BERGISCHE
UNIVERSITÄT
WUPPERTAL

Ganzheitliche generische Risikobewertung von automobilen Mobile-Access-Systemen

Dissertation
zur Erlangung eines Doktorgrades
(Dr.-Ing.)

in der
Fakultät für Maschinenbau und Sicherheitstechnik

der
Bergischen Universität Wuppertal

vorgelegt von
Thomas Termin
aus Wuppertal

Erstgutachter:	Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf
Zweitgutachter:	Univ.-Prof. Dr.-Ing. Tibor Jager
Tag der Einreichung:	12.04.2023
Tag der mündlichen Prüfung:	11.10.2023

Wuppertal 2023

Versucht, den Dingen, die ihr seht, einen Sinn zu geben, und hinterfragt, aus was sich das Universum zusammensetzt. So schwer das Leben manchmal auch erscheinen mag, es gibt immer etwas zu tun und darin gut zu sein. Es ist wichtig, dass ihr einfach nie aufgebt. Denkt daran, in die Sterne zu sehen – und nicht auf eure Füße.

Stephen Hawking

Vorwort des Erstgutachters

Technische Systeme sind heutzutage ohne Kommunikation und Datenaustausch mit der Umwelt kaum vorstellbar. Von der Konfiguration und Steuerung über die Bluetooth-Schnittstelle eines Smartphones, die die aufwendige Implementierung von Benutzerschnittstellen am Gerät entbehrlich macht, bis zur quasi permanenten Einbindung in Plattformen und Netzwerke über das Internet und Mobilfunk oder WLAN-Schnittstellen, wie man sie bei Smart-Home-Geräten z. B. antrifft, ist die IT-basierte Kommunikation wesentlicher Bestandteil der Funktionalität moderner Technik. Neben allen Vorteilen, die die IT-basierte Kommunikation bietet, birgt sie aber auch Schwachstellen, die sich z. B. aus der Verfügbarkeit der Internet- und Mobilfunkanbindung und insbesondere der Angreifbarkeit der IT-Komponenten durch die Vernetzung ergeben. Wenn wir heute über Security sprechen, meinen wir meist „Cybersecurity", also die Sicherheit IT-basierter Systeme gegen Angriffe aus dem „Cyberspace", i. d. R. aus dem Internet. Die Anbindung an das Internet bringt Angreifer aus aller Welt quasi direkt vor die Haustür oder besser: direkt ins Haus oder auch ins Fahrzeug. Die Absicherung gegen solche Angriffe wird somit zur Aufgabe, die für alle modernen und vernetzten technischen Systeme zu erfüllen ist. Dieser Tatsache tragen neuere technische Richtlinien und Standards, wie z. B. der ISO/SAE 21434: „Road Vehicles – Cybersecurity engineering", Rechnung.

Da die allgegenwärtige IT-Anbindung immer mehr technische Systeme einbezieht, werden zunehmend Konzepte „cyberphysischer Systeme" diskutiert und entwickelt. Diese Systeme zeichnen sich durch maßgebliche Wechselwirkung mit der physischen Welt aus. Ein Pkw z. B., der im Stadtgebiet durch einen Hackerangriff außer Kontrolle gerät, kann erheblichen Schaden an Menschen und Sachen verursachen. Sicherheitsrelevanten Systemen kommt in diesem Kontext eine besondere Bedeutung zu, sind sie doch zum Schutz vor physischen Gefahren entwickelt worden. Bei Systemen zur Gewährleistung der funktionalen Sicherheit, die konzeptionell immer auch Sensoren und IT-Komponenten beinhalten, rückt somit die angemessene Auslegung von IT-Sicherheitsmaßnahmen in den Fokus. Während z. B. in der Normenreihe des IEC 61508 quantitative Kriterien zur Auslegung der Verfügbarkeit (im Sinne des Ausfalls/Versagens von Komponenten oder Teilsystemen) funktionaler Sicherheitssysteme detailliert vorgegeben sind, findet man solche Vorgaben im Hinblick auf die IT-Sicherheit nicht.

Dies ist eine große aktuelle Herausforderung für die Menschen, die solche Systeme auslegen oder bewerten und mit der Frage konfrontiert sind: Wie umfangreich müssen Cyber-Sicherheitsmaßnahmen ausgelegt werden, um den Sicherheitsanforderungen in der physischen Welt im Sinne der dahinterliegenden Risiken zu entsprechen? Auch in der oben angesprochenen ISO/SAE 21434 finden sich keine quantitativen Kriterien zur Auslegung der Cyber-Sicherungssysteme. Dementsprechend fällt eine in Bezug auf das erforderliche Sicherheitsniveau angemessene und damit risikogerechte Auslegung von physischen Sicherungssystemen im Automobilbereich, wie den in dieser Arbeit adressierten automobilen Mobile-Access-Systemen, schwer. Der Grund für die immer noch bestehende Zweigleisigkeit der Bewertung von Sicherheit cyberphysischer Systeme liegt in den jeweiligen Metriken. Quantitative Sicherheitsmetriken, wie sie für eine umfassende Zusammenführung der beiden cyberphysischen Domänen erforderlich wären, sind in der IT-Security nicht gebräuchlich.

Darüber hinaus werden Wirkzusammenhänge, wie sie z. B. über statistisch beschreibbare Komponentenausfälle oder Überwindungszeiten von Barrieren in der physischen Welt hergestellt werden können, in der IT-Sicherheit in der Regel nicht abgebildet. Somit bleiben physische und IT-Sicherheitsniveaus schwer vergleichbar. Ebenso kann die in Bezug auf ein Risikoniveau angemessene domänenübergreifende Auslegung von Sicherheitsmaßnahmen cyberphysischer Systeme schwerlich beurteilt werden. Wie und wie weit lassen sich nun die beiden cyberphysischen Domänen in der Sicherheitsbewertung durch kluge Anpassung der Metriken zusammenführen, bzw. wie lässt sich eine risikogerechte Auslegung der Sicherheitsmaßnahmen in beiden Domänen, die ggf. auch von Wechselwirkungen betroffen sein können, bewerten? Dieser nicht ganz einfachen Fragestellung widmet sich die vorliegende Dissertation.

Velbert, im Oktober 2023

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

Danksagung

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

Die vorliegende Forschungsarbeit mit dem Titel „Ganzheitliche generische Risikobewertung von automobilen Mobile-Access-Systemen" ist im Rahmen des Doktorandenprogramms zwischen der Unternehmensgruppe WITTE Automotive und dem Institut für Sicherungssysteme (ISS) der Bergischen Universität Wuppertal (BUW) am Lehrstuhl für Mechatronik der Fakultät für Maschinenbau und Sicherheitstechnik entstanden. Der Weg zum Erkenntnisgewinn ist eine besondere Zeit für die persönliche Weiterentwicklung und mit großen Herausforderungen sowie Anstrengungen verbunden – sowohl für den Doktoranden als auch für die Personen, die ihn bei der Erstellung der Dissertation begleiten. Aus diesem Grund möchte ich zuallererst meinem Doktorvater, Herrn Univ.-Prof. Dr.-Ing. Kai-Dietrich Wolf, danken, der dieses Promotionsvorhaben wissenschaftlich betreute und stets für einen konstruktiven Gedankenaustausch zur Verfügung stand. Bedanken möchte ich mich bei Herrn Univ.-Prof. Dr.-Ing. Tibor Jager für das Zweitgutachten und die wertvollen Impulse im Zuge der Erstellung meiner Doktorarbeit.

Ebenfalls bedanken möchte ich mich beim Team WITTE Digital für die anregenden Ratschläge sowie Diskussionen, vor allem Paul Meier, Christian Goldschmidt und Michael Tworek für die unternehmensseitige Betreuung. Ein besonderer Dank gilt Herrn Rainer Gölz, Geschäftsführer der WITTE Automotive, der mein Promotionsvorhaben finanziell ermöglicht hat, sodass ich die Dissertation zu gleichen Teilen sowohl am Institut für Sicherungssysteme als auch bei WITTE Digital durchführen konnte. Ich bekam die Möglichkeit, meine zeitlichen Ressourcen am Institut und bei WITTE variabel zu gestalten. Weiterer Dank gilt meinen Arbeitskollegen bei WITTE und meinen Wegbegleitern in der Industrie, u.a. 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 und Daniel Hommen. Sie haben mich stets motiviert und mich bei meinen Aufgaben hilfreich unterstützt.

Bedanken möchte ich mich auch bei meinen universitären Kollegen, Dustin Witte, Max vom Stein, Christian Marré, Max Hoppe, Manfred Dillenberg und Benjamin Dymel, sowie der Assistenz des Universitätsprofessors, Sabine Kranz, die mich bei meiner Vorlesungsbetreuung und wissenschaftlichen Forschung stets unterstützten und mich in meinen Vorhaben bestärkten. Darüber hinaus danke ich Herrn Roman Kochanek, Herrn Helge Schroda, Herrn Christoph Wegener und Herrn Dejan Djordevic für den regen Austausch rund um Security-Metriken und Compliance. Einen großen Dank an Enrico Zio, Dekan der Graduate School der Universität Politecnico Milano in Italien, für den inspirierenden Austausch zum Thema Entscheidungsfindung unter Unsicherheit. Abschließend gilt ein ganz herzliches Dankeschön meinen Eltern, die mich immer emotional und finanziell unterstützt haben. Auch waren meine Geschwister, Kamil Termin und Kerstin Termin, in schwierigen Zeiten stets für mich da – danke für eure große Geduld und das geschenkte Vertrauen. Ohne ihre Hilfe wäre ich nie so weit gekommen.

Wuppertal, Oktober 2023 Thomas Termin

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.

Abstract

The growing global threat situation has far-reaching consequences for the standardization of product development processes in the automotive industry. Since automotive products are increasingly security-relevant and business models are behind the products, companies are required to conduct a threat analysis and risk assessment. Given the connection of physical security functions and information technology, two domains have to be considered in threat analysis and risk assessments of automotive products, physical security and IT security. However, the assessments of physical security and IT security do not match, since significantly different assessments in the two domains correspond to unequal vulnerability levels: In physical security, the vulnerability can be analyzed in terms of the time game between the intrusion time of an attacker and the reaction time of a defender. The quantitative basis for assessment is the interaction of protection, observation and intervention. In IT security, vulnerability is assessed via the exploitability of system-inherent weaknesses. Vulnerability is classically determined by scoring threat scenario-describing parameters. Quantitative analysis of performance is difficult to perform in IT security due to the lack of an objective performance mechanism for assessment. It is impossible to conduct an assessment in a reproducible way. Given the interfaces between hardware and software, successful IT scenarios can have an impact on safety functions and physical security mechanisms.

Therefore, from a product development perspective, the question of a suitable metric for cross-domain risk assessment comes up. In common standards and guidelines, such as ISO 26262, ISO/SAE 21434 or IEC 61508, the problem of merging safety and IT security metrics is described on an abstract level. However, approaches to enable a quantitative analysis are not presented in the standards. This doctoral thesis deals with the possibilities and limitations of performing 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 is 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.

Subsequently, it is shown how a well-defined mechanism of performance in a quantitative metric can be translated into consistent scores as part of a scoring metric. The vulnerability assessment according to Lichte, referred to in this work as the Intervention Capability Metric (ICM), is used for the quantitative calculation of physical vulnerability. For the scoring-based assessment, the Harnser metric is used. As part of a metric-based analysis, the Harnser metric is adapted in terms of the combination of scoring parameters and the scoring scale to produce equal vulnerability ratings as the ICM. Vulnerability values resulting from using the ICM are assumed to correspond to objective vulnerability levels. Examples are used to illuminate the degrees of freedom that exist in aligning the semi-quantitative Harnser metric and the quantitative ICM. The paper then examines the distortions that arise in the application of scoring-based assessments and how these can be mitigated. As an example, the Common Vulnerability Scoring System (CVSS) from the IT security domain is considered. In particular, possibilities for the reduction of metric-inherent distortions by means of the log transformation are shown. Furthermore, the architectural and metric considerations of a barrier-based CVSS approach are discussed. In this work, options to reduce distortions within the barrier-based CVSS approach are shown.

Then, ways and assumptions to align 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 IT vulnerability are considered here. Both metrics are modified with the goal of providing a comparable vulnerability rating despite different assessment bases. This alignment is done to standardize the approach to vulnerability assessment as a building block of threat analysis and risk assessments in physical security and IT security. For this purpose, a normalization of the assessment parameters via a log transformation is proposed. Furthermore, the scale categories and the parameter expressions are adapted to one another. It is explained how the scales of physical impacts and IT impacts can be normalized. The normalization of the impact scale aims at taking into account the different scalability of impacts caused by physical attacks and impacts caused by IT attacks in one scale. Beyond that, approaches to cross-domain risk assessment are discussed. Because an objective performance mechanism is difficult to obtain in IT security, the CVSS metric cannot be adapted in such a way that it is possible to generate vulnerability ratings equal to the ICM ratings.

For this reason, a security assessment of the Physical Impact on IT Vulnerability is omitted. In contrast to the CVSS metrics, the Harnser metric can be backed by an objective performance mechanism and adapted to objective vulnerability levels. Consequently, it is argued that a quantitative assessment of the impact of IT scenarios on physical scenarios is possible. In order to assess this cross-domain interaction, the new parameter IT Impact on Physical Vulnerability is introduced. Here, 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 to the physical vulnerability without the influence of an IT scenario. Finally, a rating scale is used to assess the degree of compromise. It is shown that vulnerability does not have to be made comparable in both domains in order to enable a cross-domain security assessment.

Beyond that, the determination of physical security levels and IT security levels is discussed. 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 evidence is scarce, it is reasoned that transferring the matrix for ASIL grading to physical security grading and IT security grading is difficult to implement. Instead, it is shown how Physical Assurance Levels (PAL) and CAL can be derived in the same way via mapping the impact of an event against controllability following a successful threat scenario. Next, it is explained how IT Impact on Physical Vulnerability can be considered 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 linkage of knowledge about the vulnerability by physical or IT means is performed using the Bayesian network method. To take different expert statements into account, the threat analysis and risk assessment is extended in a further step by applying a methodology for the elicitation of expert knowledge. The proposed survey methodology combines elements from the Delphi method and Cooke's survey approach.

