind a specific level. Security levels define the extent to which components or systems must be protected against certain attacks. In ISO/SAE 21434 (IT security), for example, the Cybersecurity Assurance Level (CAL) is used to classify security levels. The CAL classification is based on a tabular assignment of the attack vector to the effects of a threat scenario. It is initially proposed that the impact scale - as set out in the merging of risk assessments in physical security and IT security - be structured in the same way for both domains and set up in four sections based on ISO/SAE 21434. This step is considered necessary so that both the effects of threat scenarios from physical security and the effects of threat scenarios from IT security can be reflected in the impact scale. At the same time, a normalized impact scale creates a prerequisite for firstly being able to better compare risk levels in physical security and IT security and secondly to determine security levels for both security domains in the same way.

First of all, consideration is given to determining the physical assurance levels (PAL) such as the CAL (Cybersecurity Assurance Levels) in accordance with ISO/SAE 21434: The attack vector (context of an attack) is linked to the effects in a table. Not all IT attack vectors are a subset of the physical attack vectors, i.e. only PAL classifications for the combination of the attack vector "Physical" with the effects are permitted here. In the CAL matrix, the impact/attack vector pairs "Major-Physical" and "Moderate-Physical" are assigned the same CAL (CAL "1"). This means that two impact levels are assigned to the same security level. The question now is how a possible PAL matrix can be defined. In this work, it is determined that the PAL matrix and the CAL matrix must be structured differently, assuming a tabular link between the attack vector and the effects, so that security levels "1" to "4", for example, can be found in both assessments. For this reason, we are looking for a way to structure the security level matrix so that it is the same for both security domains.

An attempt is then made to construct the matrix for determining the security level for physical security and IT security in the same way as the Automotive Safety Integrity Levels (ASIL) matrix from ISO 26262: The impact and frequency are linked against the controllability in a table, i.e. each triplet (consisting of an impact, frequency and controllability rating) corresponds to a security classification. Controllability is a parameter from ISO 26262 and describes the possibility of avoiding (further) damage if a dangerous situation occurs. This assessment parameter is interpreted as a possibility for postvention in the field of security: To what extent can a system operator limit damage after an attack, e.g. through emergency plans, remote revocation of authorizations, etc.? Since a vulnerability level should stand behind a security level, the frequency must not be substituted by the vulnerability rating, for example. It is also associated with challenges if the threat probability is written instead of the frequency. This is due to the fact that threats are epistemic. The execution of an attack is subject to the arbitrariness of an attacker. In addition, security assessments that consider scenarios that have not occurred do not have any evidence to make statistical estimates.

For this reason, a matrix has been developed instead in which the impact of a threat scenario is set in relation to the so-called controllability. Each individual impact/controllability pair corresponds to a physical or IT security level between "1" (low level) and "4" (high level). Levels "1" to "4" are assigned to vulnerability levels in a further step: Level "4" is assigned the lowest vulnerability level "Very Low", and so on. Behind the four vulnerability levels, the assumed probability intervals of the quantitatively compliant, four-tier Harnser metric for variant ICM 1 (moderate scatter) are assumed in this paper. The choice of a four-tier scale is due to the fact that the international standard ISO/SAE 21434 proposes a four-tier classification of vulnerability. In principle, the vulnerability levels can be defined differently from use case to use case. Consultation with experts from product development is required for this.

For the assignment of security levels to physical scenarios and IT scenarios, between which there are cross-domain interactions, this paper proposes that in the event of an impairment of physical security mechanisms, the IT scenario should be assigned the same level as the physical scenario or a higher level. For economic reasons, a rule is introduced that can help users to modify the security level for the IT scenario, taking into account the ITIPV. The CAL is upgraded depending on the severity of an interaction. The scoring systems developed for physical security and IT security are then transferred into a structured procedure for threat analysis and risk assessment (TARA) in accordance with ISO/SAE 21434 as part of a risk assessment. This is then transferred to a Bayesian network in order to show that expert knowledge about the security capability of a cyber-physical system can be linked probabilistically and consistently within the domains of physical security and IT security. In addition, it is shown that interactions can also be mapped in a Bayesian network. In addition, possibilities for synthesizing model input variables using expert knowledge via a weighting approach are presented. Experts who have more confidence in their probability statements than others are given more weight in the overall result than experts who have less confidence in their probability statements. This is useful in that it feeds multiple expert assessments into the Bayesian network. It can be seen that the complexity of the network in the case of multiple attack scenarios can limit the practicality of this method.

The tabular summary of the risk analysis steps in a risk register, as shown in Harnser (2010, B6, p. 66), for example, is recommended instead of using a Bayesian network because the Bayesian network can become confusing if many threat scenarios (with cross-domain effects) are mapped. In contrast to the tabular TARA, however, the application of the Bayesian network offers the advantage that the spread in the results of a risk assessment due to different expert opinions on all input variables can be revealed. While only one expert rating is noted in the tabular TARA, any number of expert opinions can be taken into account in the Bayesian network by applying the weighting approach presented. If, after an expert survey and feeding the expert statements into the network, it is determined that, for example, 90% risk score "1" exists and 10% risk score "2", the product managers can consider whether acceptance is possible or whether a more detailed analysis is necessary. After the cross-domain risk assessment, the following steps can be conducted as suggested in ISO/SAE 21434: Determination of the type of risk treatment (security claims), definition of security objectives (security goals), definition of security measures (in the case of the mitigation risk treatment option) and derivation of security requirements.

In summary, there are various ways to reduce distortions within a metric. As demonstrated in this paper, one possibility is to change the distribution of numerical values via a transformation. Another option is to process the information content of risk contributions or vulnerability contributions and to check the consistency of assessment steps. The purpose of this processing is, for example, to identify and remove invalid or erroneous values and steps in the risk assessment. In the classic Harnser metric, for example, protection, detection and intervention are scored. However, detection is a composite event consisting of protection and observation components. It is questionable whether experts can immediately assess composite events without a known underlying metric.

In addition, when scoring protection, detection and intervention, protection would be included twice, once via the scoring of protection and once via the scoring of detection. By substituting observation for the detection assessment parameter, the elementary components of the physical mechanism of performance are assessed. Incompatibilities between two security metrics from different domains can be reduced by first prioritizing the risk contributions and excluding them from the risk assessment using (cleverly chosen) assumptions. If, for example, disjointness between the risk contributions threat, vulnerability and impact is assumed in the risk description "R = threat x vulnerability x impact" and it is defined that there is strict independence between the risk contributions, then multiplication is permitted. Insofar as the security capability of a system is assessed in the event of an attack (threat probability = 100%), the threat components associated with epistemic uncertainties can be excluded as part of the proposed procedure for conducting a prospective risk analysis. Further measures to reduce metric incompatibilities can be:

1. The metrics are normalized, i.e. the contributions of a risk metric or contributions of a vulnerability metric are brought to a comparable scale. One way to bring numerical values to a comparable scale is to apply a suitable data transformation. One example of this is the min-max normalization method: numerical values are transformed so that they all lie in a common range, e.g. between 0 and 1 or between 0 and 1000. Another possibility is logarithmic transformation, as demonstrated in this paper.
2. The metrics are converted into a common risk description, e.g. "risk = (threat x) vulnerability x impact" and a common unit, e.g. for vulnerability [%] and for impact [Euro]. These measures improve the comparison of two metrics.
3. A new security metric is being developed that ideally allows a quantitative, effectiveness-based assessment and can combine information from both metrics. Risk contributions are mapped on a common scale in this new metric.

In Table 71 the possibilities and limitations of merging physical security and IT security across domains are listed. The systematic approach developed makes a contribution to providing tools for conducting a cross-domain risk assessment.

Possibilities	Boundaries
Adjustment of the scale (division), Adjustment of the dimensioning and characteristics of the scores, standardization of the assessment process (see chapter 3, 4).	No cross-domain model with underlying, effectiveness-based metrics can be realized because the mechanism of performance in IT is missing (see chapter 3.3.1).
Transfer of quantitative parameters into consistent scores possible (see chapter 3.1).	Quality of the results based on the IT assessment system cannot be validated with metrics from IT (see chapter 3.3.3, 8.1).
Cross-domain security analysis with impact direction IT-physically mappable (see chapter 3.3.4, 4.3).	Emulated, barrier-based approach difficult to apply in practice. Protection, observation and intervention must be traced back to performance-based barriers (see chapter 3.2.2).
Probabilistically consistent merging of knowledge about the security capability of physical and IT system elements in a Bayesian network. In addition, expert knowledge can be fed into the network (see chapter 4.7, 4.8).	Cross-domain security analysis with direction of impact physical-IT cannot be mapped (see chapter 3.3.4).
Alignment of the scale levels of the vulnerability contributions from the physical security assessment with the scale levels of the vulnerability contributions from the IT security assessment (see chapter 3.3.3).	Alignment of the scale levels of the vulnerability contributions from the IT security assessment with the scale levels of the vulnerability contributions from the physical security assessment is only possible to a limited extent (see chapter 5).
Derivation of security levels for the domains of physical security and IT security (see chapter 3.3.4).	Arbitrary compression or expansion of scale categories, so that widely differing dimensions can be aligned in scales, is difficult to represent (see chapter 3.2.3).
Definition of security levels for an IT scenario if it has an impact on physical vulnerability (see chapter 3.3.4)	

Table 71: Opportunities and limitations in cross-domain merging.
Source: Own table.

6 Summary and Follow-Up Research

This research work introduces a mixed-method or mixed-metric approach to the risk assessment of MAS. In the sense of a continuous improvement process, the generic approach can be used repetitively according to the respective threat situation. It can be seen that a cross-domain assessment is possible, taking into account the direction of impact of IT scenarios on physical scenarios, because vulnerability in physical security can be assessed based on effectiveness using a quantitative metric, e.g. the ICM according to Lichte et al. (2016). Conversely, the cross-domain assessment is not possible because an effectiveness-based, quantitative assessment is difficult to find in IT security, i.e. if development is based on a CAL, it is not possible to provide sufficient proof that the exploitability that could be behind a CAL is actually achieved. In physical security, on the other hand, this is possible.

This research has been able to identify a solution for adapting the Harnser metric according to Harnser (2010) to the ICM according to Lichte et al. (2016) so that both assessments result in comparable vulnerability classifications. Incompatibilities between these two metrics can be reduced by extending the Harnser scale categories with assumed probability intervals and adjusting these to quantitative vulnerability values according to the ICM. Distortions within the Harnser metric (Harnser 2010) and within the CVSS (First.org, 2022) are analyzed qualitatively and reduced through suitable measures. On the Harnser metric side, for example, the assessment parameter Detection is replaced by the assessment parameter Observation. For the CVSS metric, for example, it is proposed that the assessment parameters PR and UI be merged into one assessment parameter because they essentially describe the same thing from different points of view.

The scorings according to Harnser (2010) and CVSS (First.org, 2022) are aligned via a log transformation and harmonization of the scale categories, so that vulnerability scores can be classified for both domains at process level on a four-tier scale - as proposed in this paper. Security levels for the physical security and IT security domains can be determined using a matrix with the same structure for both domains and, in the event of an existing interaction, can be coordinated with each other depending on the severity of this interaction. The proposed Harnser metric and the proposed CVSS metric are integrated as a building block for the attack path rating in a threat analysis and risk assessment based on the international standard ISO/SAE 21434. Furthermore, it can be shown how expert knowledge about the security capability in the domains of physical security and IT security can be linked probabilistically and consistently within a Bayesian network.

The findings of this work contribute to the risk-appropriate design of security metrics. They can be used as part of follow-up research to advance the development of a new IT security metric that allows the quantification of IT vulnerability and can be traced back to the effectiveness-based assessment parameters from physical security assessment, protection, observation and intervention. The results of this work can be used to pursue the harmonization of the description and assessment of threats in the domains of physical security and IT security, so that the metrics of all three risk contributions are built up in a risk-appropriate manner. Furthermore, the approaches presented can be used to enable the merging of metrics from functional safety and physical security or IT security.

7 Literature

7.1 Print Sources

Reference in the text	Source reference
Abendroth (2004)	Abendroth, J. (2004). Active strategies for protection target violation detection through controlled power sharing in the access control architecture. In *Detection of intrusions and malware & vulnerability assessment, GI SIG SIDAR workshop, DIMVA 2004*. Gesellschaft für Informatik e.V.
Ahmed (2019)	Ahmed, J. (2019). Empirical Analysis of a Cybersecurity Scoring System. *Digital Common*. University of California.
Ahmed et al. (2019)	Ahmed, Y., Naqvi, S., & Josephs, M. (2019, May). Cybersecurity metrics for enhanced protection of healthcare IT systems. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1-9). IEEE.
Aigner & Khelil (2020)	Aigner, A., & Khelil, A. (2020, June). A benchmark of security metrics in cyber-physical systems. In *2020 IEEE International Conference on Sensing, Communication and Networking (SECON Workshops)* (pp. 1-6). IEEE.
Aigner & Khelil (2021)	Aigner, A., & Khelil, A. (2021, May). A security scoring framework to quantify security in cyber-physical systems. In *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)* (pp. 199-206). IEEE.
Aldasso et al. (2022)	Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989.
Alguliyev et al. (2018)	Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212-223.
Allodi et al. (2018)	Allodi, L., Cremonini, M., Massacci, F., & Shim, W. (2018). The effect of security education and expertise on security assessments: The case of software vulnerabilities. *arXiv preprint arXiv:1808.06547*.
Al Shalabi & Shaaban (2006)	Al Shalabi, L., & Shaaban, Z. (2006, May). Normalization as a preprocessing engine for data mining and the approach of preference matrix. In *2006 International conference on dependability of computer systems* (pp. 207-214). IEEE.
Anderson (2001)	Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.
Anthony (2008)	Anthony (Tony) Cox Jr, L. (2008). What's wrong with risk matrices: *Risk Analysis: An International Journal*, *28*(2), 497-512.
Arabsorkhi & Ghaffari (2018)	Arabsorkhi, A., & Ghaffari, F. (2018, December). Security metrics: principles and security assessment methods. In *2018 9th International Symposium on Telecommunications (IST)* (pp. 305-310). IEEE.
Aradau (2010)	Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security dialogue*, *41*(5), 491-514.
Argentini et al. (2000)	Argenti, F., Landucci, G., Reniers, G., & Cozzani, V. (2018). Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. *Reliability Engineering & System Safety*, *169*, 515-530.
Arnold (2013)	Arnold, D. (2013). Eliciting perceptual prominence at the syllable and word level: the influence of rating scales, rating levels, and normalization.