Each expert indicates his or her subjective degree of conviction as to the extent to which a certain condition is true for an assessment variable. In addition, the expert's own confidence in the statement made is given a value between 0 % and 100 %. The subjective probabilities are weighted via the confidences. By integrating the elicitation and weighted merge of 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 risk acceptance is reached. In this research work, a mixed-method or mixed-metric approach for the risk assessment of cyber-physical systems is introduced. The generic approach can be used for different

use cases, be applied repetitively in the sense of a continuous improvement process, and enable a quantitative analysis of physical scenarios that are influenced by IT scenarios.

Overall, the proposed methods and metrics can be used to make better decisions regarding the investment in security measures because the scoring-based vulnerability assessment in physical security has been adapted to objective vulnerability levels using a quantitative metric. Both assessments yield the same risk ratings. It also shows how log transformation can be used to align security metrics from the physical security and IT security domains. The results of this work can be employed in follow-up research to develop an IT security metric with an underlying, objective performance mechanism. In addition, the approaches developed can be used to drive the alignment of the description and assessment of threats in the physical security and IT security domains so that the metrics of all three risk contributions are built in a risk-appropriate manner. In addition, the approaches and considerations shown in this paper can be used to contribute to enabling the merging of metrics from Functional Safety and Physical Security or IT Security.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung im Fließtext	Bedeutung
A	Availability
AADL	Architecture Analysis & Design Language
ABG	Allgemeine Baugenehmigung
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 Evaluating 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	Bundesamt für Sicherheit in der Informationstechnik
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-Managementsysteme
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D	Detektion
DES	Data Encryption Standard
DiD	Defense in Depth
DIN	Deutsches Institut für Normung
DKS	Digital Key Standard
EAL	Evaluation Assurance Levels
EFSA	Europäische Behörde für Lebensmittelsicherheit
EVITA	E-safety Vehicle Intrusion Protected Applications
FAIR	Factor Analysis of Information Risk
FESEM	Forcible Entry Safeguards Effectiveness Model
FMEA	Fehlermöglichkeits- und Einflussanalyse
FT	Fault Tree
FTA	Fault Tree Analysis
HARA	Hazard Analysis and Risk Assessment
I	Integrity; nur im Kontext der Asset-Bewertung
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	Safeguard Effectiveness Model
ISO	International Organization for Standardization

IT	Informationstechnik
ITIPV	IT Impact on Physical Vulnerability
ITU	International Telecommunication Union
K	Know-How
KBA	Kraftfahrtbundesamt
KRITS	Kritische Infrastrukturen
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	Protektion
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*	Aus PR und UI zusammengesetzte Größe
PR*-S	PR* Score
PRISM	Performance Risk-based Integrated Security Methodology
P-S	Protection Score
QM	Quality Management/quality managed
R	Ressourcen
RAND	Research and Development Corporation
RPN	Risk Priority Number
RSS	Radio Standard Specification
SAE	Society of Automotive Engineers
SAFE	Safeguards Automated Facility Evaluation
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	Akronym für: S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege
Sum	Summarized

SUMS	Software-Update-Managementsysteme
T	Threat
TARA	Threat Analysis and Risk Assessment
TR	Technical Report
TÜV	Technischer Überwachungsverein
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

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

In den letzten zehn Jahren hat der Einsatz cyberphysischer Systeme (CPS) weltweit zugenommen. Der Prognose in Lee et al. (2017) zufolge werden CPS in der Industrie und im Alltag des 21. Jahrhunderts eine zunehmende Rolle spielen. Laut einer Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, die im Rahmen der Begleitforschung zum Technologieprogramm AUTONOMIK für Industrie 4.0 im Jahre 2015 durchgeführt wurde, geht mit dem Einsatz von CPS eine Veränderung unternehmerischer Wertschöpfung und eine Steigerung von Anwendungspotenzialen einher (BMWi, 2015). In Neugebauer (2018) wird dargelegt, dass durch CPS sogar ein disruptiver Paradigmenwechsel im Vergleich zu rein physischen Systemen eingeläutet wird, bei dem der „Effizienzgewinn durch Flexibilisierung […] und bessere Ressourcennutzung durch die selbstoptimierende Automatisierung von Abläufen im Vordergrund steht" (Neugebauer, 2018, S. 198). Der Anstieg der Anzahl und der Anwendungen von CPS ist weltweit zu beobachten. Der Mobilitätssektor sticht dabei besonders hervor (Geisberger & Broy, 2012, S. 32-43; Möller et al., 2019, S. 171-172). Dies ist zum Teil auf die konzentrierten Bemühungen von Erstausrüstern (Original Equipment Manufacturer, OEM) und Zulieferern zurückzuführen, den durch die Digitalisierung getriebenen strukturellen Wandel zu digitalen Geschäftsmodellen und digitaler Wertschöpfung erfolgreich vollziehen zu wollen (Macher et al., 2020a; BSI Branchenlagebild Automotive, 2022).

Die Bedürfnisse der Kunden, Individualisierungs- und Vernetzungsmöglichkeiten sind wesentliche Digitalisierungstreiber (Bormann et al., 2018). Die weltweite Corona-Pandemie kann zudem als Beschleuniger des digitalen Wandels gesehen werden (Puls et al., 2021). Unternehmen stehen im Zuge des Transformationsprozesses vor der Herausforderung, historisch gewachsene Geschäftsmodellstrukturen zu überdenken und neu auszurichten. Produktentwicklungsprozesse müssen darüber hinaus nach Vorgaben aus neuen Richtlinien und Standards aufgesetzt werden. Das ist erforderlich, um konkurrenzfähig zu bleiben und die Zulassung von CPS auf dem automobilen Markt zu erhalten (Möller et al., 2019, S. 29, 34-37, 60; ISF München, 2021, S. 7, 51). Eine wichtige Grundlage für den Vollzug des digitalen Wandels ist die Nutzung von Informationstechnik und ihrer technologischen Möglichkeiten zur Speicherung, Verarbeitung und Übertragung von Daten (Hoffmeister, 2017, S. 41). Dem Einsatz von CPS kommt dabei eine Schlüsselrolle zu (Möller et al., 2019, S. xii-xiii). Neueste Entwicklungen verfolgen den Ansatz, die Funktionalität eines herkömmlichen physischen Fahrzeugschlüssels durch den Einsatz eines digitalen Zertifikats in neuen Use Cases (zu dt. Anwendungsfällen) zu erweitern (Möller et al., 2019, S. 439-440, 443-447). Bei einem digitalen Zertifikat handelt es sich um einen digitalen Schlüssel, der an eine digitale Benutzeridentität, ein Produkt und Benutzerrechte sowie Benutzungszeiträume geknüpft ist (Grimm, 2019, S. 22).

Zusätzlich zu der Verriegelung oder Entriegelung eines Fahrzeugs, z. B. per mobilem Endgerät, können weitere (datenbasierte) Services angeboten werden, wie beispielsweise Sharing, Zahlfunktionen, Navigation oder Belieferung (Möller et al., 2019, S. 220-233, 439). Sogenannte Mobile-Access-Systeme (MAS) sind eine noch recht neue Art digitalisierter Zugangssysteme. Sie verbinden als CPS die physische Domäne und die IT-Domäne miteinander, d. h. das mechanische Schließsystem wird durch Software- sowie Cloud-Komponenten erweitert (Schwerdtfeger, 2018, S. 29-34). Die vielfältigen Einsatzmöglichkeiten von CPS, das daraus resultierende Potenzial für Bedrohungen (Wurm, 2022, S. 32) und die global zunehmende Bedrohungslage (Hubbard et al., 2016, S. 8-11) sind die Motivation für die Durchführung einer Risikobewertung von MAS in konkreten Use Cases (siehe auch: Möller et al., 2019, S. 266, 271, 317, 339, 350). Betreiber sind bestrebt, ihre Produkte gegen Angriffe zu schützen, da sie zunehmend sicher-

heitsrelevant sind und hinter den Use Cases Geschäftsmodelle stehen (Becker et al., 2019; Macher et al., 2020a). MAS müssen unter Einsatz limitierter Ressourcen möglichst sicher designt werden, sodass Risiken auf ein Niveau gemindert werden können, das von allen Stakeholdern akzeptiert wird (Sowa, 2011, S. 23). In diesem Zusammenhang arbeiten ethische Hacker und Sicherheitsforscher daran, Schwachstellen in konkreten Anwendungen aufzudecken, siehe z. B. Samcurry.net (2023).

„In mehreren akademischen Angriffen auf Fahrzeuge demonstrierten Forscher [bereits], dass eine Fernsteuerung diverser Fahrzeugfunktionen über Funkschnittstellen machbar ist" (Wurm, 2022, S. 35). Die Zusammenarbeit von Industrie und Sicherheitsforschung trägt einerseits dazu bei, Produktanbieter frühzeitig auf Sicherheitslücken aufmerksam zu machen, bevor diese Schwachstellen von böswillig motivierten Angreifern ausgenutzt werden können. Andererseits unterstützt die Sicherheitsforschung die Produktentwicklung mittels der Entwicklung von Methoden und Metriken zur Sicherheitsbewertung und eines Praxistransfers ebendieser dabei, Sicherheitsfragen zu beantworten (Sifo.de, 2023). Eine Einordnung und Abgrenzung der Risiken, auf die sich diese Arbeit konzentriert, wird in Abbildung 1 vorgenommen. Grau eingefärbte Ellipsen in ebendieser Abbildung markieren den thematischen Schwerpunkt dieser Forschungsarbeit. In der vorliegenden Arbeit werden sowohl die Begriffe physische Sicherheit und IT-Sicherheit als auch ihre englischen Pendants, Physical Security und IT Security, verwendet. Die Bezeichnungen IT Security und Cybersecurity werden synonym genutzt. Die Begriffe bezeichnen den Zustand, in dem schützenswerte Funktionen und Güter ausreichend gegen Bedrohungsszenarien für Straßenfahrzeuge, ihre Funktionen und (elektronischen) Systeme geschützt sind.

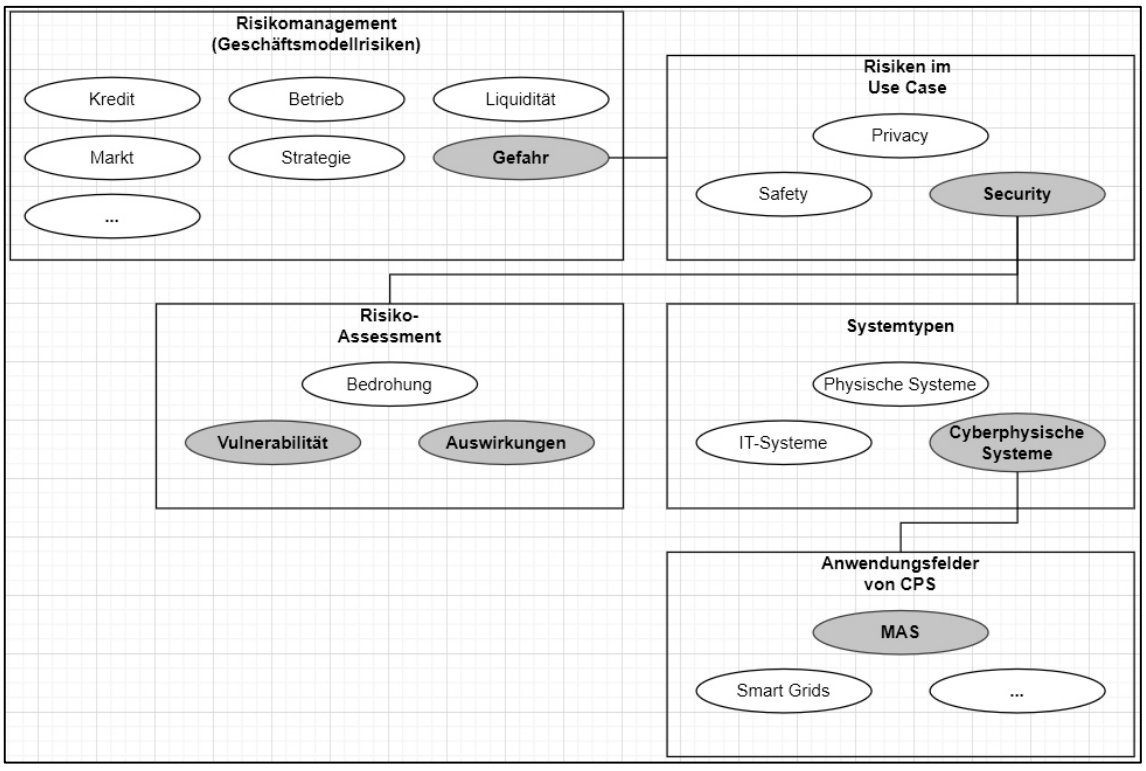


Abbildung 1: Kontextuelle Einordnung der Risikobewertung von MAS.
Quelle: Eigene Darstellung in Anlehnung an Garcia (2005, S. 3).

1.1 Problemstellung

Produktgestaltungsprozesse laufen allgemein über Pflichtenhefte, in denen Anforderungen an das Design hinterlegt sind. Richtlinien tragen dazu bei, technisch-funktionale und Sicherheitsanforderungen zu konkretisieren sowie die Komplexität, die mit dem Einsatz von CPS einhergeht (Möller et al., 2019, S. 10), beherrschbar zu machen (Schwerdtfeger, 2018, S. 35; Macher et al., 2020a). In ihnen wird definiert, was seitens der Produktentwicklung und aufseiten des Qualitätsmanagements getan werden muss, um bestimmte Anforderungen zu erfüllen. Das ist einerseits notwendig, um die Zulassung zum Markt zu erhalten. In den USA ist dafür u. a. eine Produktprüfung gem. den in 47 CFR Part 15.247 (U.S. Government Publishing Office, 2010) und RSS 247 (Government of Canada, 2017) genannten Anforderungsspezifikationen durchzuführen. Andererseits kann die Compliance mit Richtlinien von Kunden und Stakeholdern gefordert werden. Die Einhaltung ist auch ein Gütesiegel für einen Anbieter und es können Wettbewerbsvorteile gegenüber der Konkurrenz entstehen (BSI, 2016). Security ist ein Qualitätsmerkmal, das ein Unique-Selling-Point für Anbieter sein kann (Wurm, 2022, S. 37).

Ebenso können Produktentwickler anhand von Richtlinien Sicherheits- und Qualitätskriterien schon im frühen Produktgestaltungsprozess berücksichtigen. Für den Geltungsbereich Entwicklung und Herstellung von Schließsystemen ist der Tier-1-Automobilzulieferer WITTE Automotive beispielsweise nach IATF 16949 (IATF, 2016) und ISO 9001 (DIN e.V., 2015b) zertifiziert, wobei regelmäßig durchgeführte Audits die Compliance prüfen. Der digitale Satellit der WITTE Automotive Unternehmensgruppe, WITTE Digital, entwickelte eine Nachrüstlösung namens flinkey für After-Market-Fahrzeuge, um Ressourcen durch den Einsatz eines digitalen Schlüssels flexibel teilen zu können (Flinkey.de, 2021). Bisher orientiert sich die Prüfung des physischen Produkts weitestgehend an Safety-Richtlinien, beispielsweise IEC 62368 (IEC, 2021). Bei flinkey handelt es sich jedoch um ein cyberphysisches Produkt, das neben Hardware auch Firmware, Software und Cloud-Komponenten hat.

Mit der Entwicklung cyberphysischer Produkte geht die Herausforderung einher, physische Sicherheitsmerkmale und IT-Sicherheitsmerkmale zusammenzubringen (Lyu et al., 2020; Möller et al., 2019, S. 304-305). Die Merkmale in den Domänen Functional Safety, physische Sicherheit und IT-Sicherheit werden unterschiedlich bewertet, z. B. anhand verschiedener quantitativer, semi-quantitativer und qualitativer Kriterien. Die Bewertungskriterien und Vorgehensweisen sind daher nicht kompatibel (Cert, 2022; Kriaa et al., 2015). Die Berücksichtigung von Functional Safety-Anforderungen, die in dieser Arbeit nicht betrachtet werden, sowie Security-Anforderungen und die Abwägung von widersprüchlichen Anforderungen stellen eine große Herausforderung für OEM und Zulieferer in der Produktentwicklung dar (Möller et al., 2019, S. 269, 308). „Das Abwägen und Ausloten, wieviel Security geradeso ausreichend für die Sicherheit und Zuverlässigkeit des Produkts ist, aber sich noch im zeitlichen und finanziellen Rahmen befindet, ist eine Gratwanderung“, wird von Wurm (2022, S. 37) herausgestellt.

Komplizierter wird die Abwägung, wenn es zu Wechselwirkungen zwischen Sicherheitsfunktionen kommen kann. „[Die] stringenten Echtzeitanforderungen und die knappen Speichergrößen und Bandbreiten eingebetteter Systeme [stehen] oftmals im Widerspruch zum Ressourcenbedarf von Securityfunktionen“, wird in Wurm (2022, S. 38) erklärt. Es gibt jedoch bisher kein formales Security-Modell für CPS, das die Security in einem einheitlichen Rahmen behandelt, welcher sich mit Hardware-Bedrohungen, Netzwerk-Bedrohungen, physischen Bedrohungen und Software-Bedrohungen befasst (Möller et al., 2019, S. 318). Die Zusammen-

führung der Domänen Physical Security und IT Security erfordert neue Ansätze zur domänenübergreifenden (hier: cyberphysischen) Bewertung.[1] Um cyberphysische Anforderungen im Entwicklungsprozess implementieren zu können, stellt sich folglich die Frage nach einer geeigneten Metrik zur domänenübergreifenden Sicherheitsbewertung (Macher et al., 2020a; siehe die Einordnung in Abbildung 2).

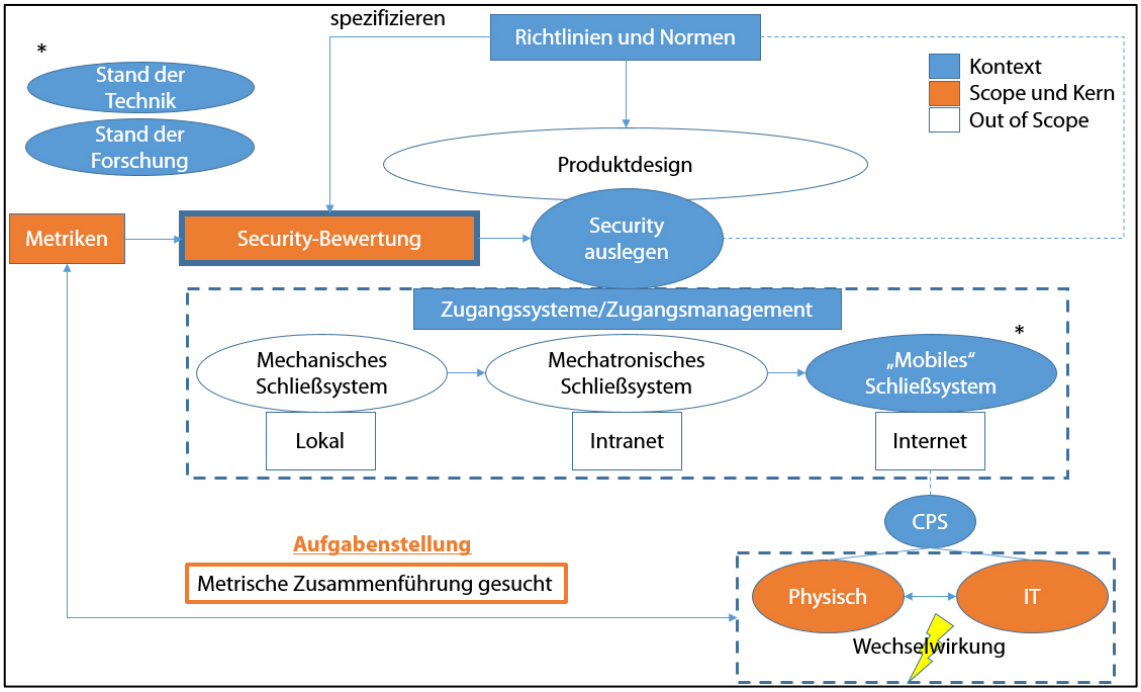


Abbildung 2: Einordnung der Forschungsarbeit.
Quelle: Eigene Abbildung.

In existierenden Standards, wie z. B. IEC TR 63069 (IEC, 2019) oder DIN ISO/TR 22100 (DIN e.V., 2014), wird das Problem der metrischen Angleichung von quantitativen und qualitativen bzw. semi-quantitativen Ansätzen abstrakt beschrieben. Eine Lösung zur metrischen Angleichung oder auch Zusammenführung von Sicherheitsmetriken wird weder in der IEC TR 63069 noch in der DIN ISO TR 22100 beschrieben. Das ist aus Produktentwicklersicht ein Problem, weil die erforderliche Vorgehensweise zur Risikobewertung, die i. d. R. durch Vorgaben aus Richtlinien und Standards bereitgestellt und in Produktentwicklungsprozessen implementiert wird, für die im vorliegenden Fall domänenübergreifende Risikobewertung unzureichend gegeben ist (Macher et al., 2020a). Dabei würden Vorgaben in diesem Zusammenhang dazu beitragen, klare Leitplanken für die Produktentwicklung zu setzen.

[1] Erste Ansätze werden im Fachausschuss 512 „Safety und Security" des Vereins Deutscher Ingenieure (VDI) diskutiert, der unter umfangreicher Industriebeteiligung aus den Disziplinen Automotive, Luftsicherheit, maritime Sicherheit, u. w. von Univ.-Prof. Dr.-Ing. Kai-Dietrich Prof. Wolf geleitet wird (Sicherungssysteme, 2021).

1.2 Herausforderungen

Bei cyberphysischen Strukturen, in denen physische Komponenten und IT-Komponenten enthalten sind, treffen zwei Paradigmen aufeinander, welche in beiden Domänen jeweils in unterschiedlichen, domänenspezifischen Ansätzen zur Risikobewertung aufgegangen sind (Macher et al., 2020a). In Macher et al. (2020a) werden die Hürden bei der Produktentwicklung unter Berücksichtigung von Sicherheitsaspekten aus zwei Domänen folgendermaßen benannt: „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). Sowohl in der physischen Sicherheit als auch in der Functional Safety werden quantitative Metriken zur Risikobewertung verwendet. Bei der physischen Sicherheit wird z. B. in Lichte et al. (2016) die Wahrscheinlichkeit, dass ein Angreifer schneller ein Asset[2] erreicht als der Verteidiger den Angreifer, als Bewertungskriterium für die Vulnerabilität herangezogen. Bei der Analyse des Zeitspiels zwischen der Eindringzeit eines Angreifers und der Reaktionszeit eines Verteidigers gibt es einen klar definierten Wirkmechanismus, bestehend aus Protektion, Observation und Intervention.

In der Functional Safety ist der Bewertungsmaßstab (insbesondere für Hardware) eine Ausfallrate einer Systemkomponente über eine konkrete Zeitspanne (Lichte et al., 2017; Wurm, 2022, S. 70). Die den Disziplinen Physical Security und Functional Safety zugrundeliegenden Metriken beruhen auf einer zeitbezogenen Wahrscheinlichkeit, die sich auf physikalische Prozesse und Zustände bezieht (Macher et al., 2020a). In der IT-Sicherheit ist es üblich, Scores zur Bewertung zu verwenden, da eine darunterliegende Zeitmetrik und ein objektiver Wirkmechanismus zur Bewertung der Schutzwirkung von Maßnahmen fehlen (Yee, 2013, S. 8; Jacobs et al., 2019; Pohlmann, 2015). In Newsome (2013) wird der Einsatz von Scoring-Systemen auf folgende Weise begründet: „[…] 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, S. 102). Ein Scoring bietet für Anwender einen Vorteil gegenüber komplizierten Berechnungen, wenn es intuitiver und einfacher ist, Risiken zu bewerten. Das setzt voraus, dass mit Scorings reale Risiken auch abgebildet werden können (Gigerenzer, 2014, S. 140).

Gängige IT-Sicherheitsmetriken sind klassischerweise qualitativ und semi-quantitativ. Sie bilden die Prozesse nicht wie in der physischen Sicherheit oder in der Functional Safety ab. Die Grundsätze in der IT-Security unterscheiden sich von denen in der physischen Security: In der IT können sowohl physische Zugangspunkte (z. B. Hardware in Serverräumen) als auch digitale Zugangspunkte (z. B. Netzwerkknoten) genutzt werden, um zu einem Daten-Asset zu gelangen (Wheeler, 2011, S. 18). Ein IT-Angreifer kann bekannte Schwachstellen ausnutzen. Zur Erzielung einer Kompromittierung können jedoch auch Schwachstellen ausgenutzt werden, die einem Betreiber unbekannt sind, sog. Zero Days (z. B. Implementierungsfehler) (BSI-Glossar, 2022). In der physischen Security wird ein Angreifer entlang eines bekannten Pfades geführt, der durch die Platzierung von Barrieren und deren Öffnungen bestimmt wird (Garcia, 2005, S. 39).

Darüber hinaus beruht die Verwendung von Wahrscheinlichkeiten in der IT-Sicherheit auf einer anderen Interpretation als in der physischen Sicherheit oder in der Functional Safety. In der IT bedeutet Wahrscheinlichkeit zum Beispiel die Möglichkeit, dass eine Schwachstelle im System ausgenutzt werden kann (Braband, 2019), oder dass z. B. 90 % aller öffentlich bekann-

[2] Nach ISO/SAE 21434 ist ein Asset „[an] object that has value, or contributes to value" (ISO/SAE, 2021b, S. 1).

ten Schwachstellen identifiziert und geschlossen werden können (Jones, 2007). In der physischen Sicherheit hingegen bedeutet Wahrscheinlichkeit, dass ein Angreifer beispielsweise in 65 % der Fälle 30 Sekunden braucht, um eine Barriere zu überwinden (Lichte et al., 2019). In der Functional Safety wird Wahrscheinlichkeit auf den Ausfall einer Komponente in einem definierten Zeitfenster bezogen (Zio, 2007, S. 50). In allen drei Fällen handelt es sich um Wahrscheinlichkeiten. Diese Wahrscheinlichkeiten passen aber nicht richtig zusammen.

In der physischen Sicherheit wird das Risiko auf der Grundlage der Auswirkungen, der Bedrohung und der Vulnerabilität, beschrieben und durch das Zusammenspiel von Protektion, Observation sowie Intervention, bewertet (Lichte et al., 2016). Es werden Szenarien betrachtet, die noch nicht eingetreten sind oder für die kaum historische Daten vorliegen (Lichte et al., 2017). Der Mangel an historischen Daten liegt darin begründet, dass Worst-Case-Szenarien, wie sie in der physischen Sicherheit betrachtet werden, in der Vergangenheit selten bis gar nicht aufgetreten sind. Deswegen sind statistische Abschätzungen und damit die Angabe absoluter Wahrscheinlichkeitswerte nicht möglich. Die Bestimmung der Bedrohungswahrscheinlichkeit ist schwierig, weswegen in der Bedrohungsanalyse Bedrohungen in Szenarien zusammengefasst werden, in denen bestimmte Kombinationen aus Wissen, Werkzeug und Angreifertyp sinnvoll und konsistent sind. Solche Szenarien sind durch einen Risikoanalysten zu isolieren, sodass ebendiese mithilfe von Experten mit Eintrittswahrscheinlichen versehen werden können (Witte et al., 2020). Die Modellierung von Szenarienwahrscheinlichkeiten und die Bewertung von Bedrohungsbeiträgen werden in dieser Forschungsarbeit nicht näher betrachtet.