Ashibani & Mahmoud (2017) Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81-97.

Balzer & Schorn (2011) Balzer, G., & Schorn, C. (2011). *Asset management for infrastructure assets-energy and water.* Berlin: Springer.

Bandow & Holzmüller (2009) Bandow, G., & Holzmüller, H. H. (2009). *This is not a model at all*! Wiesbaden: Gabler.

Becker et al. (2019) Becker, W., Stradtmann, M., Botzkowski, T., Böttler, L., Voigt, K. I., Müller, J. M., & Veile, J. W. (2019). Economic risks of Industry 4.0. *Business models in the digital world: strategies, processes and practical experiences*, 493-515.

Bennett (1977) Bennett, H. A. (1977). *EASI approach to physical security assessment* (No. SAND--76-0500). Sandia Labs.

Bertsche & Lechner (2006) Bertsche, B., & Lechner, G. (2004). *Reliability in automotive and mechanical engineering: Determination of component and system reliability.* Berlin, Heidelberg: Springer.

Bormann et al. (2018) Bormann, R., Fink, P., Holzapfel, H., Rammler, S., Sauter-Servaes, T., Tiemann, H., & Weirauch, B. (2018). *The future of the German automotive industry* (No. 03). WISO Discourse.

Bowen et al. (2021) Bowen, Z. O. U., Mengkun, L. I., & Ming, Y. A. N. G. (2021). Vulnerability learning of adversary paths in Physical Protection Systems using AMC/EASI. *Progress in Nuclear Energy*, *134*, 103666.

Box & Cox (1964) Box, G. E., & Cox, D. R. (1964). An analysis of transformations. *Journal of the Royal Statistical Society: Series B (Methodological)*, *26*(2), 211-243.

Braband (2003) Braband, J. (2003). Improving the risk priority number concept. *Journal of System Safety*, *39*(3), 21-23.

Braband (2004) Braband, J. (2004). Definition and analysis of a new risk priority number concept. In *Probabilistic Safety Assessment and Management: PSAM 7-ESREL'04 June 14-18, 2004, Berlin, Germany, Volume 6* (pp. 2006-2011). Springer London.

Braband (2008) Braband, J. (2008). Limited risk. In: *QZ. Quality and Reliability*, 53(2), 28-33.

Braband (2012) Braband, J. (2011, December). A Risk-based Approach towards Assessment of Potential Safety Deficiencies. In *Achieving Systems Safety: Proceedings of the Twentieth Safety-Critical Systems Symposium, Bristol, UK, February 7-9th, 2012* (pp. 209-223). London: Springer.

Braband (2016) Braband, J. (2016). Why 2 times 2 ain't necessarily 4 -at least not in IT security risk assessment. *arXiv preprint arXiv:1603.03710.*

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

Broy et al. (2013) Broy, M., & Kuhrmann, M. (2013). *Project organization and management in software engineering.* Heidelberg / Berlin: Springer Berlin Heidelberg.

Burns et al. (1995) Burns, A., McDermid, J., & Dobson, J. (1992). On the meaning of safety and security. *The Computer Journal*, *35*(1), 3-15.

Cardenas et al. (2009) Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security* (Vol. 5, No. 1).

Cheng et al. (2014)	Cheng, Y., Deng, J., Li, J., DeLoach, S. A., Singhal, A., & Ou, X. (2014). Metrics of security. *Cyber defense and situational awareness*, 263-295.
Chockalingam et al. (2017)	Chockalingam, S., Pieters, W., Teixeira, A., & van Gelder, P. (2017). Bayesian network models in cyber security: a systematic review. In *Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8-10, 2017, Proceedings 22* (pp. 105-122). Springer International Publishing.
Cockburn (2000)	Cockburn, A. (2000). Writing Effective Use Cases Addison. *Addison-Wesley Professional.*
Coffey et al. (2016)	Coffey, J. W., Baskin, A., & Snider, D. (2016). Knowledge elicitation and conceptual modeling to foster security and trust in SOA system evolution. *Emerging trends in the evolution of service-oriented and enterprise architectures*, 41-58.
Colson et al. (2020)	Colson, A. R., & Cooke, R. M. (2018). Expert elicitation: using the classical model to validate experts' judgments. *Review of Environmental Economics and Policy.*
Conlon (2016)	Conlon, J. (2016). *Why string theory?* CRC Press.
Cooke (1994)	Cooke, N. J. (1994). Varieties of knowledge elicitation techniques. *International journal of human-computer studies*, *41*(6), 801-849.
Costantino et al. (2022)	Costantino, G., De Vincenzi, M., & Matteucci, I. (2022). In-depth exploration of ISO/SAE 21434 and its correlations with existing standards. *IEEE Communications Standards Magazine*, *6*(1), 84-92.
Dobaj et al. (2021)	Dobaj, J., Ekert, D., Stolfa, J., Stolfa, S., Macher, G., & Messnarz, R. (2021). Cybersecurity Threat Analysis, Risk Assessment and Design Patterns for Automotive Networked Embedded Systems: A Case Study. *Journal of Universal Computer Science,* 27(8), 830-849.
Printer (2015)	Drucker, P. (2015). *If you can't measure it, you can't manage it.* Market Culture Blog, 685-718.
Dürrwang et al. (2021)	Dürrwang, J., Sommer, F., & Kriesten, R. (2021). Automation in automotive security by using attacker privileges. Ruhr University Bochum.
EFSA (2014)	European Food Safety Authority. (2014). Guidance on expert knowledge elicitation in food and feed safety risk assessment. *EFSA Journal*, *12*(6), 3734.
Fakhravar et al. (2017)	Fakhravar, D., Khakzad, N., Reniers, G., & Cozzani, V. (2017). Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. *Process Safety and Environmental Protection*, *111*, 714-725.
Fennelly et al. (2016)	Fennelly, L., & Perry, M. (2016). *Physical security: 150 things you should know.* Butterworth-Heinemann.
Field (2013)	Field, A. (2013). *Discovering statistics using IBM SPSS statistics.* Sage.
Foreman (2019)	Foreman, P. (2019). *Vulnerability management.* CRC Press.
Fosch-Villaronga & Mahler (2021)	Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer law & security review*, *41*, 105528.
Furnell et al. (2013)	Furnell, S., Lambrinoudakis, C., & López, J. (Eds.). (2013). *Trust, Privacy, and Security in Digital Business: 10th International Conference, TrustBus 2013, Prague, Czech Republic, August 28-29, 2013. Proceedings* (Vol. 8058). Springer.
Gandal et al. (2020)	Gandal, N., Riordan, M. H., & Bublil, S. (2020). A New Approach to Quantifying, Reducing and Insuring Cyber Risk: Preliminary Analysis and Proposal for Further

Research. *Reducing and Insuring Cyber Risk: Preliminary Analysis and Proposal for Further Research (February 26, 2020).*

Garcia (2005) — Garcia, M. L. (2005). *Vulnerability assessment of physical protection systems.* Elsevier.

Garcia (2007) — Garcia, M. L. (2007). *Design and assessment of physical protection systems.* Elsevier.

Geisberger & Broy (2012) — Geisberger, E., & Broy, M. (Eds.). (2012). *agendaCPS:*
Integrated Research Agenda Cyber-Physical Systems (Vol. 1). Springer-Verlag.

Gigerenzer (2014) — Gigerenzer, G. (2014). *Risk: how to make the right decisions.* btb.

Gneiting & Raftery (2007) — Gneiting, T., & Raftery, A. E. (2007). Strictly proper scoring rules, prediction, and estimation. *Journal of the American statistical Association*, *102*(477), 359-378.

Gordon et al. (2003) — Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

Graja et al. (2020) — Graja, I., Kallel, S., Guermouche, N., Cheikhrouhou, S., & Hadj Kacem, A. (2020). A comprehensive survey on modeling of cyber-physical systems. *Concurrency and Computation: Practice and Experience*, *32*(15), e4850.

Grimm (2008) — Grimm, R., Hundacker, H., & Meletiadou, A. (2008). *Application examples for cryptography.* University of Koblenz-Landau.

Grimm (2019) — Grimm, J. (2019). *Key management for dummies.* A Wiley Brand. Entrust Special Edition.

Grossert (1989) — Grossert, E. (1989). *Investigations on the load-bearing behavior of solid bridges with two-cell box cross-section.* Inst. für Baustoffe, Massivbau u. Brandschutz.

Grushka-Cohen et al. (2016) — Grushka-Cohen, H., Sofer, O., Biller, O., Shapira, B., & Rokach, L. (2016, October). CyberRank: knowledge elicitation for risk assessment of database security. In *Proceedings of the 25th ACM International on Conference on Information and Knowledge Management* (pp. 2009-2012).

Gupta (2016) — Gupta, N. K. (2016). *Inside Bluetooth low energy.* Artech House.

Hawking & Mlodinow (2010) — Hawking, S., & Mlodinow, L. (2010). The (elusive) theory of everything. *Scientific American*, *303*(4), 68-71.

Herrmann (2002) — Herrmann, D. S. (2002). *Using the Common Criteria for IT security assessment.* Auerbach publications.

Hoffmeister (2017) — Hoffmeister, C. (2017). *Digital business modeling: developing and strategically anchoring digital business models.* Carl Hanser Verlag GmbH Co KG.

Howard (1958) — Howard, M. (1958). The conversion of scores to a uniform scale. *British Journal of Statistical Psychology, 11(2),* 199-207.

Hubbard et al. (2016) — Hubbard, D. W., & Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk John Wiley & Sons. *Inc, Hoboken, NJ, USA.*

Humayed et al. (2018) — Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security-A survey. *IEEE Internet of Things Journal*, *4*(6), 1802-1831.

Ingoldsby (2010) — Ingoldsby, T. R. (2010). Attack tree-based threat risk analysis.
Amenaza Technologies Limited, 3-9.

Ittermann et al. (2018) — Ittermann, P., & Niehaus, J. (2018, January). Industry 4.0 and change in industrial work-revisited. State of research and trend definitions. In *Digitalization of industrial work* (pp. 33-60). Nomos Verlagsgesellschaft mbH & Co KG.

Jacobs et al. (2019) — Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I., & Roytman, M. (2021). Exploit prediction scoring system (epss). *Digital Threats: Research and Practice*, *2*(3), 1-17.

Johnson (2010) — Johnson, R. E. (2010, November). Survey of SCADA security challenges and potential attack vectors. In *2010 international conference for internet technology and secured transactions* (pp. 1-5). IEEE.

Jones (2007) — Jones, J. R. (2007). "Estimating software vulnerabilities." In: IEEE Security & Privacy, 5(4), 28-32.

Kan (2002) — Kan, S. H. (2002). *Metrics and models in software quality engineering.* Addison-Wesley Professional.

Kandasamy et al. (2020) — Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18.

Keene (1995) — Keene, O. N. (1995). The log transformation is special. *Statistics in medicine*, *14*(8), 811-819.

Clipper (2015) — Klipper, S. (2015). *Information Security Risk Management.* Springer Fachmedien Wiesbaden.

Cook (2013) — Koch, K. R. (2013). *Introduction to Bayesian statistics.* Springer-Verlag.

Kofler et al. (2018) — Kofler, M., et al. (2020). *Hacking & Security: The comprehensive handbook.* Rheinwerk publishing house.

King (2005) — König, H. (2005). *Peer-to-Peer Intrusion Detection Systems for the Protection of Sensitive IT Infrastructures.* German Informatics Society.

Konstantinou et al. (2015) — Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015, May). Cyber-physical systems: A security perspective. In *2015 20th IEEE European Test Symposium (ETS)* (pp. 1-8). IEEE.

Koscher et al. (2010) — Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., & Savage, S. (2010, May). Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy* (pp. 447-462). IEEE.

Kriaa et al. (2015) — Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability engineering & system safety*, *139*, 156-178.

Krisper (2021) — Krisper, M. (2021). Problems with risk matrices using ordinal scales. *arXiv preprint arXiv:2103.05440*.

Krisper et al. (2019) — Krisper, M., Dobaj, J., Macher, G., & Schmittner, C. (2019). RISKEE: a risk-tree based method for assessing risk in cyber security. In *Systems, Software and Services Process Improvement: 26th European Conference, EuroSPI 2019, Edinburgh, UK, September 18-20, 2019, Proceedings 26* (pp. 45-56). Springer International Publishing.

Kumar et al. (2014) — Kumar, S., Dalal, S., & Dixit, V. (2014). The OSI model: Overview on the seven layers of computer networks. *International Journal of Computer Science and Information Technology Research*, *2*(3), 461-466.

Kumar et al. (2017) Kumar, S. A., & Xu, B. (2017, June). Vulnerability assessment for security in aviation cyber-physical systems. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 145-150). IEEE.

Laughlin et al. (2000) Laughlin, R. B., & Pines, D. (2000). The theory of everything. *Proceedings of the national academy of sciences*, *97*(1), 28-31.

Lee et al. (2017) Lee, E. A., & Seshia, S. A. (2016). *Introduction to embedded systems: A cyber-physical systems approach*. With Press.

Lehn et al. (2000) Lehn, J., Müller-Gronbach, T., Rettig, S., Lehn, J., Müller-Gronbach, T., & Rettig, S. (2000). Regression. *Introduction to descriptive statistics*, 99-117.

Lichte et al. (2016) Lichte, D., Marchlewitz, S., & Wolf, K. D. (2016). A quantitative approach to vulnerability assessment of critical infrastructures with respect to multiple physical attack scenarios. In *Future Security 2016, Proceedings intern. conf., Berlin, Germany.*

Lichte et al. (2017) Lichte, D.; Marchlewitz, S.; Wolf, K.-D. and N. Schlüter (2017). An Approach to Holistic Safety and Security Risk Assessment Considering Contradictory Requirements under Uncertainty. European Safety and Reliability Conference ES-REL 2017, 18.-22.06.2017, Portoroz, Slovenia.

Lichte et al. (2018) Lichte, D., & Wolf, K. D. (2018). A study on the influence of uncertainties in physical security risk analysis. In *Safety and Reliability-Safe Societies in a Changing World* (pp. 1387-1394). CRC Press.

Lichte et al. (2019) Lichte, D., & Wolf, K. D. (2019, September). Bayesian network based analysis of cyber security impact on safety. In *Proceedings of the 29th European Safety and Reliability Conference, Hannover, Germany* (pp. 22-26).

Lichte et al. (2020a) Lichte, D., Termin, T., & Wolf, K. D. (2020). On the Impact of Uncertainty on Quantitative Security Risk Assessment. In *30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM15 2020* (pp. 4938-4945). Research Publishing Services.

Lichte et al. (2020b) Lichte, D., Witte, D. & Wolf, K. D. (2020). Comprehensive Security Hazard Analysis for Transmission Systems. In *ISCRAM 2020 Conference Proceedings - 17th International Conference on Information Systems for Crisis Response and Management (Blacksburg, VA, USA, 2020)*. Edited by A. Hughes; F. McNeill; C. W. Zobel. Virginia Tech.

Lichte et al. (2021) Lichte, D., Witte, D., Termin, T., & Wolf, K. D. (2021). Representing Uncertainty in Physical Security Risk Assessment: Considering Uncertainty in Security System Design by Quantitative Analysis and the Security Margin Concept. *European Journal for Security Research*, 1-21.

Lun et al. (2019) Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Di Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, *149*, 174-216.

Luo et al. (2020) Luo, C., Xu, L., Li, D., & Wu, W. (2020). Edge computing integrated with blockchain technologies. *Complexity and Approximation: In Memory of Ker-I Ko*, 268-288.

Luxhøj et al. (2016) Luxhøj, J. T., Shih, A. T., Ancel, E., & Jones, M. (2012). Safety risk knowledge elicitation in support of aeronautical R&D portfolio management: A case study. In *33rd Annual International Conference of the American Society for Engineering Management 2012, ASEM 2012-Agile Management: Embracing Change and Uncertainty in Engineering Management* (pp. 676-684).

Lyu et al. (2020) Lyu, X., Ding, Y., & Yang, S. H. (2020). Bayesian network based C2P risk assessment for cyber-physical systems. *IEEE Access*, *8*, 88506-88517.

Macher et al. (2015)	Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015, March). SAHARA: a security-aware hazard and risk analysis method. In *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 621-624). IEEE.
Macher et al. (2020a)	Macher, G., Schmittner, C., Dobaj, J., Armengaud, E., & Messnarz, R. (2020). An integrated view on automotive spice, functional safety and cyber-security. SAE.org.
Macher et al. (2020b)	Macher, G., Schmittner, C., Veledar, O., & Brenner, E. (2020). ISO/SAE DIS 21434 automotive cybersecurity standard-in a nutshell. In *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops: DECSoS 2020, DepDevOps 2020, USDAI 2020, and WAISE 2020, Lisbon, Portugal, September 15, 2020, Proceedings 39* (pp. 123-135). Springer International Publishing.
Malavasi et al. (2022)	Malavasi, M., Peters, G. W., Shevchenko, P. V., Trück, S., Jang, J., & Sofronov, G. (2022). Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics*, *106*, 90-114.
Martins et al. (2015)	Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Tang, C., & Candell, R. (2015, August). Towards a systematic threat modeling approach for cyber-physical systems. In *2015 Resilience Week (RWS)* (pp. 1-6). IEEE.
Michna et al. (2017)	Michna, S., & Gierds, C. (2017). Security as a basic building block of digitization. In *2nd Automotive Symposium Wildau: Proceedings Technical University of Applied Sciences Wildau 2017* (pp. 25-30).
Microsoft Corporation (2005)	Microsoft Corporation (2005). The STRIDE threat model.
Mo et al. (2011)	Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2011). Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, *100*(1), 195-209.
Möller et al. (2019)	Möller, D. P., & Haas, R. E. (2019). *Guide to automotive connectivity and cybersecurity*. Springer International Publishing.
Morr et al. (2019)	El Morr, C., Ali-Hassan, H., El Morr, C., & Ali-Hassan, H. (2019). Descriptive, predictive, and prescriptive analytics. *Analytics in healthcare: a practical introduction*, 31-55.
Nayak et al. (2014)	Nayak, K., Marino, D., Efstathopoulos, P., & Dumitraş, T. (2014). Some vulnerabilities are different than others: Studying vulnerabilities and attack surfaces in the wild. In *Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014. Proceedings 17* (pp. 426-446). Springer International Publishing.
Neudörfer (2011)	Neudörfer, A. (2011). *Designing safety-compliant products*. Springer.
New builder (2018)	Neugebauer, R. (2018). *Digitalization*. Springer Berlin Heidelberg.
Neuman (2009)	Neuman, C. (2009, July). Challenges in security for cyber-physical systems. In *DHS workshop on future directions in cyber-physical systems security* (pp. 22-24). Edited by Nabil Adam: US Department of Homeland Security.
Newsome (2013)	Newsome, B. (2013). *A practical introduction to security and risk management*. Sage Publications.
Nguyen et al. (2020)	Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020). Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access*, *8*, 87592-87608.

Oakley & O'Hagan (2010) Oakley, J. E. & Anthony O'H. (2010). SHELF: the Sheffield elicitation framework (version 2.0). School of Mathematics and Statistics, University of Sheffield, UK (http://tonyohagan. co. uk/shelf, accessed 26.01.2021).

Ostrom & Wilhelmsen (2019) Ostrom, L. T., & Wilhelmsen, C. A. (2019). *Risk assessment: tools, techniques, and their applications*. John Wiley & Sons.

Paar & Pelzl (2016) Paar, C., & Pelzl, J. (2016). *Cryptography understandable*. Springer Berlin Heidelberg.

Pasqualetti et al. (2015) Pasqualetti, F., Dörfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE transactions on automatic control*, *58*(11), 2715-2729.

Pearl (2011) Pearl, J. (2011). *Bayesian networks.* EScholarship. UCLA Department of Statistics Papers.

Petr et al. (2022) Mell, P., Spring, J., Dugal, D., Ananthakrishna, S., Casotto, F., Fridley, T., & Turner, C. (2022). *Measuring the Common Vulnerability Scoring System Base Score Equation*. National Institute of Standards and Technology, Gaithersburg, MD.

Piper (2020) Piper, J. W. (2020). *Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis*. Technical Report, STO-MP-IST-166.

Prokain (2008) Prokein, O. (2008). *IT Risk Management: Identification, Quantification and Economic Control*. Springer-Verlag.

Ponsard et al. (2021) Ponsard, C., Ramon, V., & Deprez, J. C. (2021). Goal and Threat Modeling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434. in *SECRYPT* (pp. 833-838).

Puhani (2020) Puhani, J. (2020). *Statistics: Introduction with practical examples*. Springer-Verlag.

Puls et al. (2021) Puls, T., Olle, W., Proff, H., Falck, O., Czernich, N., Koenen, J., & Möller, T. (2021). Structural change in the automotive industry-is the pandemic acting as an accelerator? *ifo Schnelldienst*, *74*(05), 03-35.

Rajkumar et al. (2010) Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th design automation conference* (pp. 731-736).

Randle et al. (2019) Randle, C. H., Bond, C. E., Lark, R. M., & Monaghan, A. A. (2019). Uncertainty in geological interpretations: Effectiveness of expert elicitations. *Geosphere*, *15*(1), 108-118.

Ritz (2015) Ritz, F. (2015). *Betriebliches Sicherheitsmanagement: Aufbau und Entwicklung widerstandsfähiger Arbeitssysteme*. Schäffer-Poeschel.

Ruddle et al. (2009) Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., & Wolf, M. (2009). Deliverable D2. 3: Security requirements for automotive on-board networks based on dark-side scenarios. *EVITA project.*

Saltelli et al. (2010) Saltelli, A., Annoni, P., Azzini, I., Campolongo, F., Ratto, M., & Tarantola, S. (2010). Variance based sensitivity analysis of model output. Design and estimator for the total sensitivity index. *Computer physics communications*, *181*(2), 259-270.

Sakia (1992) Sakia, R. M. (1992). The Box-Cox transformation technique: a review. *Journal of the Royal Statistical Society: Series D (The Statistician)*, *41*(2), 169-178.

Scala et al. (2019) Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119-2126.

Schmittner et al. (2018) Schmittner, C., Griessnig, G., & Ma, Z. (2018). Status of the Development of ISO/SAE 21434. In *Systems, Software and Services Process Improvement: 25th European Conference, EuroSPI 2018, Bilbao, Spain, September 5-7, 2018, Proceedings 25* (pp. 504-513). Springer International Publishing.

Schneider et al. (2019) Schneider, D., Braband, J., Schoitsch, E., Uhrig, S., & Katzenbeisser, S. (2019). Safety and security coengineering in embedded systems. *Security and Communication Networks*, *2019*.

Schneider et al. (2021) Schneider, M., Lichte, D., Witte, D., Gimbel, S., & Brucherseifer, E. (2021). Scenario analysis of threats posed to critical infrastructures by civilian drones. In *Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021)* (pp. 520-527). Research Publishing Services.

Schnieder et al. (2018) Schnieder, L., & Hosse, R. S. (2018). *Guide to automotive cybersecurity engineering*. Springer Fachmedien Wiesbaden.

Schwerdtfeger (2018) Schwerdtfeger, A. (2018). *Design and assessment of a process for the holistic security assessment of mobile access systems*
(Dissertation, Wuppertal University Library).

Shadbolt et al. (2015) Shadbolt, N. R., Smart, P. R., Wilson, J., & Sharples, S. (2015). Knowledge elicitation. *Assessment of human work*, 163-200.

Sharma et al. (2015) Sharma, Anuja, Sarita Sharma, and Meenu Dave. "Identity and access management-a comprehensive study." 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE, 2015.

Sinha et al. (2015) Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X. (2015). From physical security to cybersecurity. *Journal of Cybersecurity*, *1*(1), 19-35.

Sowa (2011) Sowa, A. (2011). *Metrics-the key to successful security and compliance monitoring*. Wiesbaden: Vieweg+ Teubner Verlag.

Spring et al. (2018) Spring, J., Hatleback, E., Manion, A., & Shic, D. (2018). Towards improving CVSS. *Software Engineering Institute, Carnegie Mellon University, Tech. Rep.*

Stephens (1946) Stevens, S. S. (1946). On the theory of scales of measurement.
Science, *103*(2684), 677-680.

Tachtsoglou et al. (2017) Tachtsoglou, S., König, J., Tachtsoglou, S., & König, J. (2017).
Standard normal distribution and z-transformation. *Statistics for Educational Scientists: Concepts, Examples and Applications in SPSS and R*, 111-125.

Teixeira et al. (2015) Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, *51*, 135-148.

Date et al. (2020) Termin, T., Lichte, D., & Wolf, K. D. (2020). Approach to generic multilevel risk assessment of automotive mobile access systems. In *30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM15 2020* (pp. 4611-4618). Research Publishing Services.

Date et al. (2021) Termin, T., Lichte, D., & Wolf, K. D. (2021). Physical security risk analysis for mobile access systems including uncertainty impact. In *Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021)* (pp. 504-511). Research Publishing Services.

Date et al. (2022) Termin, T., Lichte, D., & Wolf, K. D. (2022). An Analytic Approach to Analyze a Defense-in-Depth (DiD) Effect as Proposed in IT Security Assessment. In: *Proceedings of the 32nd European Safety and Reliability Conference* (Dublin, Ireland, 28.08. - 01.09.2022). Edited by Maria Chiara Leva, Edoardo Patelli, Luca

Podofillini, Simon Wilson. ISBN: 978-981-18-5183-4, doi:10.3850/978-981-18-5183-4_R26-01-246-cd.

Torgerson (2007) Torgerson, M. (2007, June). Security metrics for communication systems. In *12th International Command and Control Research and Technology Symposium, Newport, Rhode Island*.

Tsolkas et al. (2017) Tsolkas, A., Schmidt, K., Tsolkas, A., & Schmidt, K. (2017). Access control via authentication. *Roles and authorization concepts: Identity and access management in the enterprise*, 129-160.

Vallverdú (2008) Vallverdú, J. (2008). The false dilemma: Bayesian vs. frequentist. *arXiv preprint arXiv:0804.0486*.

Vernon (2009) Vernon, W. (2009). The Delphi technique: a review. *International Journal of Therapy and rehabilitation*, *16*(2), 69-76.