Durch die quantitative Bewertung von Sicherheitsfunktionen im Angriffsfall (das System ist einer Bedrohung ausgesetzt) ist eine Kosten-Nutzen-Optimierung in Bezug auf den Einsatz von Sicherheitsmaßnahmen gegen konkrete Bedrohungsszenarien möglich (Lichte et al., 2019). Diese Annahme kann durch die Argumentation von Krisper (2021) begründet werden:

> 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).

Voraussetzung für die Modellierung und die Bewertung eines Sicherungssystems im Angriffsfall ist die Annahme, dass Bedrohungsanteile disjunkt von Vulnerabilitätsanteilen und von Auswirkungsanteilen sind. In der Realität ist diese Idealisierung nicht gegeben, da z. B. in Bedrohungsanteilen auch Vulnerabilitätsanteile und Auswirkungsanteile innewohnen können (Harnser, 2010, B5, S. 57). Die Attraktivität eines Ziels beispielsweise kann von der möglichen Auswirkung abhängen. Die Vulnerabilität hat aber auch Bedrohungsanteile, weil sie von Bedrohungsszenarien abhängt. In diesem Idealfall wird strenge Unabhängigkeit zwischen den Ereignissen von Bedrohung, Vulnerabilität und Auswirkungen angenommen.

Die physische Vulnerabilität kann auf einer ganz konkreten, wirksamkeitsbezogenen Ebene bewertet werden (Harnser, 2010, B4, S. 47). Einerseits ist eine quantitative Bewertung physischer Vulnerabilität, z. B. mit der Vulnerabilitätsmetrik nach Lichte et al. (2016), möglich. Für die quantitative Vulnerabilitätsbewertung nach Lichte et al. (2016) wird in Anlehnung an Garcia (2005) die Bezeichnung Intervention Capability Metric (ICM) in dieser Arbeit eingeführt. Zur Wahl geeigneter Sicherheitstechnologien erklärt Garcia (2005): „Selection of the appropriate technologies depends on threat capability and motivation" (Garcia, 2005, S. 152). Und weiter: „For an immediate response, neutralization capability and the probability of communication are key performance measures" (Garcia, 2005, S. 250). Mittels der ICM wird bewertet, ob ein Angreifer mehr Zeit zur Überwindung der Barrieren bis zum Asset braucht als ein Verteidiger

zur erfolgreichen Intervention. Es können Unsicherheiten über die Sicherheitsfunktionen eines physischen Systems in Form von Dichtefunktionen für Protektion, Observation und Intervention berücksichtigt werden (Lichte et al., 2021). Das Zusammenspiel der Bestandteile des physischen Wirkmechanismus wird typischerweise für eine einzige Bedrohung aufgestellt. Die Mittelwerte und Standardabweichungen einer Dichtefunktion, bei der beispielsweise eine Normalverteilung zugrunde gelegt wird, können sich jedoch ebenso auf ein Set mehrerer Bedrohungen beziehen. Der schwächste Pfad des Sicherheitssystems bestimmt in diesem Kontext die physische Vulnerabilität des betrachteten Systems, weil angenommen wird, dass der Weg eines Angreifers ungewiss ist (Lichte et al., 2016).

Andererseits gibt es in der physischen Sicherheit auch Scoring-Systeme. Ein Beispiel dafür ist die Harnser-Metrik aus der Performance Risk-based Integrated Security Methodology (PRISM) nach Harnser (2010). In der Harnser-Metrik werden die Parameter Protektion, Detektion und Intervention von Experten mit Werten zwischen „1" (niedrig) und „5" (hoch) bewertet. Die Bezeichnung der Bewertungsparameter in Harnser (2010) ist eine andere als in Lichte et al. (2016). In der Harnser-Metrik wird für die zweite Bewertungsgröße der Begriff „Detektion" verwendet. In Lichte et al. (2016) findet die Bezeichnung „Observation" Anwendung. Detektion ist gem. der ICM nach Lichte et al. (2016) ein Bewertungsparameter, der sich aus Observations- und Protektionsanteilen zusammensetzt, d. h. es handelt sich um ein zusammengesetztes Ereignis (Lichte et al., 2016). Demzufolge würde die Protektion zweimal in die Vulnerabilitätsbewertung nach Harnser einbezogen werden: Einmal über die Bewertung der Protektion und einmal über Bewertung der Detektion. Grundsätzlich ist zu hinterfragen, ob Experten in der Lage sind, Bewertungsgrößen, welche sich aus mehreren Parametern zusammensetzen, direkt zu bewerten. Die Vulnerabilität beispielsweise kann ohne eine Vulnerabilitätsmetrik schwerlich durch Experten direkt eingeschätzt werden. Es ist vielmehr erforderlich, die Vulnerabilitätsbestandteile gem. der verwendeten Vulnerabilitätsmetrik zu bewerten, sodass als Output der Vulnerabilitätsmetrik ein Vulnerabilitätswert resultiert. Daher ergibt es mehr Sinn, den Bewertungsparameter „Detektion" in „Observation" umzubenennen.

Die Scores der Bewertungsgrößen Protektion, Detektion und Intervention werden in der Harnser-Metrik anschließend zu einem Vulnerabilitäts-Score addiert. Dies führt zu Abweichungen im Vergleich zur ICM: Liegt die Protektion beispielsweise bei „3" (moderate Auslegung), die Detektion bei „1" (Minimalauslegung) und die Intervention bei „5" (Maximalauslegung), dann ist die Vulnerabilitätsbewertung nach Harnser (2010) im mittleren Bereich (Wert „9"). Gemäß der ICM ist das System unter diesen Bedingungen in hohem Maße vulnerabel, wenn folgende Annahmen vorliegen (Lichte et al., 2016)[3]:

- Die Kombination von Protektion und Observation an Barrieren ist notwendig, da ein Angreifer immer in der Lage ist, eine Barriere zu durchbrechen, wenn er unendlich viel Zeit hat, ohne entdeckt zu werden.
- Die Detektion eines Angriffs ist nur möglich, wenn die Protektion ausreichend ist, um einen Durchbruch bis zur Detektion zu verhindern.
- Nach der Detektion kann ein Angriff nur dann gestoppt werden, wenn der verbleibende Schutz entlang des verbleibenden Angriffspfades lange genug anhält, um den Angreifer bis zum Abschluss der Intervention daran zu hindern, das Asset zu erreichen.

Die Harnser-Metrik sagt nicht, wie Detektions-Score „1" zu Detektions-Score „5" steht (ist Score „5" fünfmal so gut wie Score „1"?). Die Metrik liefert keine Informationen darüber, weil die Scores lediglich Ordinalwerte sind, d. h. Werte ohne absolute Bezugnahme auf die Größe. Vulnerabilitäts-Score-Werte bei Harnser unterhalb der „3" oder Zwischenwerte sind undefiniert,

[3] Unter Berücksichtigung der drei genannten Annahmen für die ICM ist stets ein gewisses Zusammenspiel der Protektion, Observation und Intervention erforderlich, um eine Schutzwirkung zu erzielen.

so z. B. Scores zwischen „4“ und „5“. Ein ähnliches Phänomen zeigt sich auch bei anderen semi-quantitativen Metriken. Ein Beispiel dafür ist die Fehlermöglichkeits- und Einflussanalyse (FMEA) (Braband, 2003; Braband, 2004): Es werden die drei Parameter Auftreten, Bedeutung und Entdeckung zwischen „1“ (niedrig) und „10“ (hoch) gescort. Daraufhin werden die Scores miteinander multipliziert. Das Produkt von Auftreten, Bedeutung und Entdeckung ist die sog. Risikoprioritätszahl (Risk Priority Number, RPN). Der höchste erreichbare Wert ist die (10 x 10 x 10 =) „1000“ (maximales Risiko), der nächstkleinere Wert ist dagegen die „900“ (10 x 10 x 9). Wird anstelle der maximalen Ausprägung die minimale Ausprägung betrachtet, dann fällt auf, dass das Risiko bei kleinen Scores anders skaliert als bei großen. Das kleinste Risiko ist hierbei (1 x 1 x 1 =) „1“, das nächsthöhere (1 x 1 x 2 =) „2“.

Die Distanz zwischen diesen beiden Scores beträgt scheinbar „1“, bei den zwei obersten Werten dagegen „100“. Da es sich um einen semi-quantitativen Ansatz mit einer Ordinalskala handelt, fehlt jedoch ein Bezugspunkt, der eine Verhältnismäßigkeit erlauben würde. Das FMEA-Scoring suggeriert, dass das Risiko bei hohen Scores anders skaliert als bei niedrigeren Scores (Braband, 2004). Ob das tatsächlich realen Gegebenheiten entspricht, muss kritisch hinterfragt werden (Krisper, 2021). Zudem kann bei der FMEA nicht die volle Bandbreite an möglichen Ergebniswerten zwischen „1“ und „1000“ erzielt werden. Der Ergebnisraum ist durch die gegebenen Parameterkombinationen und die zugrunde gelegte Rechenvorschrift restringiert. In Braband (2003) werden die systemischen Schwächen der FMEA folgendermaßen zusammengefasst:

- Auftreten, Bedeutung und Entdeckung sind Merkmale auf einer ordinalen Skala, weswegen die Multiplikation mathematisch nicht definiert ist.
- Ähnliche Risiken sollen dieselbe RPN zugewiesen bekommen. Bei der FMEA kann das nicht gewährleistet werden.
- Risiken mit derselben RPN werden nicht in gleichem Maße akzeptiert.

Folgende drei Forderungen werden in Braband (2012) an eine Risikoskala zur Ermittlung der RPN gestellt:

> Rational scaling: The scaling of the evaluation tables must be at least approximately rational, i.e. the bandwidths b of the classes should be approximately equal. Monotonicity: If the risk for scenario i is 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, S. 216-217).

Die Harnser-Metrik differenziert zum einen nicht zwischen einzelnen Barrieren, wie es die ICM tut. Zum andern werden Protektion, Detektion (bzw. nun Observation) und Intervention als gleichwertig interpretiert. Das ist nicht der Fall, wie die folgenden Erklärungen zeigen: Angenommen, die Protektion ist im Idealfall 100 % und es gibt keine Observation und keine Intervention[4]. Das würde bedeuten, dass jeder Angreifer aufgehalten werden kann. In diesem Fall ist das betrachtete System gem. der ICM zu 0 % vulnerabel. 100 % Protektion entspricht einer idealen Barriere, die ohne Observations- und Interventionsanteile auskommt. Mit nur einem Harnser-Protektions-Score „5“ (maximale Protektion)[5] würde vermutet werden, die Vulnerabilität liegt im Mittelfeld. Wenn es keine Protektion und keine Intervention gibt[6], sondern nur

[4] Ein solcher Extremfall ist eher unrealistisch, weil null Observation bedeutet, dass beliebige (schwere, laute, auffällige) Angriffsmittel möglich sind. Die aufgeführten Beispiele sollen zeigen, dass Protektion, Observation und Intervention nicht gleichwertig sind.
[5] Gedanklich würden Observation und Intervention jeweils den Score „0“ annehmen.
[6] Gedanklich würden hier Protektion und Intervention den Score „0“ annehmen.

eine 100 %-ige Observation, dann wird diese Konstellation nach der ICM zu maximaler Vulnerabilität führen, weil zwar jeder Angreifer erkannt, aber nicht aufgehalten wird. Die Harnser-Score-Summe (0 + 5 + 0 =) „5" attestiert in solch einem Falle ein Maß an Sicherheit, welches nicht vorhanden ist. Eine 100 %-ige Intervention ohne Protektion und ohne Observation ist unsinnig, da zwar theoretisch alle Angreifer aufgehalten werden können. Sie werden jedoch vorher nicht als solche erkannt.

Bestmögliche Protektion kann für sich alleine stehen, um theoretisch 0 % Vulnerabilität zu erzielen. Observation und Intervention können es dagegen nicht. Wenn es keine Protektion gibt, dafür aber z. B. 100 % Observation und 100 % Intervention im Verbund, dann ist das System wie bei dem Fall „nur 100 % Protektion" zu 0 % vulnerabel. Observation und Intervention zusammen könnten schlussfolgernd ohne Protektionsanteile wirksam sein. Die Harnser-Score-Summe von „10" (0 + 5 + 5) liegt jedoch erneut im Mittelfeld. Weitere Probleme bei der Verwendung semi-quantitativer Ansätze im Vergleich zu quantitativen Ansätzen werden z. B. in Krisper (2021), Braband (2004), Braband (2008), Braband (2009), Braband (2016), Termin et al. (2021), Ahmed (2019) und Hubbard et al. (2016, S. 85-95) aufgezeigt. In Krisper (2021) werden insgesamt 24 Probleme bei der Anwendung semi-quantitativer Metriken im Vergleich zu quantitativen Ansätzen diskutiert, u. a. „ordinal scales, semi-quantitative arithmetics, range compression, risk inversion, ambiguity, and neglection of uncertainty" (siehe Abbildung 3).

In der IT-Sicherheit fehlt ein objektiver Wirkmechanismus zur Bewertung der Sicherheitsfähigkeit eines Systems (Jacobs et al., 2019). Ohne eine quantitative Metrik mit objektiv bewertbarem Wirkmechanismus kann ein Scoring-System nicht so angepasst werden, dass reale Risikoeinstufungen resultieren (Krisper, 2021). Eine international verwendete Metrik in der IT-Security ist das Common Vulnerability Scoring System (CVSS) in der Version 3.1, kurz v3.1 (First.org, 2022). Vulnerabilität wird beim CVSS über den Grad der Ausbeutbarkeit (Exploitability) einer systeminhärenten Schwachstelle bewertet. Ein Exploitability-Score wird anhand der Szenario-beschreibenden Parameter Attack Vector (AC), Attack Complexity (AC), Privileges Required (PR) und User Interaction (UI) berechnet: Numerische Werte werden zu den Ausprägungen eines jeden Parameters geordnet, beispielsweise „AV – Physical – 0.2", „AC – High – 0.44", usw., und über einen multiplikativen Zusammenhang, der der Exploitability-Bewertung nach CVSS zugrunde liegt, miteinander verknüpft. Der numerische Wert einer jeden Bewertungsgröße liegt jeweils zwischen 0 und 1 und stellt einen Exploitability-Beitrag dar. Je höher diese Zahl, so die Annahme, desto ausbeutbarer ist das betrachtete System. Der Exploitability-Score kann gem. ISO/SAE 21434 (ISO/SAE, 2021b, S. 47) einer Attack Feasibility Kategorie bzw. nach Braband (2019) einer Likelihood-of-Exploitability-Kategorie (LoE) zugeordnet werden.