Virlics (2013) Virlics, A. (2013). Investment decision making and risk. *Procedia Economics and Finance*, *6*, 169-177.

Vogl (2017) Vogl, S. (2017). Quantification. *KZfSS Cologne Journal of Sociology and Social Psychology*, *69*(Suppl 2), 287-312.

Voss (2013) Voß, J. (2013). What actually is data? *LIBREAS. Library Ideas*, (23), 4-11.

Walz (1992) Walz, G. (Ed.). (2013). *Handbook of security technology: perimeter security, access control, intrusion and hold-up detection technology*. Springer-Verlag.

Wang et al. (2010) Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for cyber physical system. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing* (pp. 733-738). IEEE.

Wang et al. (2011) Wang, X., & Williams, M. A. (2011, October). Risk, uncertainty and possible worlds. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (pp. 1278-1283). IEEE.

Wang et al. (2017) Wang, L., Jajodia, S., & Singhal, A. (2017). *Network Security Metrics*. Cham, Switzerland: Springer International Publishing.

Wang et al. (2020) Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, *89*, 101659.

Weber et al. (1999) Weber, J., & Schäffer, U. (1999). *Development of performance measurement systems*. WHU Koblenz.

Wheeler (2011) Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Elsevier.

Willmott et al. (2005) Willmott, C. J., & Matsuura, K. (2005). Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance. *Climate research*, *30*(1), 79-82.

Witte (2018) Witte, F. (2018). *Metrics for Test Reporting: Analysis and Reporting for Effective Test Management*. Springer-Verlag.

Witte et al. (2020) Witte, D., Lichte, D., & Wolf, K. D. (2020). Threat Analysis: Scenarios and Their Likelihoods. In *30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM15 2020* (pp. 4589-4595).

Woit (2011)	Woit, P. (2011). *Not even wrong: The failure of string theory and the continuing challenge to unify the laws of physics*. Random House.
Woods et al. (2021)	Woods, D. W., & Böhme, R. (2021, May). SoK: Quantifying cyber risk. In *2021 IEEE Symposium on Security and Privacy (SP)* (pp. 211-228). IEEE.
Wu et al. (2017)	Wu, J., Zhou, R., Xu, S., & Wu, Z. (2017). Probabilistic analysis of natural gas pipeline network accident based on Bayesian network. *Journal of Loss Prevention in the Process Industries*, *46*, 126-136.
Worm (2022)	Wurm, M. (2022). *Automotive Cybersecurity: Security Building Blocks for Automotive Embedded Systems*. Springer Berlin/Heidelberg.
Xie et al. (2010)	Xie, P., Li, J. H., Ou, X., Liu, P., & Levy, R. (2010, June). Using Bayesian networks for cyber security analysis. In *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)* (pp. 211-220). IEEE.
Yee (2013)	Yee, G. O. (2013). Security metrics: An introduction and literature review. *Computer and Information Security Handbook*, 553-566.
Zio (2007)	Zio, E. (2007). *An introduction to the basics of reliability and risk analysis* (Vol. 13). World scientific.

7.2 Online Sources

Reference in the text	Source reference
5Star (2021)	5StarProjects (2021). https://5starsproject.com/, accessed on 16.07.2021.
Airbnb (2021)	Airbnb (2021). https://www.airbnb.com/, accessed on 07.12.2021.
Autosec.se (2016)	Autosec (2016). *Security models*. https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf, accessed on 25.04.2022.
Azure (2021)	Micrososft Azure (2021). https://azure.microsoft.com/de-de/services/key-vault/, accessed on 11.11.2021.
Bayesian merger (2021)	Bayesfusion (2021). *GeNIe Modeler User Manual*. https://support.bayesfusion.com/docs/GeNIe.pdf, accessed on 12.08.2021.
Bayesia.com (2021)	Bayesia (2021). *Bayesia Expert Knowledge Elicitation Environment (BEKEE)*. https://library.bayesia.com/articles/#!bayesialab-knowledge-hub/bayesia-expert-knowledge-elicitation-environment-bekee, accessed on 01.12.2021.
BayesiaLab (2012)	BayesiaLab (2012, August 29). *Introduction to BEKEE, the Bayesia Expert Knowledge Elicitation Environment*. https://www.youtube.com/watch?v=6SkdFIR8FAA&t=2470s, accessed on 01.12.2021.
BHE (2021)	BHE (2021). *Perimeter security*. https://www.bhe.de/publikationen/konzepte-and-broschueren/freigelaendeueberwachung, accessed on 16.07.2021
BKA.de (2021)	BKA (2021). *Motor vehicle crime*. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Kfz-Kriminalitaet/kfz-kriminalitaet_node.html, accessed on 31.08.2021.
BMWi (2021)	BMWi (2021). *The German Gaia-X Hub*.

https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html, 08.07-2021, accessed on 16.07.2021.

Brownlee (2020)
Brownlee (2020, June 10). *How to Use StandardScaler and MinMaxScaler Transforms in Python.* https://machinelearningmastery.com/standardscaler-and-minmaxscaler-transforms-in-python/, accessed 21.03.2021.

BSI (2016)
BSI-Bund (2016). *Cyber security as a competitive advantage in digitalization.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.html, accessed on 12.09.2021.

BSI industry situation (2022)
BSI-Bund (2022, September 19). *Automotive sector situation report 2022.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.pdf?__blob=publicationFile&v=8, accessed on 20.09.2022.

BSI Glossary (2022)
BSI-Bund (2022). *Zero-day exploit.* https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html, accessed on 12.09.2022.

CC (2022)
CC (2022). *The Common Criteria.* https://www.commoncriteriaportal.org/, accessed 18.06.2022.

Cert (2022)
Marty (2021, April 1). *UNECE WP.29 / R155 - How cyber security will impact the automotive market from June 2022.* https://certx.com/de/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/, accessed on 10.05.2022.

Charter Global (2020)
Charter Global (2020, November 20). *Understanding physical security standards.* https://www.charter-global.com/physical-security-standards/, accessed on 21.10.2021.

Chester (2021)
Chester, J. (2021, October 21). *A closer look at CVSS scores.* https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/, accessed on 10.05.2022.

Cimpanu (2020)
Cimpanu, C. (2020, May 18). *Mercedes-Benz onboard logic unit (OLU) source code leaks online.* https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/, accessed on 01.09.2021

CVE (2021)
CVE (2021). CVE. https://cve.mitre.org/, accessed on 16.07.2021.

CVSS Work Items (2022)
CVSS v4.0 Work Items (2022). https://docs.google.com/document/d/1qmmk9TQulW9d1cuipu_ziXDX0pUs-wbZ1WSQyynHbvKU/edit#, accessed on 11.05.2022.

Eddie (2021)
Eddie (2021, March 18). *Feature Scaling Techniques in Python - A Complete Guide.* Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/05/feature-scaling-techniques-in-python-a-complete-guide/, accessed on 21.03.2021.

Electronics compendium (2021)
Electronics Compendium (2020, November). *Client-server architecture.* https://www.elektronik-kompendium.de/sites/net/2101151.htm, accessed on 02.012.2021.

Embitel (2018)
Embitel (2018). *Understanding How ISO 26262 ASIL is Determined for Automotive Applications.* https://www.embitel.com/blog/embedded-blog/understanding-how-iso-26262-asil-is-determined-for-automotive-applications, accessed on 18.06.2022.

ENISA (2021)
ENISA (2021, October 27). *ENISA Threat Landscape 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, accessed on 27.06.2022.

EPSS (2021)
First.org (2021). *Exploit Prediction Scoring System.* https://www.first.org/epss/, accessed on 11.05.2022.

Euro NCAP (2021)
Euro NCAP (2021). https://www.euroncap.com/de, accessed on 16.07.2021.

EVITA (2022)
EVITA (2022). https://www.evita-project.org/objectives.html, accessed on 27.06.2022.

FAIR (2021)
FAIR Institute (2021). *The Standard Quantitative Model for Information Security and Operational Risk.* https://www.fairinstitute.org/, accessed on 16.07.2021.

First.org (2022)
FIRST SIG (2019, March 12). *FIRST is the global Forum of Incident Response and Security Teams.* https://www.first.org/, accessed 16.01.2022.

flaticon.com (2021)
Flaticon (2021). *Access 9.7M+ vector icons & stickers.* https://www.flaticon.com/, accessed on 08.10.2021.

Flinkey.de (2021)
WITTE Automotive (2021). *Digital vehicle access.* https://www.flinkey.com/, accessed on 08.10.2021.

Gabler (2021)
Lackes, R. (2021). *Expert knowledge.* https://wirtschaftslexikon.gabler.de/definition/expertenwissen-34831, accessed on 21.12.2021.

Gabler (2022)
Bendel, O. (2021). *Cyberecurity.* https://wirtschaftslexikon.gabler.de/definition/cybersecurity-99856, accessed on 31.05.2022.

Violinist (2021)
Geiger, M. (2021). *Safety vs. security: The difference explained simply (and how you can combine both goals).* https://www.sichere-industrie.de/safety-security-unterschied-erklaert-kombination-ziele-industrial-security/, accessed on: 05.05.2020.

Gulp (2022)
Feralisch, J. (2022, December 09). *Junior vs. senior: Experience makes the difference.* https://www.gulp.de/knowledge-base/18/ii/auswertung-junior-oder-senior-die-erfahrung-macht-den-unterschied.html, accessed on 21.12.2022.

Hafi.de (2015)
HAFI (2015, January). *Amok prevention.* https://hafi.de/wp-content/uploads/2019/04/hafi-protect_20190503.pdf, accessed on 28.01.2021.

Harris (2021)
Harris, A. (2021) *Comparison of "peer-to-peer" vs "client-server" Network Models.* https://www.networkstraining.com/peer-to-peer-vs-client-server-network/, accessed on 02.12.2021.

Harnser (2010)
Harnser Group for the European Commission (2010, Summer). *A Reference Security Management Plan for Energy Infrastructure.* https://www.ab.gov.tr/files/ardb/evt/Reference_Security_Management_Plan_for_Energy_Infrastructure_2010.pdf.

InCommon (2013)
InCommon (2013, February 11). *Identity Assurance Profiles Bronze and Silver.* https://incommon.org/wp-content/uploads/2019/04/IAP.pdf, accessed on 04.02.2021.

ISF Munich (2021)
ISF Munich (2021, June 8). *Research Report Upheaval in the Automotive Industry.*

https://www.isf-muenchen.de/wp-content/uploads/2021/06/Forschungsreport-Umbruch-in-der-Automobilindustrie.pdf,
accessed on 30.12.2021.

Kantara (2021)

Kantara (2021). *Identity Assurance.* https://kantarainitiative.org/idassurance/, accessed on 16.07.2021.

KBA (2021)

KBA (2021). *Type approval granted.*
https://www.kba.de/DE/Themen/Typgenehmigung/Typgenehmigungserteilung/typgenehmigungserteilung_node.html, accessed on 02.10.2021.

MaaS Alliance (2022)

MaaS Alliance (2022, October). *Mobility Data Spaces and MaaS.* https://maas-alliance.eu/wp-content/uploads/2022/10/MaaS-Alliance-Whitepaper-on-Mobility-Data-Spaces-1.pdf, accessed 10.10.2022.

MDS (2022)

MDS (2021). *Data Sharing Community.*
https://mobility-dataspace.eu/de, accessed on 24.05.2022.

MEI (2021)

Microsoft (2021). *The Microsoft Exploitability Index.*
https://www.microsoft.com/en-us/msrc/exploitability-index,
accessed on 11.05.2022.

NIST (2010)

NIST (2010). *Interagency Report 7628 Guidelines for Smart Grid Cyber Security.*
https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf,
accessed on 16.02.2022.

NIST (2021)

NIST (2021). *National Vulnerability Database.* https://nvd.nist.gov/, accessed on 16.07.2021.

NIST CVSS (2022)

NIST (2022).
Common Vulnerability Scoring Calculator.
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, accessed on 10.08.2022.

NIST Vulntology (2021)

NIST (2021).
https://github.com/usnistgov/vulntology, accessed on 11.05.2022.

Pohlmann (2015)

Pohlmann, N. (2015). *Effect of IT security measures - The new challenge.* https://norbert-pohlmann.com/app/uploads/2015/08/285-Wirkung-von-IT-Sicherheitsma%C3%9Fnahmen-%E2%80%93-die-neue-Herausforderung-Prof-Norbert-Pohlmann.pdf, accessed on 16.11.2021.

Pohlmann (2021)

Pohlmann, N. (2021). *Authentication.* https://norbert-pohlmann.com/glossar-cyber-sicherheit/authentifikation/, accessed on 16.07.2021.

RAND (2021)

RAND (2021). *Delphi Method.*
https://www.rand.org/topics/delphi-method.html, accessed on 29.11.2021.

RCAR (2021)

RCAR (2021). https://www.rcar.org/, accessed on 16.07.2021.

Red Hat (2021)

Red Hat (2021). *Understanding Red Hat security ratings.*
https://access.redhat.com/security/updates/classification,
accessed on 11.05.2022.

Risk-based security (2017)

Risk-based Security (2021, January 05). *CVSS v3 Newer is better right.*
https://www.riskbasedsecurity.com/2017/01/05/cvssv3-newer-is-better-right/,
accessed on 11.05.2022.

Samcurry.net (2023)

Curry, S. (2023, January 3). Web Hackers vs. *The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More.*
https://samcurry.net/web-hackers-vs-the-auto-industry/,
accessed on 04.01.2023.

Schneider (1999)

Schneider, B. (1999, December). *Attack Trees.*

	https://www.schneier.com/academic/archives/1999/12/attack_trees.html, accessed on 12.07.2022.
Security systems (2021)	Institute for Security Systems (2021). *Establishment of new technical committee in the VDI: Synthesis of safety and security.* http://www.sicherungssysteme.net/de/aktuell/fachausschussimvdi.html, accessed on 21.10.2021.
Sifo.de (2023)	SIFO (2023). https://www.sifo.de/sifo/de/home/home_node.html, accessed on 02.01.2023.
SoQrates (2022)	SoQrates (2022). *SoQrates software offensive Bavaria.* https://soqrates.eurospi.net/index.php, accessed on 11.05.2022.
SSVC (2021)	CERTCC (2021). *SSVC.* https://github.com/CERTCC/SSVC, accessed on 11.05.2022.
Statista (2011)	Statista (2011, April). *Forecast on the number of networked devices worldwide.* https://de.statista.com/statistik/daten/studie/479023/umfrage/prognose-zur-anzahl-der-vernetzten-geraete-weltweit/, accessed on 12.08.2021.
SUSRS (2021)	Microsoft (2021). *Security Update Severity Rating System.* https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system, accessed on 11.05.2022.
Thatcham (2021)	Thatcham (2021). *Thatcham Security Certification.* https://www.thatcham.org/what-we-do/security-certification/, accessed on 16.07.2021.
Tony O'Hagan (2021)	O'Hagan, T. (2021). *The Sheffield Elicitation Framework (SHELF).* http://www.tonyohagan.co.uk/shelf/, accessed on 29.11.2021.
TÜV (2021)	TÜV (2021). *TÜVRheinland.* https://www.tuv.com/germany/de/, accessed on 16.07.2021.
Uber (2021)	Uber (2021). *Uber - Get in the driver's seat and get paid.* https://www.uber.com/de/en/, accessed on 07.12.2021.
VDA (2022)	Perl, A. (2022). *The NCAP program.* https://www.vda.de/de/themen/automobilindustrie/standards-und-normung/euro-ncap-anforderungen, accessed on 07.07.2022.
Williams (2022)	Williams, J. (2022). *OWASP Risk Rating Mythodology.* https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, accessed on 09.05.2022.

7.3 Guidelines and Standards

Reference in the text	Source reference
47 CFR Part 15.247	U.S. Government Publishing Office (2010, October 1). 47 CFR Part 15.247. *Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz.* https://www.govinfo.gov/app/details/CFR-2010-title47-vol1/summary, accessed February 25, 2021.
BSI (2020)	BSI (2020, December 17). *IT-Grundschutz Compendium (2021 edition).* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, accessed on 12.11.2021.
CCC (2021)	Car Connectivity Consortium (CCC) (2021). https://carconnectivity.org/, accessed on 16.07.2021.
DIN e.V. (2018)	DIN e.V. (2018, August). DIN pocket book 408: *Information security management.* BEUTH-Verlag.
DIN EN 1627	DIN e.V. (2021a). DIN EN 1627:2021-11 *Doors, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification; German and English version prEN 1627:2019.* https://www.beuth.de/de/norm-entwurf/din-en-1627/299758611, accessed on 16.07.2021.
DIN EN 1628	DIN e.V. (2021b). DIN EN 1628:2021-11. *doors, windows, curtain walling, grilles and shutters - Burglar resistance - Test method for the determination of resistance under static loading; German and English version prEN 1628:2019.* https://www.beuth.de/de/norm-entwurf/din-en-1628/299762309, accessed on 16.07.2021.
DIN EN 61508	DIN e.V. (2011). DIN EN 61508-1:2011-02; VDE 0803-1:2011-02. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:2010); German version EN 61508-1:2010.* https://www.beuth.de/de/norm/din-en-61508-1/135302584, accessed 17.12.2021.
DIN EN ISO 9000	DIN e.V. (2015a). DIN EN ISO 9000:2015-11. *Quality management systems - Fundamentals and terminology (ISO 9000:2015); German and English version EN ISO 9000:2015.* https://www.beuth.de/de/norm/din-en-iso-9000/235671064, accessed 13.12.2021.
DIN EN ISO 9001	DIN e.V. (2015b). DIN EN ISO 9001:2015-11 *Quality management systems - Requirements (ISO 9001:2015); German and English version EN ISO 9001:2015.* https://www.beuth.de/de/norm/din-en-iso-9001/235671251, accessed on 25.02.2021.
DIN ISO/TR 22100	DIN e.V. (2014). DIN ISO/TR 22100-2:2014-09 Safety of machinery - Relationship to ISO 12100. https://www.beuth.de/de/technische-regel/din-iso-tr-22100-1/252378999, accessed on 22.10.2021.
DIN SPEC 27070	DIN e.V. (2020). DIN SPEC 27070:2020-03. *Requirements and reference architecture of a security gateway for the exchange of industry data and services.* https://www.beuth.de/en/technical-rule/din-spec-27070/319111044, accessed on 10.05.2022.
GDPR (2021)	European Union (2018, May 25). *General Data Protection Regulation (GDPR).* https://dsgvo-gesetz.de/, accessed on 16.07.2021.

IATF 16949

IATF (2016). IATF 16949:2016-10. *Requirements for quality management systems for series and spare parts production in the automotive industry.* https://www.beuth.de/de/technische-regel/iatf-16949/263942493, accessed 25.02.2021.

IDSA (2016)

IDSA (2016). *International Data Spaces Standard (IDS).* https://internationaldataspaces.org/, accessed on 16.07.2021.

IEC 61508

IEC (2010). IEC 61508-1:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (see Functional Safety and IEC 61508).* https://www.vde-verlag.de/iec-normen/217178/iec-61508-2-2010.html, accessed 22.10.2021.

IEC 62368

IEC (2021). DIN EN IEC 62368-1:2021-05. *audio/video, information and communication technology equipment - Part 1: Safety requirements (IEC 62368-1:2018); German version EN IEC 62368-1:2020 + A11:2020.* https://www.beuth.de/de/norm/din-en-iec-62368-1/336074670, accessed on 22.10.2022.

IEC TR 63069

IEC (2019). IEC TR 63069: 2019. *Industrial-process measurement, control and automation - Framework for functional safety and security.* https://www.vde-verlag.de/iec-normen/247681/iec-tr-63069-2019.html, accessed on 22.10.2021.

ISO 21434 (free)

ISO/SAE (2021a). ISO/SAE 21434:2021. *Road vehicles - Cybersecurity engineering.* https://www.iso.org/obp/ui/#iso:std:iso-sae:21434:ed-1:v1:en, accessed on 25.04.2022.

ISO 26262

ISO (2018). ISO 26262-1:2018 - ISO 26262-10:2018 *Road vehicles - Functional safety.* https://www.beuth.de/de/erweiterte-suche/272754!search?alx.searchType=complex&alx.autoSuggest=true&searchAreaId=1&query=ISO+26262-1+&facets%5B276612%5D=&hitsPerPage=10, accessed on 17.12.2021.

ISO/PAS 5112

ISO (2022). ISO/PAS 5112:2022 *Road vehicles - Guidelines for auditing cybersecurity engineering.* https://www.iso.org/standard/80840.html, accessed on 10.05.2022.

OSS Association (2021)

OSS Association (2021). *Standard Offline by OSS Application.* https://www.oss-association.com/standards/oss-standard-offline/, accessed on 23.09.2021.

RSS 247

Government of Canada (2017, February). RSS 247 *Digital Transmission Systems (DTSs), Frequency Hopping Systems (FHSs) and License-Exempt Local Area Network (LE-LAN) Devices.* https://ised-isde.canada.ca/site/spectrum-management-telecommunications/en/devices-and-equipment/radio-equipment-standards/radio-standards-specifications-rss/rss-247-digital-transmission-systems-dtss-frequency-hopping-systems-fhss-and-licence-exempt-local, accessed on 21.03.2021.

SAE (2021)

SAE (2021). SAE J3061-12:2021 *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* https://www.sae.org/standards/content/j3061_202112, accessed on 25.04.2022.

ISO/SAE (2021b)

ISO/SAE (2021b). ISO/SAE 21434:2021-08. *Road Vehicles - Cybersecurity Engineering.* https://www.sae.org/standards/content/iso/sae21434, accessed 25.04.2022.

SPICE (2015) Automotive SIG (2015, July 16). *Automotive SPICE Process Assessment / Reference Model.*
https://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf, accessed on 25.04.2022.

UNECE R 155 UNECE (2021, January 22). *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.*
https://unece.org/sites/default/files/2021-03/R155e.pdf,
accessed on 25.04.2022.

VDA (2020) VDA (2020). ACSMS:2020-12. *ACSMS 2020_GERMAN.*
https://webshop.vda.de/QMC/de/acsms-de_2020, called on 25.04.2022.

8 Attachments

8.1 Discussion of the Problem

> We are moving into a world in which assets are primarily digital and not physical. [...] Digital assets are increasingly subject to cyber risks. [...] Cyber-attacks can [...] result in huge or even catastrophic losses for two reasons: (i) correlated risk and (ii) interdependent risk.
> (Gandal et al., 2020, p. 5).

A central problem in the risk assessment of mobile access systems (MAS) is the cross-domain assessment of physical security and IT security in specific use cases using a suitable metric. Ideally, this metric should be able to dock onto the physical domain and the IT domain and link the physical scenario with the IT scenario so that interactions can be identified and assessed. A model that would quantitatively depict cause-and-effect relationships could illuminate the effect of measures in the network, so that cost-benefit optimization would be possible in a quantitative way. However, it must be possible to correctly map security measures in the cyber-physical network by means of a suitable assessment in order to enable a cross-domain security assessment independent of generic threat scenarios. The question arises as to how the principles from both domains can be brought together so that a cross-domain assessment for security can contribute to making MAS (more) secure as early as the development process.

Wang et al. (2017) state that there is a lack of effective (i.e. objective, effectiveness-based) security metrics that can be used to (quantitatively) assess attacks on networks: "One of the most pertinent issues in securing mission-critical [...] networks against security attacks is the lack of effective security metrics" (Wang et al., 2017, Preface). This statement is justified by the fact that existing metrics, such as CVSS (First.org, 2022), refer to the measurement of an individual and usually known vulnerability, but the interaction of a vulnerability with other vulnerabilities (of other system units) must be found out by administrators (Wang et al., 2017, p. 3). Several reasons are given as to why developing an effective metric in IT security is difficult (Wang et al., 2017, pp. vii, viii, 2, 54, 65):

- In addition to known vulnerabilities and attacks, scenarios that have not yet occurred must also be assessed.
- More and more new security vulnerabilities are published every week, which administrators have to take into account. This raises the question: How does the risk manager deal with new information?
- Attackers sometimes carry out complex, multi-step attacks.
- Current detection methods cannot cope with the complexity of attacks.
- It must be possible to assess security consistently in order to compare and weigh up risks and to justify the introduction of mitigation measures, which are subject to scarce resources.
- There are sometimes major uncertainties in the assessment of individual risk contributions. This raises the question: How does the risk manager deal with major uncertainties?

Cheng et al. (2014, p. 8) list further challenges:

- Lack of a "real-time response" to attacks.
- Lack of understanding of the impact of events on operations.
- Lack of quantitative metrics and measures for a comprehensive security assessment.
- Lack of integration of human (analytical) insights into cyber-physical situational awareness.

Wang et al. (2017, pp. 2, 6) explain that composing metrics into a global measure is not trivial and simple. The consequence of a "naïve" composition can lead to misleading results, as

- different metrics are not necessarily consistently structured and compatible, because something different may be assessed at the core.
- should not be calculated with scores. This is due to the lack of an absolute size reference.
- fewer vulnerabilities does not mean more secure.
- business-relevant resources can be compromised with seemingly non-critical vulnerabilities. There are interactions between units.
- the exploitation of one or more vulnerabilities may be accompanied by the compromise of (further) business-relevant resources only after some time.
- it is not immediately obvious which causes can lead to a certain consequence. Depending on the use case, the systems to be assessed are different in terms of their design and inherent structures.
- the reference to the hardware is often ignored.

The consideration of cybersecurity in addition to physical security brings with it the following four challenges:

> "1. long-term historical data do not exist.
> 2. there are adversaries creating the dangers, and these adversaries behave strategically.
> 3. there is interdependent security and correlated risks.
> 4. cyberattacks can go undetected for long periods of time" (Gandal et al., 2020, p. 7).

In order to implement security measures in a targeted manner, the interaction between the components of a network must first and foremost be understood (Wang et al., 2017, p. 2). This is a challenge that must be met not only in the context of a domain-specific view, but also in the course of a cross-domain view of physical security and IT security or safety and physical security or IT security. In safety, requirements for the system that must be fulfilled in order to achieve the corresponding SIL are traditionally defined by specifying Safety Integrity Levels (SIL), for example.

Due to the increasing use of IT in safety-relevant application areas, however, according to the considerations in Lyu et al. (2020), IT security requirements must also be taken into account in system design in addition to safety requirements, as safety functions can be compromised by exploited IT vulnerabilities. System operators face challenges with regard to the quantitative verification of failure rates in the combination of safety and IT security, because threats and vulnerability cannot really be quantified in IT security. The requirements for safety and physical security or IT security can also be contradictory. In addition, there are different nomenclatures and assessment frameworks that make it difficult to bring them together (Macher et al., 2020a). The question arises as to the metric for assessing such a system, which combines security features from several domains. A key difficulty lies in defining a corresponding IT security level for, for example, "safety integrity level three" from safety or vice versa. In particular, it must be possible to record and assess interfaces between system units and interactions. Assessments are typically conducted using models (Bandow & Holzmüller, 2009, p. vii). On the one hand, there are assumptions and, on the other, metrics on which the assessments are based. If an assessment is to be conducted for safety or physical security and IT security in combination, for example, the following questions arise for the risk manager:

- How can properties, technological artifacts and measures be mapped in a model?
- Which assessment metrics can be used specifically to assess the interactions between safety, physical security and IT security?