Exploitability bezieht sich auf die Wahrscheinlichkeit, dass ein böswillig motivierter Angreifer eine Systemschwachstelle ausnutzen kann, um entweder eine unerwünschte Aktion auszuführen oder ein Asset anzugreifen (First.org, 2022). Eine hohe Exploitability bedeutet, dass eine Schwachstelle leichter als eine Schwachstelle mit niedriger Exploitability ausgenutzt werden kann. Mit der Attack Feasibility (Ausführbarkeit eines Angriffs) wird die Wahrscheinlichkeit bewertet, dass ein Angreifer einen erfolgreichen Angriff auf ein System durchführen kann. Nun kann argumentiert werden, dass ein System erfolgreich angegriffen werden kann, wenn es mindestens eine Schwachstelle gibt, welche ausbeutbar ist. In der ISO/SAE 21434 (ISO/SAE, 2021b, S. 47) wird vorgeschlagen, eine der drei folgenden Ansätze als Methode für das Attack Feasibility Rating heranzuziehen:

1) Attack potential-based approach (Bewertungsparameter: elapsed time, specialist expertise, knowledge of the item or component, window of opportunity, equipment).
2) CVSS-based approach (Bewertungsparameter: attack vector, attack complexity, privileges required, user interaction).

3) Attack vector-based approach (Bewertungsparameter: vorherrschender Angriffskontext; z. B. physical, local, adjacent, network).

Die Anwendung des CVSS-basierten Ansatzes ist eine Möglichkeit zur Bewertung der Exploitability. Die Bewertung der Exploitability-Beiträge mit dem CVSS resultiert in einem Exploitability-Value, welcher in der ISO/SAE 21434 einer Attack-Feasibility-Kategorie zugewiesen wird (ISO/SAE, 2021b, S. 69). In Braband (2019) beispielsweise wird ein Exploitability-Score einer Likelihood-of-Exploitability-Kategorie (LoE) zugeordnet. Auf Basis der vorangegangenen Ausführungen können LoE bzw. Exploitability und Attack Feasibility gleichgesetzt werden. Beim CVSS werden neben der Exploitability auch die Auswirkungen (Impacts), bestehend aus der Schutzzielverletzung der Vertraulichkeit, Verfügbarkeit und Integrität, zur Ermittlung eines Vulnerability-Scores herangezogen. Im engeren Sinne erzeugt das CVSS im Ergebnis keinen Vulnerabilitäts-Score, weil Vulnerabilitätsanteile und Auswirkungsanteile miteinander verknüpft werden. Würde das CVSS zusätzlich zu der Bewertung von Vulnerabilität und Auswirkungen eine Metrik zur Bewertung von Bedrohungen beinhalten, könnte das Ergebnis des CVSS als Risiko-Score interpretiert werden.

In Braband (2019) wird vorgeschlagen, die CVSS-Score-Werte zu logarithmieren. Das wird getan, um die CVSS-Metrik zur Bewertung der Exploitability in einen semi-quantitativen Scoring-Ansatz zu überführen. Die Logarithmierung von Werten ist eine Standardmethode in der Statistik (Gneiting & Raftery, 2004; Field, 2003, S. 203). Bei der Transformation dürfen nur Formeln verwendet werden, die die Reihenfolge der Datenpunkte nicht vermischen. Das ist notwendig, um die relativen Unterschiede zwischen Ausprägungen einer Variable beizubehalten. Transformiert werden können Daten z. B. auch über eine (Quadrat-)Wurzelfunktion, über die Addition einer Konstante, über die Bildung des Kehrwerts (reziproke Transformation) oder über das Reverse-Scoring. Beim letztgenannten Ansatz wird jeder Score-Wert von dem Maximum abgezogen (Field, 2013, S. 201-210).

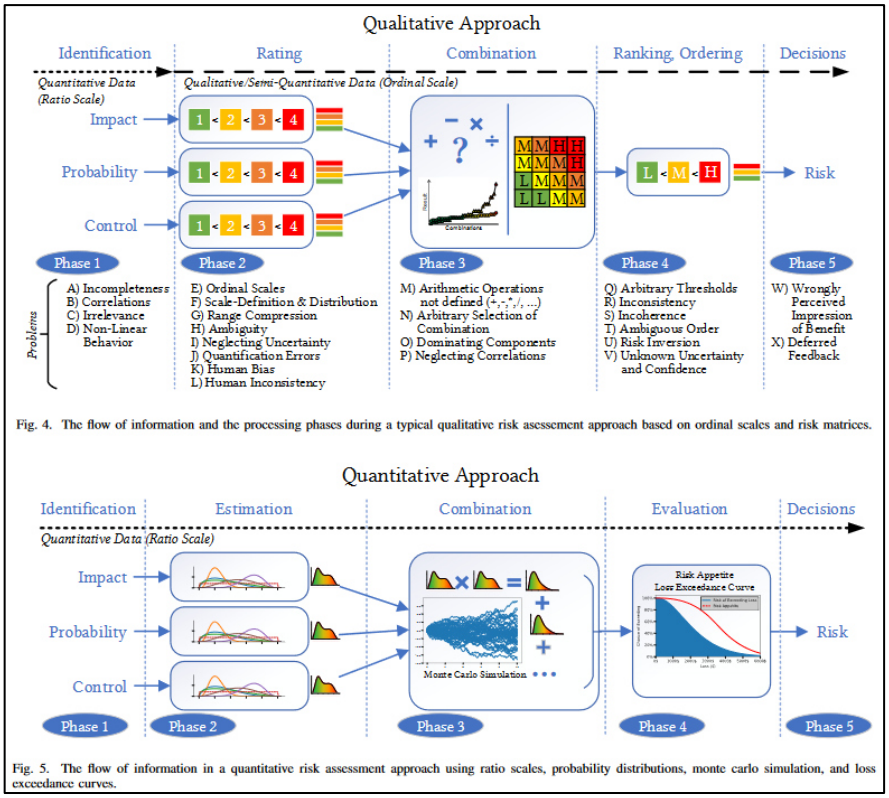


Abbildung 3: Phasen des semi-quantitativen und quantitativen Assessments. Quelle: Krisper (2021).

Bei der Umwandlung von Daten wird allgemein zwischen der linearen Transformation und der nichtlinearen Transformation unterschieden (Lehn et al., 2000). Bei einer linearen Transformation wird eine lineare Funktion auf jeden Zahlenwert des Datensatzes angewendet, z. B. unter Einsatz der allgemeinen Formel „y = a·x + b". Das „y" ist der transformierte Wert, das „a" beschreibt den Skalierungsfaktor, „x" ist der Ursprungswert und „b" bezeichnet den Verschiebungsfaktor. Arten linearer Transformationen sind z. B. die Skalierung (Multiplikation der Werte des Datensatzes mit einer Zahl) oder die Translation (Addition der Werte des Datensatzes mit einer Zahl). Eine in der Statistik verbreitete lineare Transformation ist die z-Transformation, auch Standardisierung genannt. Daten werden hier derart normalisiert, dass sie in eine Standardnormalverteilung mit dem Mittelwert von 0 und der Standardabweichung von 1 überführt werden (Tachtsoglou et al., 2017, S. 111-125).

Eine Erweiterung der z-Transformation ist die Robust-Scaler-Methode, die robust gegenüber Datenausreißern ist (Brownlee, 2020; Eddie, 2021). Der neue, normalisierte Werte wird mittels „X_neu = (X – Q2) / (Q3 – Q1)" bestimmt. „X" beschreibt den Ursprungswert, „Q1" bis „Q3" bezeichnen die Quartile der Datensätze: „Q1" teilt einen Datensatz in die untersten 25 %, „Q2" (Median) in die mittleren 50 % und „Q3" in die obersten 25 % der Daten. Bei der nichtlinearen Transformation wird ein Datensatz auf eine andere Skala übertragen. Die Funktion, die auf den Datensatz angewendet wird, ist entsprechend nichtlinear, d. h. die „Ausgabe" ist nicht proportional zur „Eingabe". Beispiele für nichtlineare Transformationen sind die Box-Cox-Transformation (Daten werden in eine Normalverteilung transformiert, siehe Box & Cox (1964)), und die log-Transformation (Daten werden auf eine logarithmische Skala gebracht, siehe Keene (1995)). Die log-Transformation wird klassischerweise verwendet, wenn vermutet wird, dass ein Wachstumsprozess mit einer schief verteilten oder nichtlinearen Struktur vorliegt. Mit der Logarithmierung kann ein multiplikativer Zusammenhang in einen additiven Zusammenhang überführt werden (Gneiting & Raftery, 2004). Es kann also eine nichtlineare Wachstumsfunktion in lineare Wachstumsstufen überführt werden. Bei der Logarithmierung kann ein künstlicher Nullpunkt grundsätzlich beliebig gesetzt werden, wobei die Basis, zur der logarithmiert wird, die Dimensionierung definiert. Bei der Bestimmung der Exploitability (E) nach CVSS wird ein multiplikativer Zusammenhang vermutet (E = 8.22 · AV · AC · PR · UI) (First.org, 2022).[7]

Zudem wird ein Barriere-basierter Ansatz auf das CVSS angewendet, der einen Defense-in-Depth-Effekt (DiD) postuliert (Braband, 2019). Bei DiD wird angenommen, dass jede Barriere Implementierungsfehler aufweist und jede weitere Barriere die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert (Schnieder et al., 2018, S. 24-25). In der IT-Security fehlt jedoch ein objektiver Wirkmechanismus zur Bewertung der Überlegungen des vorgeschlagenen Scoring-Systems. Deswegen wird in Termin et al. (2022) vorgeschlagen, die Überlegungen aus der IT-Security-Bewertungen in der physischen Security-Bewertung zu emulieren. Die Emulation bringt jedoch keine eindeutigen Ergebnisse hervor, ob es Besserungen bringt, die Anzahl der Barrieren in der physischen Vulnerabilitätsbewertung zu berücksichtigen. Aus der vorangegangenen Darlegung ergeben sich die Fragen:

- Inwiefern kann eine domänenübergreifende Sicherheitsbewertung von Physical Security und IT Security funktionieren?
- Wie können Inkompatibilitäten[8] zwischen der semi-quantitativen Harnser-Metrik und der quantitativen ICM aus der physischen Sicherheit objektiv nachgewiesen werden? Unter

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

[8] Mit Inkompatibilität ist gemeint, dass zwei Metriken bzw. die Ergebnisse auf Basis der Metriken nicht zusammenpassen. Inkompatibilitäten zwischen zwei Sicherheitsmetriken sind z. B. vorzufinden, wenn den Ausprägungen der jeweiligen Risikostufen der Metriken unterschiedliche objektive Risikobeträge zuzuordnen sind. Beispiele für Inkompatibilitäten sind ferner unterschiedliche Definitionen und Interpretationen von Messgrößen, unterschiedliche Skalen, unterschiedliche Messmethoden, Messzeitpunkte sowie unterschiedliche Einheiten (Kan, 2002, S. 219-226).

welchen Randbedingungen können diese Inkompatibilitäten reduziert werden? Welche Forderungen sind zur Ermöglichung einer Angleichung zu stellen?
- Wie können Verwerfungen[9] innerhalb der Harnser-Metrik und innerhalb der CVSS-Metrik reduziert werden?
- Wie können die Harnser-Metrik aus der physischen Sicherheit und die CVSS-Metrik aus der IT-Sicherheit aneinander angeglichen werden?
- Wie können Sicherheitslevel in den Domänen Physical Security und IT-Security aufeinander (ebenso unter Berücksichtigung von Wechselwirkungen) abgestimmt werden?

Die aufgeworfenen Fragen regen zur Betrachtung an, wie zwei Metriken aus den Domänen physische Sicherheit und IT-Sicherheit angeglichen, von Verwerfungen befreit und in einer domänenübergreifenden Risikobewertung zusammengeführt werden können, die nicht auf dem demselben physikalischen Prozess beruhen, unterschiedliche Einflussgrößen beschreiben und wo es Wechselwirkungen zwischen beiden Domänen geben kann. Die Wechselwirkungen müssen auf Basis von Expertenaussagen abgebildet und an einzelnen Stellen punktuell verknüpft werden. Diese Verknüpfungen müssen gleichzeitig im Gesamtzusammenhang konsistent sein und auch mit einer bestimmten Wahrscheinlichkeit versehen werden können, sodass Vulnerabilität im Idealfall auf quantitativem Wege berechnet werden kann. Aufgrund der genannten Herausforderungen muss die Risikobewertung von automobilen Produkten sorgfältig durchdacht werden, um Anwendern einen Methodenbaukasten an die Hand zu geben, mit dem die risikogerechte Verteilung von knappen Ressourcen in Sicherheitsmaßnahmen unterstützt werden kann.

1.3 Zielsetzung

Ziel dieser Forschungsarbeit ist es, ein Rahmenwerk zur Durchführung einer domänenübergreifenden Bedrohungsanalyse und Risikobewertung zu entwickeln, welches sich an gängigen Automotive-Standards orientiert. Auf Basis des erarbeiteten Ansatzes sollen Anwender aus der industriellen Praxis befähigt werden, sowohl domänenspezifische Security-Risikobewertungen als auch domänenübergreifende Security-Risikobewertungen von MAS-Anwendungen durchzuführen. Grundlage dafür soll die Konzentration auf die Vulnerabilität von Sicherungstechnologien sein, welche in MAS eingesetzt werden. Für die Beschreibung der physischen Eigenschaften sollen Wahrscheinlichkeiten für die Vulnerabilität auf Basis von Angreifereigenschaften ermittelt werden können. Für die Beschreibung von IT-Eigenschaften sollen auch auf Basis von Angreifereigenschaften vermutete Wahrscheinlichkeiten für die Ausbeutbarkeit (Exploitability) ermittelt werden können.[10] Es soll darüber hinaus eine Vorgehensweise geben, um Expertenwissen in die Metrik einzuspeisen, die dem Bewertungsschema aus der physischen Sicherheit bzw. aus der IT-Sicherheit zugrunde liegt. Die favorisierte Lösung für die probabilistisch konsistente Zusammenführung der physischen Sicherheitsbewertung und der IT-Sicherheitsbewertung ist die Überführung der Sicherheitsbewertungen in Bayes'sche Netze.

Um an das Ziel der Forschungsarbeit zu gelangen, wird eine cyberphysische Bedrohungsanalyse und Risikobewertung vorgeschlagen, die auf bekannte Standards und Ansätze zur physischen Vulnerabilitäts- und IT-Exploitability-Bewertung aufbaut sowie in Teilen auf Methoden der mathematischen Statistik und Wahrscheinlichkeitstheorie beruht. Zuvorderst soll mittels

[9] Verwerfungen umfassen Metrik-inhärente Probleme und Unstimmigkeiten. Sie treten nur innerhalb einer Metrik auf und nicht zwischen Metriken. Verwerfungen sind z. B. die Nicht-Berücksichtigung relevanter Faktoren bezogen auf den zu untersuchenden Sachverhalt, fehlerhafte Daten oder subjektive bzw. nicht replizierbare Einschätzungen (Kan, 2002, S. 63-69).

[10] Die Bewertungsgrößen in IT-Scoring-Systemen können nicht auf einen objektiven Wirkmechanismus zurückgeführt werden, weil eine quantitative Metrik fehlt. Deswegen wird „vermutete" Wahrscheinlichkeit geschrieben.

einer metrischen Analyse am Beispiel von Metriken aus der physischen Sicherheitsbewertung aufgezeigt werden, wie ein Scoring-System unter Zuhilfenahme einer quantitativen Metrik mit objektivem Wirkmechanismus kalibriert respektive quantitativ konform gemacht werden kann, sodass trotz der unterschiedlichen Metriken gleiche Vulnerabilitätseinstufungen erzielt werden können. Es wird dargelegt, welche Forderungen und Randbedingungen für eine Angleichung von Scoring-basierten Metriken an eine quantitative Metrik zu definieren sind und wie die Güte von Scoring-basierten Bewertungsschemata bewertet werden kann. Darüber hinaus sollen Forderungen an die Ermöglichung einer Angleichung von Metriken aus den Domänen Physical Security und IT Security definiert werden, sodass trotz unterschiedlicher Bewertungen vergleichbare Risikoeinordnungen erzielt werden können. Aufbauend auf den vorangegangenen Teilzielen soll ein Ansatz erarbeitet werden, um domänenübergreifende Wechselwirkungen zwischen IT-Szenarien und physischen Szenarien zu bewerten.

Für die Schaffung einer domänenübergreifenden Sicherheitsmetrik, die mit Industriestandards kompatibel ist, wird die Methode der Szenario-Analyse für die Bedrohungsanalyse und Risikobewertung herangezogen. Das Vorgehen liefert eine Grundlage für die Sammlung von Daten für die Durchführung einer domänenübergreifenden Security-Risikobewertung (Cheng et al., 2014, S. 5). Insgesamt gliedert sich die Bedrohungsanalyse und Risikobewertung im Kern in drei Teile: die Beschreibung der mathematischen Zusammenhänge einer Bewertungsmetrik von physischer Vulnerabilität, IT-Vulnerabilität und cyberphysischer Vulnerabilität. Im dritten Teil sollen Auswirkungen von IT-Security-Bedrohungen auf Überlegungen der physischen Security einbezogen werden. Diese Arbeit stellt einen ganzheitlichen Ansatz vor, um Expertenwissen, Use-Case-spezifische Bedrohungsszenarien und technologische Artefakte sowie Auswirkungen im Falle eines erfolgreichen Angriffs im Rahmen einer cyberphysischen Bedrohungsanalyse und Risikobewertung zu berücksichtigen. Für die Einspeisung von Expertenwissen in die Bedrohungsanalyse und Risikobewertung wird ein Verfahren auf Basis der Delphi- und der Cooke'schen Erhebungsmethode vorgestellt, mit dessen Hilfe Wahrscheinlichkeitsaussagen einzelner Experten zusammengebracht werden können. Die dem vorgeschlagenen Ansatz zugrundeliegende Metrik besitzt insgesamt folgende Eigenschaften:

1. Sie ist modular, d. h. es können beliebige MAS-Konfigurationen und technologische Artefakte bewertet werden.
2. Sie ist für beide Domänen auf Verfahrensebene konsistent aufgebaut.
3. Sie ist so gestaltet, dass der Schutzeffekt von Maßnahmen zur Vulnerabilitätsreduktion abgebildet werden kann.
4. Expertenwissen kann erhoben und in das Bewertungssystem überführt werden.
5. Sie kann einen Vergleich von MAS mit herkömmlichen physischen Zugangssystemen zulassen, da durch den erarbeiteten Ansatz auch eine domänenspezifische Bewertung möglich ist.

Die Metrik leistet einen Beitrag zur Risikobewertung und kann als Baustein eines unternehmerischen Risikomanagements dienen, sodass Risiken von konkreten MAS-Use-Cases auf Systemebene bewertet werden können. Die Ergebnisse der Dissertationsschrift können ferner zur Erarbeitung einer Richtlinie für die Gestaltung von CPS beitragen und den Förderer des Vorhabens, WITTE Automotive, dabei unterstützen, cyberphysische Produkte, die einen Mehrwert aus Daten liefern, sicherer auszulegen.

1.4 Aufbau der Arbeit

In dem Grundlagenkapitel 2 wird der Stand der Wissenschaft und Technik beschrieben. Es wird die wissenschaftliche Auseinandersetzung mit cyberphysischer Sicherheit beleuchtet. Anschließend werden die Begriffe Sicherheit und Risiko definiert sowie Metrik-Arten zur Bewertung von Risiken vorgestellt. Es folgt eine Darstellung etablierter Bewertungsansätze in der physischen Security-Bewertung und in der IT-Security-Bewertung. Gängige Methoden, Modelle und Metriken werden beschrieben. Es werden Vor- sowie Nachteile der erläuterten Ansätze benannt. In Kapitel 3 wird die Genese eines Ansatzes zur Sicherheitsbewertung von Physical Security und IT Security dargelegt. In den Kapiteln 3.1 und 3.2 wird eine strukturelle Analyse der Harnser-Metrik und der Common-Vulnerability-Scoring-System-Metriken (CVSS) durchgeführt: Auf der einen Seite wird in Kapitel 3.1 die semi-quantitative Harnser-Metrik der quantitativen Interventionsfähigkeitsmetrik gegenübergestellt. Anhand einer Barriere und einem Asset werden die Sicherungsfähigkeiten eines betrachteten, fiktiven Systems für verschiedene Konfigurationen einmal mit der einen Metrik, einmal mit der anderen Metrik bewertet und verglichen.

Die Ergebnisse zeigen dann für beide Fälle eine Vulnerabilitätsbewertung in Abhängigkeit der gewählten Sicherungskonfiguration auf. Gleichzeitig wird das Problem der Inkompatibilität von Metriken näher beleuchtet und es werden Herausforderungen, metrische Randbedingungen und Forderungen zur Angleichung beider Metriken detailliert herausgearbeitet. Ziel ist es, trotz unterschiedlicher Bewertungsmetriken gleiche Vulnerabilitätseinstufungen zu erzeugen. Andererseits wird in Kapitel 3.2 das klassische CVSS und der in Braband (2019) eingeführte, Barriere-basierte CVSS-Ansatz analysiert, wobei Verwerfungen und Möglichkeiten zur Reduktion von Verwerfungen innehrhalb von CVSS diskutiert und analytisch untersucht werden. In Kapitel 3.3.1 werden die Vulnerabilitätsbeschreibung in der physischen Sicherheit und die Vulnerabilitätsbeschreibung in der IT-Sicherheit gegenübergestellt. Gemeinsamkeiten sowie Unterschiede in der Beschreibung von Vulnerabilität in beiden Domänen werden herausgearbeitet. Daraufhin werden in Kapitel 3.3.2 Annahmen und Möglichkeiten zur Angleichung der Risikobeschreibungen und Risikobewertungen in beiden Security-Domänen aufgezeigt. In Kapitel 3.3.4 wird dargelegt, wie Sicherheitslevel in der physischen Sicherheit und in der IT-Sicherheit definiert und im Falle einer domänenübergreifenden Wechselwirkung aufeinander abgestimmt werden können. Aufbauend auf den Erkenntnissen der Analysen wird anschließend in Kapitel 4 dargelegt, inwiefern trotz erheblich unterschiedlicher Bewertungsmetriken in beiden Domänen eine Angleichung ermöglicht werden kann.

Daraufhin wird in den Kapiteln 4.1 bis 4.5 die Genese einer prospektiven Risikoanalyse für CPS dargelegt, welche sich an Vorgaben aus der ISO/SAE 21434 orientiert. Es wird beschrieben, wie Assets, Bedrohungen, Vulnerabilitäten und Auswirkungen im Rahmen eines Cyber-Physical Threat Analysis and Risk Assessments (CPTARA) bewertet werden können. In einem weiteren Schritt werden die Überlegungen zur CPS-Risikoanalyse in den Kapiteln 4.6 bis 4.8 in Bayes'sche Netze überführt, um die Metriken in beiden Domänen probabilistisch konsistent zu machen. Abschließend wird eine an die Delphi-Methode und den Cooke'schen Erhebungsansatz angelehnte Vorgehensweise vorgestellt, um Expertenwissen zu erheben und als Input in das Bayes'sche Netz zu überführen. In Kapitel 5 findet eine Diskussion des erarbeiteten Ansatzes statt. Die Ergebnisse werden anschließend in Kapitel 6 zusammengefasst. In einem Ausblick werden Anknüpfungspunkte für eine mögliche Anschlussforschung beleuchtet. Im Anhang wird in Kapitel 8.1 die Problemstellung ausführlicher diskutiert. In Kapitel 8.2 im Anhang werden Paradigmen in der physischen Sicherheit und in der IT-Sicherheit ausführlich dargelegt. Kapitel 8.3 im Anhang zeigt die Problematik der domänenübergreifenden Zusammenführung am Beispiel der Synthese von Theorien in der Physik auf.

2 Grundlagen

2.1 Richtlinien und Standards

Seit über fünfzehn Jahren nimmt der Einsatz von CPS in Fahrzeugen zu (BSI Branchenlagebild Automotive, 2022). Unumgänglich für Betreiber wird dabei die Bewertung von CPS aus der physischen Sicherheitsperspektive und aus der IT-Sicherheitsperspektive. „Die Automobilbranche ist durch nationale, wie auch internationale Vorgaben stark reguliert. […] In über 150 Einzelregelungen werden technische Vorgaben und Prüfverfahren vor allen Dingen zur Verkehrssicherheit des Fahrzeugs definiert" (BSI Branchenlagebild Automotive, 2022). „Gleichzeitig decken Standards und Normen noch nicht alle Bereiche der Fahrzeugentwicklung ab, sodass zahlreiche Aspekte OEM- bzw. Zuliefer-spezifisch gelöst werden und deshalb zu inhomogenen Lösungen führen können" (Wurm, 2022, S. 41). Im automobilen Bereich gibt es für die Functional Safety bereits in der Industrie verankerte Standards, insbesondere ISO 26262 (ISO, 2018) und DIN EN 61508[11] (DIN e.V., 2011), sowie Metriken, z. B. Automotive Safety Integrity Level (ASIL) (siehe ISO 26262-3:2018, Abschnitt 6.4.3, S. 10, 19-26). Diese unterstützten Anbieter dabei, Fahrzeuge und Sub-Systeme funktional sicher im Zuge der Produktentwicklung zu gestalten. „Das Inkrafttreten und die Weiterentwicklung von neuen Standards und Normen sollen hierzu einen entscheidenden Beitrag leisten", wird dazu im Branchenlagebild Automotive 2022 des Bundesamts für Sicherheit in der Informationstechnik (BSI) erklärt (BSI Branchenlagebild Automotive, 2022). In Deutschland definiert die allgemeine Bauartgenehmigung (ABG) Anforderungen an die Zulassung von Fahrzeugen im Straßenverkehr (KBA, 2021).

Der Technische Überwachungsverein (kurz: TÜV) bietet ein „umfassende[s] Portfolio an Services in den Bereichen Prüfungen und Zertifizierungen, Auditierungen sowie Beratung rund um Fahrzeuge" (TÜV, 2021) an. Es handelt sich um eine Organisation, die Sicherheitskontrollen am Fahrzeug durchführt. Die Kontrollen sind in der Bundesrepublik Deutschland durch Gesetze und Anordnungen vorgeschrieben. Sie bestätigen die Konformität eines Fahrzeugs mit vorgegebenen Safety-Anforderungen. Die Qualitätssicherung im Automobilsektor umfasst auch Crashtest-Ratings, wie beispielsweise nach RCAR (RCAR, 2021) und Euro NCAP (Euro NCAP, 2021). Crashtests tragen zur Verbesserung der Safety bei. Als sicher bewertete Fahrzeuge ziehen Kunden den schlechter bewerteten Fahrzeugen i. d. R. vor (VDA, 2022). Für die Security von CPS gibt es solche Tests bisher nicht. Prüfungen auf Konformität mit vorgegebenen IT-Security-Anforderungen sind jedoch in Arbeit.