- How can uncertainties be taken into account and how can expert knowledge be integrated?
- How can comparability be created, e.g. to achieve coordinated risk levels?

Wang et al. (2017, p. 2) warn that the naive combination of, for example, safety (with models and metrics from safety), physical security (with models and metrics from physical security) and IT security (with models and metrics from IT) in a cross-domain assessment does not make sense. Performance-based assessment metrics for the cross-domain assessment of safety and IT security or physical security and IT security are difficult to find, as shown in the state of guidelines and standards. A classic approach to designing systems taking uncertainties into account is to assume worst cases and set security margins (Harnser, 2010, B3, p. 2; First.org, 2022). However, too much security can become uneconomical. "Products with excessive security measures are too expensive for this industry and therefore not competitive", states Wurm (2022, p. 37). Too little security, on the other hand, would be negligent. This raises the question of a good cost-benefit ratio and justifying the investment to the company's management. However, adding security margins is only practicable as long as a risk manager does not have to compare risks. Ideally, risks must be quantified in order to be able to compare risks. The challenge lies in the fact that the domains do not have the same prerequisites for this:

In semi-quantitative approaches such as those used in IT security assessment, e.g. the Common Vulnerability Scoring System (CVSS, First.org, 2022) or OWASP Risk Assessment (OWASP, 2022), there is no metric at any point in the assessment process that states how assessment variables are measured. If a risk analyst asks an expert about a vulnerability contribution and then receives a semi-quantitative assessment between "zero" (minimum) and "ten" (maximum), there is no assignment of these scores to a specific size reference. After the assessment, there is merely a "sequence of numbers". It is therefore a monotonic function, i.e. if the input variables are large, then the output variables are also large. This type of assignment is the case, for example, with the DuPont scheme according to Harnser (2010) - the Harnser metric (see chapter 2.5). However, this cannot be used to establish a quantitative correlation that indicates, for example, that a score of "three" is twice as bad as a score of "four". Consequently, these semi-quantitative values cannot really be used in calculations, as there is no quantitative metric with an objective mechanism of performance to describe the protective effect in terms of vulnerability reduction. However, this is often done in common practice, as explained in Krisper (2021).

If a metric is now stored with the scores, e.g. centimeters, then an expert has a comparative measure with which to calculate. In this respect, a metric such as that used in physical security based on time (see the vulnerability model in chapter 2.5) is not available in IT security, the scores cannot simply be used for calculations. This is because arithmetic operations cannot be reasonably applied to scores. In IT security, there is no objective mechanism for describing the IT protection effect. IT scoring, e.g. CVSS (First.org, 2022), only ensures that one number is greater than, equal to or less than another number. Furthermore, if two experts independently assess a system, they must agree on what a specific score value means. If an underlying metric is available, then quantification is possible, even taking uncertainties into account (e.g. Lichte et al. (2016)). However, this requirement is not met in IT security (Schneider et al., 2019; see also Chapter 2.5).

The question also arises as to how effective IT measures are. This in turn raises the question of which mechanisms can be used to measure effectiveness in IT security. In physical security, this is clearly defined via a delay and detection time, so that a risk analyst can say what the probability of vulnerability is over a certain time base, which is available as an intervention. The probability of vulnerability therefore means precisely that the residual overcoming time is less than the intervention, as illustrated by the vulnerability model according to Lichte et al. (2016). This is a very clear definition of vulnerability or a successful attack in terms of a metric. A risk analyst in IT does not have this prerequisite because they cannot calculate correctly with makeshift numerical values - scores (Braband, 2019). What can a consistent assessment basis for the assessment of CPS look like? The state of research on cyber-physical security (see chapter 2.2) will show a clear need for action here.

For this research work, the question must be asked: Can this mapping be done for both domains in any way, if so, what are the requirements? The mapping of interactions is not arbitrarily complex via a metric, therefore only estimations are made in practice (Wang et al., 2017). In this context, assumptions can be used for simplification (Lichte et al., 2019). For example, the existence of disjunctive events could mean that the threat is completely excluded from the considerations because it is particularly difficult to quantify. Vulnerabilities are therefore only considered if it is assumed that impacts can be quantified. In this case, an assessment would be accessible and in principle presentable. However, there is a problem here: in IT security, there is no reasonable description of the (temporal) process in relation to vulnerability. Therefore, a quantitative metric for the physical vulnerability assessment cannot really be docked to the IT attack process.

The comparison of the assessment of, for example, triple DES (Data Encryption Standard, 3DES) and DES (Paar & Pelzl, 2016, pp. 72, 78) clearly shows the challenge: How much longer does the attacker need to overcome DES or 3DES? If a risk analyst had this basis, then a quantitative metric could be generated to compare one risk with the other. A risk analyst does not have this, as shown by the example of linking vulnerability shares and impact shares in CVSS (First.org, 2022). CVSS generates figures, but categories have to be written above them. These numbers are even used to operate, as described above. This should not be done, as there is no concrete reference point. This is essentially a problem that must be dealt with in the consistent assessment of CPS. A key question is therefore: How can this be resolved? An illustrative example of this problem is the conflict of objectives between safety and security for a door: safety means "a person is out quickly enough", whereas security means that an attacker is stopped long enough before they reach a system function worth protecting, also known as an asset[80] , for example. An expert can now use the vulnerability assessment according to Lichte et al. (2016) to determine overcoming times for the physical barriers. This provides a metric that can be used to quantify vulnerability. It must also be possible to map interactions. However, the consideration of interactions by means of a quantitative metric does not exist either in the physical security assessment or in the IT security assessment. The question arises as to how physical security and IT security can be correctly assessed together in a consistent approach. There are still different scenarios when two security domains are considered.

Assuming there are no interactions to begin with. Nevertheless, it must be possible to coordinate security levels for physical security and IT security so that a system provider can say: If, for example, IT security level "three" is given, then the same form of physical security is required, i.e. also level "three". This is necessary so that the vulnerability in physical security does not negate the design in IT security, and vice versa. An IT attack path, for example, should be secured with the same level of security from a physical perspective. This raises the question: How can the same level of security be defined and achieved in both domains? If an operator specifies that security level "four" is required, then the experts from physical security and the experts from IT security can ask: How can the security level of IT security be brought together

[80] An asset is something of special value that should be protected against misuse by appropriate security measures.

with physical security in a reasonable and consistent manner? What kind of approach could be used to align security levels with each other?

If the previous door example (conflicting goals of safety and security) is considered, then this is logical: the longer an attacker needs to overcome the door, the better it is for security if it only has the property of overcoming time, and the worse it is for safety at the same time. However, doors can also have other properties. Modern doors in educational institutions, for example, make it easy to leave a room via the door if someone wants to go outside. However, it is then more difficult to enter than to leave (Hafi.de, 2015). This peculiarity cannot yet be mapped in a metric. If there is no consistent metric for assessing CPS security due to incompatible assessment approaches, the two domains cannot be easily linked. The question now is how this can be resolved so that any interactions that may exist can be mapped. On the other hand, an operator wants to achieve coherent security levels. If, assuming a consistent metric, there is a security level of "two" in the physical domain, for example, then a risk analyst only has to show that the risk reduction in the IT domain is at the same level, provided there are no dedicated interactions between these domains.

If, ideally, completely separate attack paths are considered, then there are no interactions at all. This means that there is only the possibility of accessing an asset via physical security or via the possibilities in IT, but nothing that is now combined. In reality, the existence of interactions must be assessed by experts. It would therefore make sense to assess IT security and physical security simultaneously and consistently. The individual assessments and cyber-physical links must then be brought together to form a consistent whole. Ideally, this requires a metric that can be used to compare risk levels or vulnerability levels on a one-to-one basis, e.g. based on the effectiveness of measures. If a risk analyst continues to ask experts how an IT measure affects the physical risk or how a physical measure affects the IT risk, they cannot arrive at a consistent overall result without having an underlying, quantitative metric. Within a metric or domain, however, this is possible subject to restrictions as formulated in Wang et al. (2017, pp. 2, 6). Any complex metric constructs or models can be built, but it must be answered how both domains can be brought together in the core. In short, bringing them together causes problems (see chapter 2.2). The objective would be to achieve equivalent resilience in the other domain on the basis of risk reduction in one domain so that, for example, the vulnerability determined is accepted by the operator.

On the one side are IT processes, on the other are physical processes. The processes in the IT domain and the processes in the physical domain must come to similar risk assessments, and therefore to similar risk metrics. This means, for example, that very serious, moderately serious and minor cases have roughly the same assessment. This also makes it possible to prioritize risks. Because MAS can be categorized as CPS, there is a physical security level and an IT security level that must be taken into account in a risk analysis. If the metrics in the physical domain and in the IT domain were to describe the same physical processes, then this would be the natural level at which the physical metrics and IT metrics are brought together. This means that if the physical security metric describes how likely a door is to be closed, for example, and the safety metric describes how likely this door must be open, then these two metrics can be brought together based on the physical conditions because there is a reference to these physical conditions.

To make matters worse, there is no single metric or parameter link or model that is used in the same way by all risk managers in every field of application, neither in physical security nor in IT security (see chapter 2.5). Consequently, there is also the challenge of finding a suitable model - where possible - and a suitable metric or combination of metrics that can make it possible to map interactions in such a way that, for example, the effect of measures on vulnerability can be reflected. A legitimate question is how the problem of cross-domain vulnerability assessment of physical security and IT security for CPS can be resolved at a metric level in order to create sound decision-making support in the form of a risk assessment process on the basis of which risks, e.g. in the case of MAS for vehicles, can be assessed and weighed up against each other.

8.2 Paradigms in Physical and IT Security

8.2.1 Structure and Properties of the IT Layer

According to the Gabler Business Dictionary, IT security can be defined as follows:

> Cybersecurity or IT security is the protection of networks, computer systems, cyber-physical systems and robots against theft or damage to their hardware and software or the data they process, as well as against interruption or misuse of the services and functions they offer. The data is both personal and operational (which in turn may be personal). (Gabler, 2022).[81]

Data plays a key role in the functionality and security of a system (Wheeler, 2011, p. 8; BSI-Bund, 2021). They are individual observable, measurable elements that, when strung together, constitute information (Voss, 2013). Information is stored in binary units, i.e. zeros and ones, in machine-readable form on physical hardware (Anderson, 2001, p. 365) and can be represented in alphanumeric characters, letters, digits and symbols. These can be read and interpreted by humans. Data allows for analysis, synthesis, separation, assessment, storage, processing and transmission (Bodendorf, 2016, pp. 1-6). They are transferred between at least two actors via a physical or wireless channel. On the one hand, this requires suitable interfaces on both sides, and on the other hand, both parties must agree on the rules according to which they exchange which data and when (Paar & Pelzl, 2016, p. 5). Protocols are necessary for this (Anderson, 2001, p. 63). To ensure that unauthorized persons cannot intercept and read messages, messages are encrypted using cryptographic techniques (Paar & Pelzl, 2016, p. 4). Ideally, the secret for decryption is known to both parties and must be protected against misuse (Paar & Pelzl, 2016, pp. 6-7). Signatures are used, for example, to prove the accuracy of one's own identity to the other party (Paar & Pelzl, 2016, pp. 335-338, 392-395). This is necessary to ensure trust in the course of communication.

Data forms the basis of identity and access management (IAM) and associated services (Indu et al., 2018). It is received and processed by cyber-physical products, such as mobile access systems (MAS), and transferred into a physical action, e.g. locking or unlocking a vehicle by operating a locking mechanism (Flinkey.de, 2021). Data is accessed via wireless or wired interfaces. These must also be protected against unauthorized access (Ashibani & Mahmoud, 2017). Convenience flaps are implemented in the product barriers to protect the data so that authorized persons can gain access to functions for using data. A user must authenticate themselves at these convenience flaps with their credentials (Tsolkas et al., 2017, pp. 129-160). Credentials can be knowledge, possession or characteristics (Pohlmann, 2021). If authentication is successful, access is granted, otherwise not. In addition, "guards" are implemented that can observe the behavior of users and function calls and detect anomalies (König, 2005; Kofler et al., 2018, pp. 37-38). These are firewalls or anti-malware programs, for example.

In IT, a range of data is usually logged (Sowa, 2011, p. 3). This is basically observation. If an operator has forgotten not to log something, then activities relating to these unrecorded data points are also not observed. Monitoring, in turn, represents the derivation of action and is therefore detection. After successful detection, an alarm can be triggered, which can usually only be viewed by a higher-level instance, e.g. an administrator. Automated approaches and normalized log data can be used so that recorded data from IT systems can be compared (Sowa, 2011, p. 5). Once anomalies have been detected, automated and/or human-initiated intervention measures are taken, such as blocking a user account to prevent potential misuse

[81] As can be seen from the definition, the terms cyber security and IT security are equated.

of sensitive (business-relevant) data, for example (Wheeler, 2011, p. 155). Attacks are traditionally followed by a feedback process in the sense of knowledge management, i.e. lessons are learned from the attack and the knowledge gained from the analysis and assessment is incorporated into the optimization of the design of security measures (Ritz, 2015, pp. 15, 22, 43). This part is assigned to resilience management.[82]

The German Institute for Standardization (DIN) and the German Federal Office for Information Security (BSI) generally recommend that best practices from frameworks[83] should first be used at all levels (mobile device, cloud, etc.) (DIN e.V., 2018, p. 81; BSI, 2020, p. 6). In addition, experience from industry or sector-specific experience and experience from incidents can supplement the best practices. Best practices are measures that a provider can anticipate because it is generally known that attacks on specific IT components have been successful in a certain way in the past, e.g. in other systems. In this context, there is, for example, OWASP[84] . The nonprofit organization's website lists the "Top 10"/"Top 100" vulnerability lists, including for mobile devices, for example, and publishes them approximately every three years. Vulnerabilities that are listed there must therefore be closed by default. With best practices, the system therefore does not need to be extensively analyzed. If these vulnerabilities are not fixed (closed), then it is very likely that an attacker will exploit them. These can be, for example, organizational specifications or specifications for organizational and technical processes (Sowa, 2011, p. 36). In ISO 27002, for example, there is a catalog of measures with a large number of preventive, detective and reactive measures (DIN e.V., 2018, pp. 86-193).

Overall, providers of data-based services pursue controlled and restricted access to data worthy of protection, so-called data assets (Balzer & Schorn, 2011, p. 365; Sowa, 2011, p. 24; BSI, 2020, p. 31). In order to ensure access only by authorized persons (groups), three essential protection goals are defined, which must be protected by suitable properties and measures (BSI, 2020, p. 13):

- Availability: Ensuring that functions are maintained.
- Confidentiality: Data may only be viewed by authorized persons.
- Integrity: Data changes must be traceable and transparently recordable.

If a cyber-physical locking product or all other units required to use or provide the access service (e.g. cloud components and mobile devices) are directly threatened by an attacker, the protection goals of integrity, availability and confidentiality are compromised from an IT perspective (Abendroth, 2004). In IT, system-inherent vulnerability is defined by a breach of a protection objective (First.org, 2022). A breach of the protection objective means that an attacker can use data assets for their own maliciously motivated purposes. In the case of CPS, there are data assets of varying value. The operator of a CPS does not want to give either the customer or external parties unrestricted access to (certain business-relevant) data, such as a valid digital certificate that can be used to lock or unlock a vehicle. For this reason, roles and authorizations are linked to user credentials, e.g. there are developers, administrators and users, whereby the roles and rights can be differentiated in different ways. A basic distinction is made between the three functions "read", "write" and "execute" for specific use cases (Anderson 2001, pp. 93-99). These define the respective functional scope of users and machines. They are defined in so-called "policies" (Grimm, 2019, p. 22).

[82] Resilience management is essentially about the recovery and adaptability of a system after a security incident or attack (Ritz, 2015, p. 22).

[83] This includes standards with catalogs of measures, as elaborated by Schwerdtfeger (2018).

[84] OWASP (Open Web Application Security Project) is a non-profit organization that aims to improve security in the development of web-based applications and services through specifications such as those outlined in the Application Security Verification Standard (ASVS). At its core, it is about ensuring secure programming through rules, training and the use of testing tools.

There is a wide variety of roles and access rights in IT. Users or machines with high authorizations, e.g. administrators, control and regulate the roles and rights of users and machines with lower authorizations. They also have access to more sensitive data than simple users. On the other hand, subordinate entities should not be able to modify actors higher up in the hierarchy, i.e. a user with read rights, for example, should not be able to deprive a full administrator of their rights. On the other hand, subordinate entities must be prevented from viewing data at a higher level. This principle is referred to as multi-level security (Anderson, 2001, p. 243). Security between entities that are hierarchically arranged at the same level and thus coordinated, and the principle of several security mechanisms of a single entity connected in series, such as two-factor authentication (Kofler et al., 2018, p. 51), comprise so-called multi-lateral security (Anderson, 2001, p. 276).

IT allows systemic configurations with different scopes of access, e.g. internet, intranet or locally connected systems (First.org, 2022). In principle, this logic is also characterized by interaction between layers of a unit and between systemic actors (Kumar et al., 2014). In IT, there is a standard concept called the server-client model, which describes the relationship between the units of an IT system and the distribution of tasks between the IT units (DIN SPEC 27070). Before discussing the properties, functions and topological structures of the server-client model and its characteristics, the following terms are defined based on Harris (2021) to aid understanding:

1. A server can be described as a program that gives clients access to services.
2. A client (service user) can request services from a server. It uses a program to do this. The server provides the client with services.
3. A program is a sequence of defined instructions to execute certain functions on a programmable, data-processing system.
4. A service is a type of communication protocol for exchanging data between the server and the client according to fixed rules.

It is also necessary to differentiate between the terms request and response. Request describes the client's request to the server to be allowed to use a service. The response, on the other hand, is the server's answer to the client's request (see Figure 65).

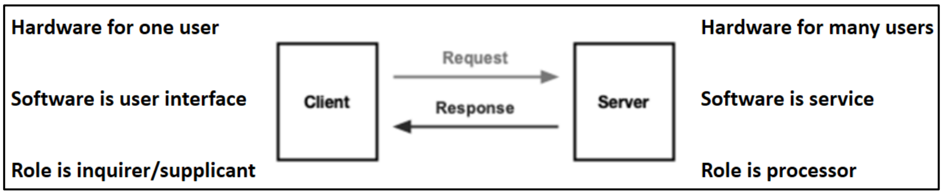


Figure 65: Basic structure and basic principle of a server-client connection.
Source: Electronics Compendium (2021).

The relationship and communication between servers - or service providers in general - and clients - the service users - can take on different forms. A common distinction is the division into the peer-to-peer network (P2P) and the classic server-client network (Harris, 2021). A P2P network is characterized by decentralized computers. The aim of using such a network is to share information with either all or selected users. All computers are equal, i.e. every participant has access to all available services and resources. Each node is authorized to offer services and also to obtain services from others. Each participant can therefore be a client and server at the same time. Other nodes can be informed of what services are being used and to which other nodes there is connectivity. In contrast to the P2P network, the client-server model is a centralized structure (see Figure 66).

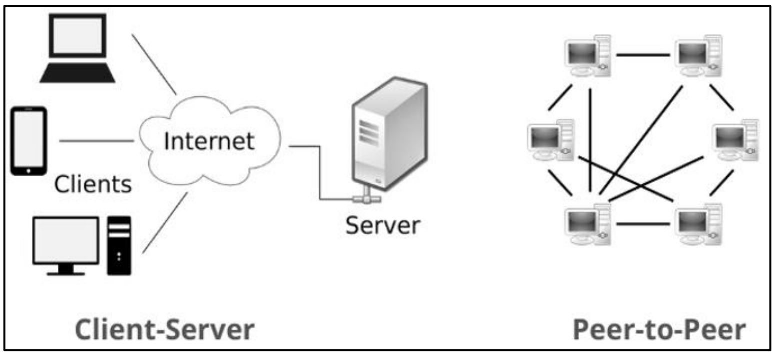


Figure 66: Figure of the client-server and P2P network.
Source: Harris (2021).

A server manages resources and services and makes them available to clients, e.g. computers, which are all connected to the server in a network. A network is, for example, the internet. In the server-client model, the server is therefore the intermediary in the network and waits until clients request services or resources - only then does the server traditionally respond. Understanding these basic structures is relevant for a security assessment because the inherent characteristics and topology of the network define the following security-relevant points, among others:

- Number of participants
- Layout, physical accessibility and IT accessibility[85]
- Role concept or functions, tasks and access rights (read, write, execute)
    - User management
    - Authorization management
    - Key Management
    - Etc.
- Interfaces to other nodes and user interfaces
- Data model
    - Protocols (fixed communication rules) for storing, processing, editing and transferring data
    - Synchronization and upgrade
    - Service and resource management
- Security measures to ensure confidentiality, availability and integrity

Essentially, a use case defines the functional scope of services, actors and technical units on the IT side, as well as their interfaces with each other, the role concept, the data model (i.e. the handling of data) and technical security measures. In summary, there are service providers on the one hand and service users on the other. Online rental services for apartments or vehicles, for example, offer their customers simple booking and payment via app (see e.g. Uber (2021) and Airbnb (2021)). However, the question arises as to how customers get into the vehicle or apartment. Although the physical key could be handed over by the owner or previous tenant, this may not be very practical in the event of a high turnover of tenants - especially around the world. For this reason, there needs to be a way of transferring the booked rental service from the online world (the app) to the physical world. MAS have a key role to play here. For example, a tenant could book an apartment and, after paying, receive a digital certificate with which they can authenticate themselves at the locking system in the door to enter the apartment. The MAS therefore physically implements the digital service. Different role concepts can also be implemented with regard to access to MAS. It is conceivable that there could be administrators who manually assign authorizations to certain users, e.g. cleaning staff.

[85] As a rule, the computers are used by human users.

The classic client-server model, which only represents the logical structure at IT level, can therefore be extended to include the physical representative of a service (the locking device) (see Figure 67). Basically, the physical representative is also a type of client that executes certain actions (e.g. locking or unlocking) on behalf of the server according to defined rules (a user must be in possession of a valid digital certificate). In addition, there could be connections between the individual clients, whereby a direct connection between the locking device and the server would also be possible, e.g. to update the time and the list of blocked users.

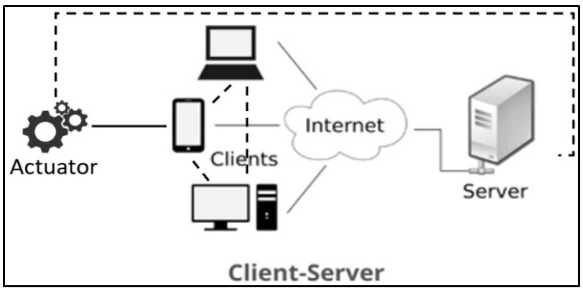
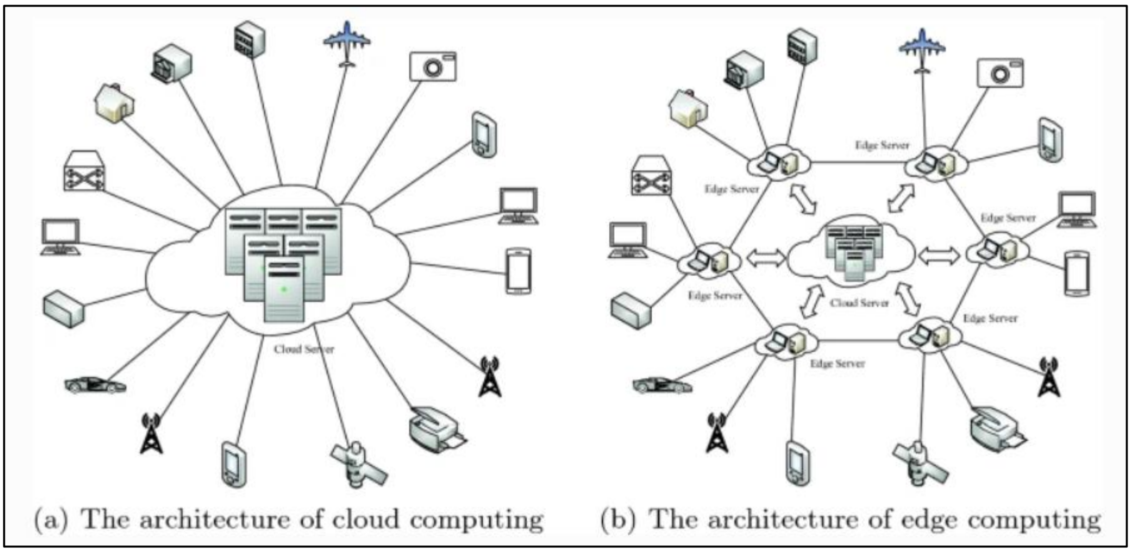


Figure 67: Extension of the client-server model through the physical component and interconnectivity between the clients.
Source: Own Figure in Harris (2021).

If an architecture now consists of units that are interconnected in any number of complicated ways and can be divided into several subordinate servers, which in turn offer different services to a large number of clients, then this is referred to as edge computing (Luo et al., 2020) (see Figure 68). Edge computing is a form of cloud computing, whereby the classic server-client model forms the basis of cloud computing. There are usually users behind the servers and clients. Users have different roles and associated functions. At the same time, the server-client model implicitly involves the management of different tasks.



(a) The architecture of cloud computing (b) The architecture of edge computing

Figure 68: Comparison of cloud and edge computing.
Source: Luo et al. (2020).

According to DIN EN ISO 9000:2015-11 (DIN e.V. 2015a), the bundling of processes and procedures so that certain tasks can be conducted in accordance with specific requirements is referred to as a "management system". Management systems in the context of access consist of the elements user management, device management, key management, interface management (API management) and authorization management (Grimm, 2019, p. 36). User and device management are also summarized under the term "identity management". Key management, interface management (API management) and authorization management are summarized under the term "access management" (Sharma et al., 2015). MAS are identity and access management systems (IAM) due to this classification. Different parts of the management systems can be administered by different units of the architecture.

For example, one unit can offer key management and interface management as a service, while another unit is responsible for user and device management. However, the division of tasks does not always have to be clearly defined. Services and associated data can also be hosted by one or more instances. For example, a host can own servers and offer their use to its clients in the form of a service. Clients of a host can use these services and offer their own clients further services that dock onto the host services. But why is an understanding of the distribution of tasks and interdependencies within an architecture important for a security assessment? On the one hand, the architectural structures show actors, their functional scope and interfaces, and on the other hand, they provide an indication of possible entry points, attack paths and possible effects on the provision or use of services in the event of a successful attack (Kofler et al., 2018, pp. 31-35; Möller et al., 2019, p. 308). With CPS, it is assumed that successful attacks on data assets always manifest themselves in the physical domain.