Klassische physische Schließsysteme sind in Deutschland stark genormt (Schwerdtfeger, 2018, S. 3-5). Physische Sicherheit ist historisch gewachsen. Es gibt in der Industrie etablierte Ansätze, physische Sicherheit zu messen. Diese sind bereits seit Jahren in Standards und Richtlinien verankert. In physischen Sicherheitsnormen werden Anforderungen für unterschiedliche Anwendungsfälle und missbräuchliche Szenarien spezifiziert. Die DIN EN 1627 (DIN e.V., 2021a) definiert z. B. Widerstandsklassen, sog. Resistance Classes (RC), für Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse. Hinter einer RC stehen Widerstandszeiten gegen Angreifer mit bestimmten Fähigkeiten und Werkzeugen (Harnser, 2010, C2, S. 10). Je höher die RC, desto höher ist die Widerstandszeit. Die DIN EN 1628 (DIN e.V., 2021b) beschreibt beispielsweise Verfahren, um die Wirksamkeit von physischen Protektionseigenschaften zu prüfen.

[11] Bei der DIN EN 61508 handelt sich um die deutsche Fassung der IEC 61508 (IEC, 2010), welche eine Grundnorm der ISO 26262 ist.

Thatcham, eine Testinstitution für Fahrzeuge aus Großbritannien, bietet Zertifizierungen und Maßnahmenkataloge an, die die physische Security von Fahrzeugen und von Zugangssystemen betreffen (Thatcham, 2021). Schlösser und Türgriffeinheiten werden in mechanischen Penetrationstests auf ihre Widerstandsfähigkeit gegen Überwindungsversuche geprüft und mit Security-Ratings versehen. Für funkbasierte Schließsysteme gibt es noch keine Vorgaben. Im Gegensatz zu Standards für die physische Sicherheit sind Standards für die IT-Security recht neu. Es gibt zum Beispiel die ISO 27.000-Familie (DIN e.V., 2018) oder Vorgaben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), so z. B. das BSI-Grundschutzkompendium (BSI, 2020). Das BSI-Grundschutzkompendium umfasst Vorgaben zum Design und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) (Furnell et al., 2013, S. 151). Diese sind jedoch nicht Use-Case-spezifisch, und nicht alle Best Practices sind Teile des Kompendiums.

Der Digital Key Standard (DKS) des Car Connectivity Konsortiums (CCC, 2021) definiert Anforderungen an den virtuellen Fahrzeugschlüssel eines digitalen Fahrzeugzugangssystems, wie z. B. den Einsatz eines embedded Secure Elements (eSE) in mobilen Endgeräten zur Speicherung von digitalen Schlüsseln und zur Unterstützung kryptographischer Operationen. Die in Potsdam ansässige Non-Profit-Organisation Open Security Standards (OSS) Association arbeitet an der Entwicklung internationaler Standards für Zugangskontrollsysteme. Sie veröffentlichte bereits den OSS Standard Offline (OSSSO) für den immobilen Zugang via Smart Cards. Elektronische Schlösser sollen mithilfe des OSSSO herstellerunabhängig Berechtigungen einer Zugangskarte lesen und diese in gleicher Art und Weise interpretieren" (OSS Association, 2021) können. Im Automobilbereich stand die Functional Safety in den letzten zehn Jahren an erster Stelle der Prioritäten der Industrie (Macher et al., 2020a; Möller et al., 2019, S. 302). Das zunehmende Wachstum von IT-Komponenten macht moderne Fahrzeuge zu Datenhubs. Gleichzeitig sind die Daten von fahrzeugimmanenten Systemen attraktive Ziele für Cyberattacken (BSI Branchenlagebild Automotive, 2022).[12] Erfolgreiche Angriffe können, bedingt durch die Interoperabilität von Systemkomponenten innerhalb des Fahrzeugs, unerwünschte Schadensereignisse hervorrufen, die die Functional Safety oder die physische Security betreffen (Macher et al., 2020a; Möller et al., 2019, S. 266, 271). Insbesondere die Berücksichtigung von Cybersecurity in Produktentwicklungsprozessen wird zunehmend wichtiger (Möller et al., 2019, S. 294; Schmittner et al., 2018).

Um den Herausforderungen durch Cyberbedrohungen zu begegnen, wurde im Januar 2021 die UNECE R 155-Regulation (kurz: R 155) für Cybersecurity-Managementsysteme (CSMS) von der United Nations Economic Commission for Europe (UNECE) eingeführt (UNECE, 2021). Sie ist Teil der UNECE Working Party 29 (WP.29). Diese stellt neben Vorgaben für die Implementierung eines CSMS (R 155) ebenso Vorgaben für Software-Update-Managementsysteme (SUMS; R 156) und Automated Lane Keeping Systems (ALKS; R 157) aufstellt. Mit der R 155 werden Unternehmen adressiert, die Fahrzeuge auf den Markt bringen, z. B. Original Equipment Manufacturer (OEM). Die Handhabung von Cybersecurity ist Stand April 2022 noch keine formale, regulatorische Anforderung für die Zulassung von neuen Fahrzeugen zum Markt (Homologation). Die Konformität mit der R 155 wird bereits ab Juli 2022 für alle neuen Fahrzeugtypen gefordert, die in den UNECE-regulierten Markt gebracht werden. Zu diesem Markt gehören die EU, Südkorea und Japan gehören. Ab Juli 2024 ist die Konformität mit der R 155 hier für alle neuen Fahrzeugzulassungen verpflichtend.

Eine Möglichkeit, diese Konformität nachzuweisen, ist die Zertifizierung nach der ISO/SAE 21434 „Road Vehicles – Cybersecurity Engineering". Informative Ausschnitte des Standards

[12] Das BSI und das Kraftfahrtbundesamt (KBA) arbeiten seit Dezember 2020 stärker zusammen, um „Digitalisierung weiter sicher zu gestalten und verlässliche Rahmenbedingungen für Investitionen und Innovationen zu schaffen" (BSI Branchenlagebild Automotive, 2022).

können öffentlich eingesehen werden (ISO/SAE, 2021a). Die Vollversion wird von der Society of Automotive Engineers (SAE) bereitgestellt (ISO/SAE, 2021b). Grundlage der Norm ist die SAE J3061 „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (SAE, 2021). Die SAE J3061 beinhaltet einen Praxisleitfaden für das Cybersecurity Engineering in Bezug auf Produkte im Fahrzeug über den gesamten Lebenszyklus. In der SAE J3061 werden die Threat and Operability Analysis (TOA), Attack Tree Analysis (ATA) und das HEAVENS Security Model (Autosec, 2016) zur Analyse und Bewertung von Cybersecurity-Risiken vorgeschlagen. Die ISO/SAE 21434 fasst den Umfang etwas weiter und beschreibt allgemein Anforderungen an die Informationssicherheit[13], die Prozessgüte[14] und die Produktsicherheit[15]. Im Gegensatz zum risikobasierten Ansatz der Threat Analysis and Risk Assessment (TARA) aus der ISO/SAE 21434 wird in der ISO 26262 eine HARA (Hazard Analysis and Risk Assessment) durchgeführt. „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, S. 6). Nach Wurm (2022) ist die Aufgabe der TARA, „eine vollständige und systematische Untersuchung aller möglichen und wahrscheinlichen Angriffsvektoren für ein konkretes System" (Wurm, 2022, S. 35) durchzuführen.

Nach ISO 26262 ist das Safety-Risiko definiert als die Kombination aus der Wahrscheinlichkeit des Auftretens eines Schadens und dem entsprechenden Schadensausmaß. Risiko kann nach der HARA aus der ISO 26262 ferner als Funktion der Häufigkeit des Auftretens eines gefährlichen Ereignisses (Frequency, F), der Fähigkeit, einen Schaden durch rechtzeitige Reaktionen der beteiligten Personen oder durch externe Maßnahmen zu vermeiden, wenn ein gefährlicher Zustand eingetreten ist (Controllability, C) und der potenziellen Schwere des resultierenden Schadens (Severity, S) definiert werden. Die drei Risikoparameter F, C und S werden in vier Stufen eingeteilt und innerhalb der HARA kombiniert, um den Automotive Safety Integrity Level (ASIL) zu bestimmen. Der ASIL kann als Maß für die erforderliche Risikominderung interpretiert werden (Krisper, 2021).

Das Security-Risiko nach ISO/SAE 21434 hingegen ist definiert als eine Kombination aus der Eintrittswahrscheinlichkeit eines Schadens (Attack Feasibility) und dem entsprechenden Schadensausmaß (Impact): Der Risikoparameter Impact wird mit dem vorliegenden Angriffsvektor, bestehend aus den Deskriptoren „Physical", „Local", „Adjacent" und „Network", verknüpft, um das Cybersecurity Assurance Level (CAL) zu bestimmen (ISO/SAE, 2021b, S. 59) (siehe auch Kapitel 3.3.4). Über die Definition des CAL wird in Macher et al. (2020b) geschrieben:

> The CAL should have be 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, S. 10).

In der SAE J3061 gibt es eine Vielzahl von Parallelen zur ISO 26262. Beim Cybersecurity Process Overview (SAE J3061, Teil 8) sind die Phasen des Entwicklungszyklus an die Teile 3-8 der ISO 26262 angelehnt (SAE, 2021; Costantino et al., 2022). Sie beinhalten die Konzeptphase, die Systementwicklung (Hardware, Software), die Produktion und unterstützende Prozesse. Sie gilt für Bauteile (elektronische Teile und Software) von in Serie hergestellten Fahrzeugen sowie für

[13] Als „Dach", beschrieben in ISO 27001 (DIN e.V., 2018).
[14] Als „Träger", beschrieben in Automotive SPICE Supply Chain & Cybersecurity (SPICE, 2015).
[15] Als „Fundament". Die Threat Analysis and Risk Assessment (TARA) der ISO/SAE 21434 (ISO/SAE, 2021b, S. 41-49) bildet eine wichtige Vorgehensweise zur Ableitung von Cybersecurity-Anforderungen.

Ersatzteile und Zubehör. Die ISO/SAE 21434 deckt die Phasen der Entwicklung, der Produktion, des Betriebs, der Wartung und der Außerbetriebnahme im Lebenszyklus eines Fahrzeugs ab. OEM müssen folglich die Anforderungen aus der Norm über die gesamte Lieferantenwirkkette nachweisen (Macher et al., 2020b). Zentrale Punkte der ISO/SAE 21434 sind der Aufbau sowie der Betrieb eines Cybersecurity-Managementsystems (CSMS) und die Bedrohungsanalyse und Risikobewertung (TARA). Die TARA ist nach Kandasamy et al. (2020) eine von vier gängigen Cybersecurity Risk Frameworks, die zur Bewertung von vernetzten Geräten verwendet werden kann (Umfang, Vor- und Nachteile der vier Rahmenwerke siehe Tabelle 1).

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

Tabelle 1: Cybersecurity Risk Frameworks.
Quelle: Kandasamy et al. (2020).

Die Schritte zur Durchführung einer TARA sind in Abbildung 4 dargestellt. Die hellgrau markierten Einträge repräsentieren Arbeitspakete. Der Prozess der TARA ist von links nach rechts zu lesen. Inputs und Outputs der einzelnen Arbeitspakete sind durch die jeweiligen Pfeilrichtungen gekennzeichnet. Mit einem schwarzen Rahmen markiert ist die Bestimmung des CAL, weil es sich um ein optionales Arbeitspaket handelt. In Tabelle 2 sind die dazugehörigen, methodischen Schritte aufgeführt. Die Schritte in der HARA und TARA sind ähnlich (Macher et al., 2020b). Assets werden identifiziert und Schadensszenarien werden bewertet: Während sich die HARA mit der Bewertung möglicher Unfälle befasst, geht es bei der TARA um die Bewertung böswilliger Angreifer (Ponsard et al., 2021). In beiden Fällen werden nach der Bewertung von Unfallszenarien (ISO 26262) bzw. Angriffsszenarien (ISO/SAE 21434) Sicherheitsanforderungen und Sicherheitsmaßnahmen abgeleitet. „Beide Normen verfolgen [aber] ein gemeinsames Ziel: die Entwicklung eines zuverlässigen, fehlerfreien und sicheren (safe und secure) Systems indem Risiken für Hazards und Threats möglichst reduziert werden“ (Wurm, 2022, S. 69).

Die ISO/SAE 21434 beschreibt jedoch lediglich ein Rahmenwerk (Costantino et al., 2022; BSI Branchenlagebild Automotive, 2022), das sich auf die Festlegung von Mindestkriterien für die Cybersicherheit in der Automobilindustrie fokussiert (Macher et al., 2020a). Die konkrete Implementierung liegt beim Anwender: „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, S. 3).

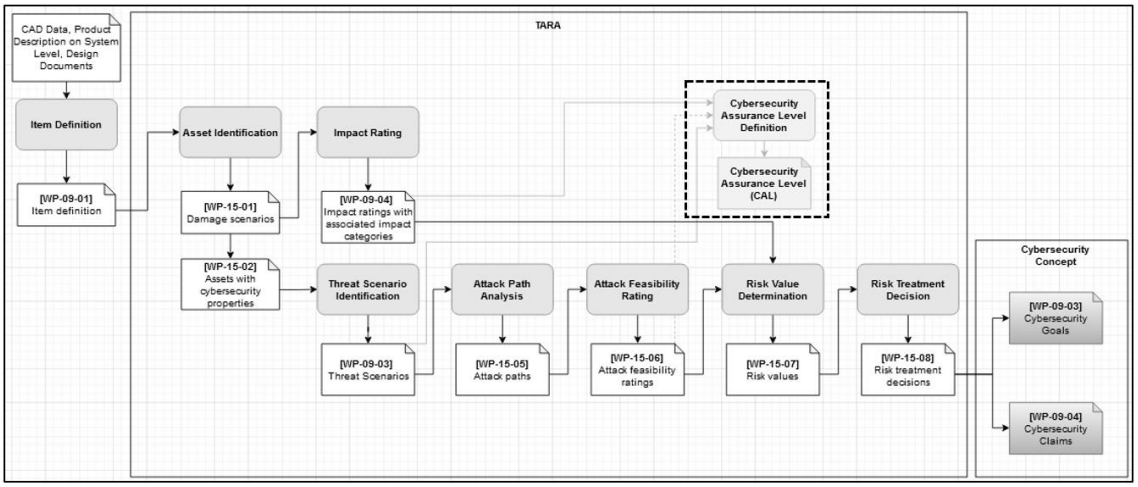


Abbildung 4: TARA nach ISO/SAE 21434.
Quelle: ISO/SAE (2021b, S. 73-78).[16]

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. Die erste Ziffer steht für die Klausel in der ISO/SAE 21434. Die zweite Ziffer ist eine fortlaufende Identifikationsnummer.