For example, if an attacker succeeds in gaining administrator rights, security mechanisms can be overridden, role rights of other users can be revoked or modified or backdoors can be implemented to secure long-term access to data or physical assets. In the case of automotive MAS, for example, the theft of one or more vehicles is a possibility. The physical attack could be facilitated by the compromise of an IT unit. For this reason, and partly due to a lack of measures for targeted observation and intervention, IT security generally relies 100% on protection (Wheeler, 2011, p. 18). In addition, IT is constantly evolving (at ever shorter intervals), which means that security measures previously considered secure are classified as obsolete. IT security assessment therefore takes a strong binary view, i.e. a system is either secure or insecure and must be tested at regular intervals (Kofler et al., 2018, p. 29). Furthermore, although a method can generally be considered theoretically secure, it is the implementation in hardware or software that determines security in practice (BSI-Bund, 2021b).[86] State-of-the-art security mechanisms are considered sufficiently secure as long as no new, exploitable vulnerabilities (so-called zero days) are published, e.g. in the National Vulnerability Database (NIST, 2021; Kofler et al., 2018, pp. 47-48). There could also be direct measures to counter such cases, e.g. in the form of an administrator who is on the move in forums and thus immediately notices when there are published zero days. By being up to date, the response time can generally be optimized so that it is possible to upgrade your own system. However, there will always be a delay between detection and implementation (implementation of a fix) (First.org, 2022).

[86] The article by ZDNet (Cimpanu, 2020) in particular shows that an inadequately secure implementation can have business-relevant consequences. According to the news website ZDNet, the source code for smart car components of Mercedes-Benz vans was "leaked" online. This leak came about after Till Kottmann, a software engineer from Switzerland, discovered a so-called Git web portal of Mercedes-Benz AG. "Kottmann told ZDNet that he was able to register an account on Daimler's code-hosting portal and then download more than 580 Git repositories containing the source code of onboard logic units (OLU) installed in Mercedes vans," writes Cimpanu on ZDNet (Cimpanu, 2020). The problem with this leak was that none of the repositories had an open source license, meaning it was proprietary information that was not intended for the public. Such a scenario must be reflected in the vulnerability assessment of MAS.

8.2.2 Structure and Properties of the Physical Layer

Physical security, also known as object protection, is an elementary component of IT security, as elements for storing, processing and transferring data are tied to physical hardware (Anderson, 2001, pp. 365-388). The aim of physical security is to use technology to protect people, property and assets, including data assets (Garcia, 2007, p. 8). Physical assets are protectable goods of value to an operator or user (Klipper, 2015, p. 75). Crime prevention can generally be achieved through "environmental design" (Fennelly et al., 2016, p. 4). When assessing physical security, physical risk is considered on the basis of physical vulnerability, i.e. the properties and mechanisms for protection, observation or detection and intervention in the event of a physical attacker are assessed in the use case (Fennelly et al., 2016, p. 18). The interaction between physical barriers, sensors and the processing of alarms is considered for this purpose (Garcia, 2007, p. 87). Physical access systems are the comfort flap that makes the use of a vehicle possible in the first place. Access systems are needed in the physical world to ensure that only authorized persons have access to physical assets. Different options can be used to prove authorization for physical access, e.g. biometric (feature), mechanical (possession/knowledge) or contactless (knowledge, e.g. passwords) (Pohlmann, 2021).

The basic principle of physical security is referred to as Defense in Depth (DiD) or Protection in Depth (PiD) (Harnser, 2010, C3, p.14; Garcia, 2007, p. 59). Physical barriers are arranged topologically one behind the other, similar to onion skins, and enclose the physical asset in the nucleus. Each barrier is equipped with one or more access systems. When assessing physical threats, attack paths through the barriers to the physical asset are considered (Harnser, 2010, B4, p. 50). Physical security is about how assets must be equipped with barriers so that specific attackers can be stopped for as long as possible to enable timely intervention by the physical defender. In Harnser (2010, p. 7), this step is taken in the design phase, also known as "conceptualization" (of security measures). Attackers can also be detected during the realization of an attack, provided that suitable detection measures are in place. Sensor systems, for example, detect whether someone is approaching or attempting to gain (abusive) physical access to something (Harnser, 2010, C3, p. 17).

For example, the error rate of detection measures must be taken into account (BHE, 2021). If an attacker is detected in good time, it may still be possible to intervene before the attacker reaches their target. What can happen after an attack is assessed in particular for critical infrastructures (KRITIS) (Harnser, 2010, B3, p. 40). In the classic vulnerability model, as proposed in Garcia (2005) and Lichte et al. (2016), the attack process is only assessed until the asset is reached. Part of the considered components of the physical mechanism of performance in physical security is monitoring. First of all, this requires observation, i.e. technologies or people must continuously check whether a potential attack is taking place (Lichte et al., 2016). Observation is therefore a form of identification in the sense that something is perceived that could become a threat. If an attack is then actually conducted, it must be recognized as such. This, in turn, is detection (Garcia, 2007, p. 58). Only once detection has taken place can an intervention be initiated, e.g. in the form of an intervening security team (Harnser, 2010, B4, p. 47). The attacker must be stopped long enough so that he either abandons his plan or is stopped by an intervention unit. The mechanism of performance considered here is protection (Harnser, 2010, B4, p. 47).

Protection can be achieved through protective measures, such as armoring a door. In contrast to a protective measure, which refers to the condition of a barrier to make intrusion more difficult ("door closed"), a security measure describes that the barrier is present at all or that it has a certain vulnerability ("window of defined security level installed") (Harnser, 2010, C2, p.10). Access control and the authentication of users by means of access systems play a decisive role

(Harnser, 2010, C3, p.15). The security function of the components connected to a physical system is assessed using metrics. A physical attack can be described by a time sequence in which the attacker must overcome a defined number of n barriers in order to gain access to the physical asset (Garcia, 2007, p. 58) (see Figure 69).

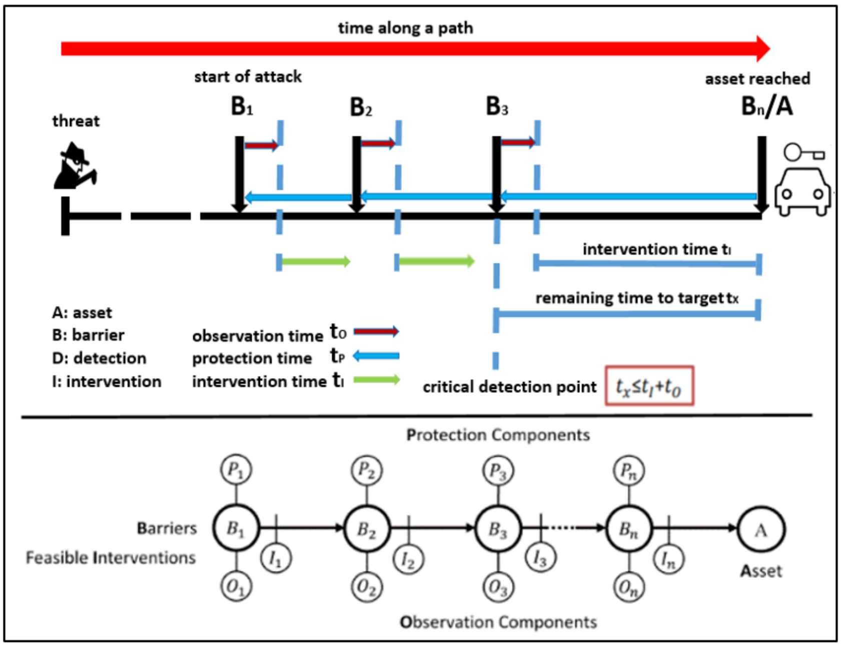


Figure 69: Physical vulnerability model.
Source: Own Figure based on Garcia (2005) and Lichte et al. (2017); image source: Flaticon.com (2021) and Flinkey.de (2021).

Barriers delay an attacker from reaching their target. If the attacker is detected early, the defender still has enough time to initiate appropriate intervention measures. The average intervention time must be less than the attacker's residual overcoming time (Lichte et al., 2016). The remaining overcoming time is the time that the intervention unit has left to dissuade the attacker from his plan before he can cause damage to the asset or steal it. In physical security, the time between the intrusion time and the reaction time is therefore assessed. Conversely, this means that if the intervention takes too long, the operator, for example, must consider what measures need to be taken and in what form - i.e. with what effectiveness - so that the attacker can be prevented from succeeding (Garcia, 2007, pp. 58, 66).

This is important in prospective analysis, e.g. using the scenario technique, as there is then still an opportunity to optimize the system in terms of vulnerability before a worst-case event has occurred. Risk analysis initially involves identifying possible weak points or vulnerable paths that can be exploited by the attacker (Klipper, 2015, p. 97-106). In principle, it can be assumed that the attacker will consider ways to achieve the objective before launching the attack and will choose the weakest path (Ingoldsby, 2016). Physical security management and IT security management are both based on the Plan-Do-Check-Act model (PDCA) (BSI, 2020, p. 93; Fennelly et al., 2016, p. 5; Schwerdtfeger, 2018, p. 21).

8.3 Cross-Domain Consolidation in other Disciplines

The problem of aligning and merging metrics from two domains can also be observed outside of security research, e.g. in physics. Work is underway to develop a "world formula". The aim of physics is to find a universal model with which all fundamental interactions between the basic forces of physics (gravity, electromagnetism, weak interaction and strong interaction) can be explained and brought together in one theory (Laughlin et al., 2000). However, there are also hurdles here, as the following example briefly outlines: According to Einstein's theory of relativity, the basic force of gravity is a theory of the geometry of space and time, also known as space-time. In simple terms, it is about distances that can be measured with quantitative precision. This is quite possible in the world of the large. In the world of the very small, the quantum world, both the distances between so-called point particles[87] and the speeds of these particles cannot be measured precisely (Conlon, 2016, pp. 11-20). In this context, we speak of the so-called uncertainty principle. For this reason, simply put, the theory of gravity is not compatible with quantum theory.

The theory of strings was therefore introduced in physics. According to this theory, elementary particles and gravity can be described using the oscillation forms of a string (Conlon, 2016, p. 67). Although this theory initially became popular as a possible world formula, a mathematically consistent string theory does not work in the universe as described by Einstein with three spatial and one temporal dimension. A total of ten dimensions are possible. Statements of string theory have not yet been proven experimentally (Conlon, 2016, pp. 107-208). Based on this, theoretical model universes were constructed in which the jump theory could be applied (Woit, 2011). Consideration was given to eliminating the six extra dimensions in order to represent the known universe. However, this was not successful. In Hawking & Mlodinow (2010), the world formula is therefore described as "elusive". In conclusion, comparable challenges in merging metrics, such as those presented in this paper using the example of physical security and IT security, also exist in other domains.

[87] In simple terms, point particles refer to particles that are interpreted as points in space. Precise interactions can be calculated by considering the individual mass and charge of each particle.

Curriculum Vitae

The curriculum vitae is not included for reasons of data protection.

Conferences

Termin, T., Lichte, D., & Wolf, K. D. (2023). Risk Adjusting of Scoring-based Metrics in Physical Security Assessment. *In: Proceedings of the 33rd European Safety and Reliability Conference* (ESREL 2023, Southampton, United Kingdom, 03.09. - 08.09.2023). Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Cépin and Enrico Zio. doi: 10.3850/978-981-18-8071-1_P011-cd.

Termin, T., Lichte, D., & Wolf, K. D. (2022). An Analytic Approach to Analyze a Defense-in-Depth (DiD) Effect as Proposed in IT Security Assessment. *In: Proceedings of the 32nd European Safety and Reliability Conference* (Dublin, Ireland, 28.08. - 01.09.2022). Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, Simon Wilson. doi:10.3850/978-981-18-5183-4_R26-01-246-cd.

Lichte, D., Witte, D., Termin, T., & Wolf, K. D. (2021). Representing Uncertainty in Physical Security Risk Assessment: Considering Uncertainty in Security System Design by Quantitative Analysis and the Security Margin Concept. *In: European Journal for Security Research*; November 28, 2021. doi: 10.1007/s41125-021-00075-3.

Termin, T., Lichte, D., & Wolf, K. D. (2021). Physical security risk analysis for mobile access systems including uncertainty impact. *In: Proceedings of the 31st European Safety and Reliability Conference* (Angers, France, Sept. 19-23, 2021). Edited by B. Castanier; M. Cepin; D. Bigaud; C. Berenguer; ISBN / doi: 10.3850/978-981-18-2016-8 175-cd.

Lichte, D., Termin, T., & Wolf, K. D. (2020). On the Impact of Uncertainty on Quantitative Security Risk Assessment. *In: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (Venice, Italy, Nov. 1-6, 2020). Edited by P. Baraldi; F. Di Maio; E. Zio; ISBN / doi: 978-9981-14-8593-0.

Termin, T., Lichte, D., & Wolf, K. D. (2020). Approach to generic multilevel risk assessment of automotive mobile access systems. *In: Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference* (Venice, Italy, Nov. 1-6, 2020). Edited by P. Baraldi; F. Di Maio; E. Zio; ISBN / doi: 978-9981-14-8593-0.

Guest Contributions

Mühl, Kim Y. (2020). AGILITY & OPEN SOURCE FOR A SUCCESSFUL DIGITAL TRANSFORMATION, *In: Bionic Wealth: The next generation of investing is inspired by life.* pp. 130-133. self-published.

Mutschler, A., Alexandropoulos, K., Termin, T., & others (2023). Research Paper AUTOMOTIVE. Why you should reorient your automotive business model, now. *20blue edition.* 20blue Project GmbH 2023.