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.

Tabelle 2: TARA-Prozess inklusive Methodenbeschreibung.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 73-78).

Weil die OEM zur Homologation gemäß UNECE R 155 für ihre Produkte (Fahrzeuge) das CSMS über die gesamte Lieferantenwirkkette nachzuweisen haben, werden diese von den automobilen Zulieferern Konformität mit den Anforderungen an ein CSMS und die Erstellung einer TARA fordern. Weiterhin werden die Nachweise zur Cybersecurity-Testumsetzung und die Testergebnisse im Rahmen des CSMS über die Lieferantenwirkkette nachzuweisen sein. „Hersteller müssen zur Umsetzung eines ganzheitlichen Securitykonzepts bestimmte Anforderungen an ihre Lieferanten übertragen“, so Wurm (2022, S. 36) in diesem Zusammenhang. Grundsätzlich liegt die Homologation in der Verantwortung der OEM. Es gibt Ausnahmen, z. B. im Falle von Systemen der passiven Sicherheit. Hierbei kann der Tier-1-Supplier auch eigenständig Systeme homologieren. Mit der ISO/PAS 5112:2022 (ISO, 2022) „Road Vehicles – Guidelines for Auditing Cybersecurity Engineering“ wurde ein Standard herausgegeben, in dem die Auditierung eines CSMS und die Komponenten des CSMS Auditors definiert sind. Wie aber OEM den Nachweis der ISO 21434-Konformität von Tier-1 fordern, ist jeweilige OEM-Sache. Die Notwendigkeit zur Durchführung einer TARA seitens eines Tier-1-Suppliers ist dagegen wahrscheinlich. Um die Fahrzeughersteller bei der Vorbereitung auf das Assessment zu unterstützen, hat der Verband der Automobilindustrie (VDA) das Dokument „Automotive Cyber Security Management System Audit" veröffentlicht (VDA, 2020). Es „definiert den Fragenkatalog und das Bewertungsschema, das bei der Auditierung des CSMS sowohl der OEMs als auch der Vertragspartner zur Anwendung kommen kann“ (VDA, 2020).

Bei der TARA handelt es sich um eine Szenario-basierte Analyse, bei der der Impact eines IT-Szenarios auf die Safety qualitativ auf einer Skala von „Negligible“ (S0: No injuries) bis „Severe“ (S3: Life-threatening injuries) eingeordnet wird (ISO/SAE, 2021b, S. 63-64). Nach SAE J3061 ist die Functional Safety eine Teilmenge der Cybersecurity (siehe Abbildung 5 rechts). So sind Safety-Architekturen durch Cybersecurity-Elemente erweiterbar. Safety Engineering und Cybersecurity Engineering haben darüber hinaus Schnittmengen in Arbeitsschritten (siehe Abbildung 5 links). Anforderungen aus beiden Domänen können Teil einer gemeinsamen Spezifikation sein. „Cybersecurity ist ein Querschnittsthema, welches ähnlich wie Funktionale Sicherheit mit quasi allen anderen Disziplinen verknüpft ist. „Ein Arbeiten in „Silos“ sollte (auch) deshalb systematisch verhindert werden“, so Wurm (2022, S. 60). Es kann z. B. zunächst die HARA durchgeführt werden. Die Ergebnisse werden als Input in die TARA eingeführt, d. h., Functional Safety-Ziele können in Form von zu schützenden Assets in der TARA formuliert

werden (Prinzip siehe Abbildung 5). Eine ähnliche Vorgehensweise wird von der North Atlantic Treaty Organization Science and Technology (NATO S&T) vorgeschlagen (Piper, 2020).

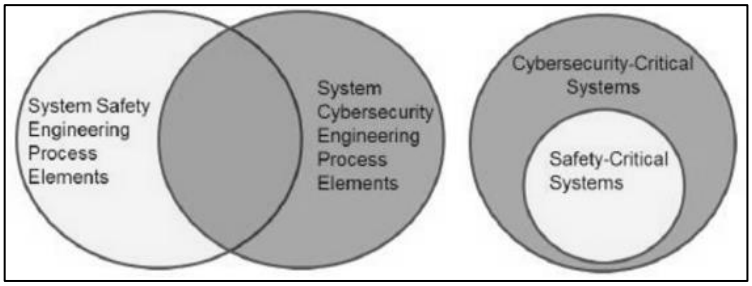


Abbildung 5: Schnittmengen von Functional Safety und Cybersecurity.
Quelle: SAE (2021, S. 17).

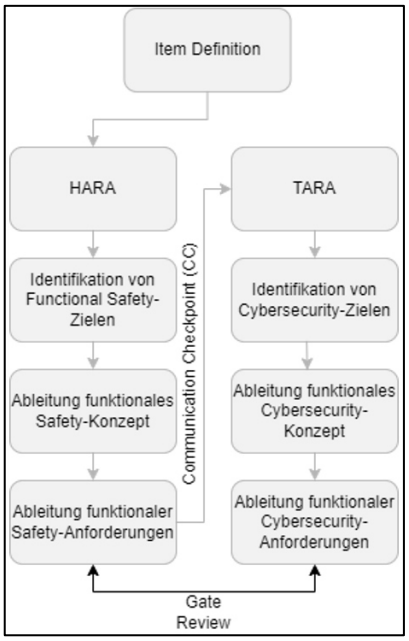


Abbildung 6: Beispielhafte Verknüpfung von HARA und TARA.
Quelle: Eigene Abbildung in Anlehnung an SAE (2021, S. 40).

Die SoQrates-Initiative treibt das Vorhaben voran, die deutsche Industrie bei der Implementierung von Automotive SPICE zu unterstützen (SoQrates, 2022). Ferner gibt die European Union Agency for Cybersecurity (ENISA) einen umfassenden Report zu Incidents, Trends und Prime Threats nach Sektor sowie Mitigationsmaßnahmen zum Thema Cybersecurity heraus. Einer der drei Hauptbereiche, der seitens ENISA als besonders bedroht eingestuft und im Rahmen des Reports betrachtet wird, ist der Transportsektor (ENISA, 2021, S. 29). In dem „E-safety Vehicle Intrusion Protected Applications (EVITA)" Projekt, das in konsortialer Zusammenarbeit mit dem Fraunhofer-Institut, der BMW Group, Bosch, Infineon und weiteren Partnern getragen wird, wurde ein Dokument veröffentlicht, das Verfahren zur Ermittlung und Bewertung von Sicherheitsanforderungen darlegt.

Der vorgeschlagene EVITA-Ansatz wird z. B. in Ruddle et al. (2009) am Beispiel von Fahrzeug-On-Board-Netzen angewendet. Die darin erarbeiteten „Security requirements for automotive on-board networks" (Ruddle et al., 2009, S. 24-57) liefern Beiträge zum Entwurf einer sicheren On-Board-Architektur. EVITA verfolgt das Ziel, „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).

Darüber hinaus wird im 5StarS Consortium daran gearbeitet, ein Rahmenwerk zur Bewertung von Fahrzeug-Cybersecurity aus Versicherungsperspektive zu entwickeln (5Star, 2021). Für die Klassifizierung von Vulnerabilitäten in der Cyberdomäne wurde bereits im Jahr 1995 eine Taxonomie namens AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target) eingeführt, die Anwender bei der Bewertung von Risiken unterstützen kann (Möller et al., 2019, S. 328). Produktentwickler stehen sowohl vor der Herausforderung einer domänenübergreifenden Zusammenführung von Modellen aus der Physical Security, der Functional Safety und der IT Security als auch vor der Herausforderung einer Zusammenführung von Metriken aus der Physical Security bzw. Functional Safety und IT-Security. Ein Grund dafür ist die erforderliche quantitative Analyse. Wurm (2022) stellt hier klar:

> Redundante Safety-Pfade sind unzureichend für den Schutz gegen Security-Angriffe. […] Die Kritikalität beschränkt sich allerdings nicht auf Safety-Aspekte. Ohne ausreichenden Schutz vor Cybersecurity-Angriffen könnten vernetzte und automatisierte Fahrzeuge leicht von Diebstahl, Sabotage oder Hacktivismus betroffen werden. (Wurm, 2022, S. 30).

Bei vernetzten Systemen kann es keine Functional Safety ohne Security geben. Aus diesem Grund sollten keine Functional-Safety-Anforderungen an IT-Security-Funktionen gestellt werden (Wurm, 2022, S. 38). Aus Betreibersicht können Vertrauensverluste seitens des Kunden und Reputationsschäden eine realistische Folge erfolgreicher Angriffe sein (Wurm, 2022, S. 30). Eine quantitative Analyse ist bei IT-Bedrohungsszenarien nur schwer zu leisten (Scala et al., 2019). Anforderungen müssen gegeneinander abgewogen werden, aber Ansätze, die eine quantitative Analyse ermöglichen könnten, sind in aktuellen Standards bisher nicht zu finden (Macher et al., 2020a).

Die UNECE WP.29 fordert jedoch vom Fahrzeughersteller eine „Risikobewertung […] einzelner Fahrzeugsysteme sowie deren Wechselwirkung untereinander und mit externen Systemen" (Elektronik Automotive, 2020, S. 27-28). In Fosch-Villaronga & Mahler (2021) wird beschrieben, dass Functional Safety und Security in bisherigen Richtlinien weitestgehend getrennt betrachtet werden: „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" (Forsch-Villaronga & Mahler, 2021, S. 1). In Möller et al. (2019) wird eine ähnliche Auffassung vertreten:

> 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, S. 350).

Grund für die bisher weitestgehend getrennte Betrachtung ist u. a. der fehlende Wirkmechanismus in der IT-Security (Jacobs et al., 2019). In der IEC 61508 Ausgabe 2.0wird beispielsweise eine integrierte Vorgehensweise zur Verknüpfung der Bewertung von Functional Safety und IT-Security vorgeschlagen: IT-Security-Bedrohungen sollen während der Gefährdungsanalyse und Risikobewertung aus der Functional Safety berücksichtigt werden. Die integrierte Bedrohungsanalyse wird jedoch nicht weiter in der IEC 61508 spezifiziert. Empfehlungen bezüglich der Interaktion zwischen Safety und Security werden darüber hinaus in der ISO 26262 Ausgabe 2.0 im Annex E gegeben (Macher et al., 2020a). Diese bieten aber keine Lösung zur Synthese der inkompatiblen Metriken aus beiden Disziplinen an. In Macher et al. (2020a) wird der

derzeitige Stand der Standardisierung von Produkten im Automobilsektor zusammengefasst: „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, S. 3). Beim Design von automobilen Produkten, die Sicherungsfunktionen aus beiden Domänen vereinen, gibt es zwei zentrale Probleme: „(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 multi-disciplinary product" (Macher et al., 2020a, S. 2).

Für die Bereitstellung von Services müssen Daten ausgetauscht, gespeichert und verarbeitet werden können. Fragen, die die Ablage und den Umgang mit Daten im Anwendungsfall betreffen, sollen im Zuge von aus Europa heraus getriebenen Entwicklungen beantwortet werden. Beispiele dafür sind die Datenschutzgrundverordnung (DSGVO, 2021) und GAIA-X (2021). GAIA-X ist ein von den EU-Mitgliedstaaten gefördertes Vorhaben zum Aufbau einer vertrauensvollen, europäischen Datenverkehrsinfrastruktur. Durch Einsatz des International-Data-Spaces-Standards (IDS) (IDSA, 2021), der in der DIN SPEC 27070 (DIN e.V., 2020) „Requirements and reference architecture of a security gateway for the exchange of industry data and services" aufgegangen ist, möchten die Länder der EU einen legalen und kommerziellen Rahmen für Unternehmen schaffen, um datengetriebene Geschäftsmodelle konform zu Privacy-Aspekten, u. a. rund um das Ökosystem Fahrzeug, anbieten zu können (MDS, 2022). Im Kern soll die Implementierung von IDS die standardisierte Vernetzung von Systemen und Anwendungen ermöglichen (MaaS Alliance, 2022). Die Berücksichtigung von Privacy-Aspekten macht insbesondere die Durchführung einer Risikobewertung zusätzlich kompliziert. Insgesamt zeigt der Stand der Technik in der Schließtechnik sowie im Automotive-Bereich Bedarfe in der metrischen Zusammenführung von Physical Security und IT Security auf (siehe Tabelle 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	Allianz für Cybersicherheit (BSI)
ISO 31000:2018	ISO 8800	automotive.wiki
ISO PAS 5112	NHTSA	SoQrates
Auto ISAC		ENX Association
VDA Automotive SPICE Extension for Cybersecurity		Cybersicherheitsrat Deutschland 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-Grundschutz-Kompendium		**AUTOSAR, SHE, SHE+, OMG, CCC, HIS**
DfT UK (Principles for Cybersecurity)		**NIS2 Directive**
ACEA		**SafEUr**
		PRESERVE

Tabelle 3: Projekte, Standards und Assoziationen im Bereich Schließsysteme und Automotive. Quelle: Eigene Tabelle erweitert nach Schwerdtfeger (2018)[17]

2.2 Forschung zur cyberphysischen Sicherheit

Die wissenschaftliche Forschung zur Risikobewertung von MAS ist recht neu. Seitens des Instituts für Sicherungssysteme (ISS) gibt es zu MAS bereits wissenschaftliche Beiträge. Beispiele dafür sind Schwerdtfeger (2018) zur Security-Risikobewertung von immobilen MAS und Termin et al. (2020) bzw. Termin et al. (2021) zu automobilen MAS. Weil MAS als CPS charakterisiert werden können, wird nachfolgend der Stand der Forschung zur Security von CPS betrachtet. Wissenschaftliche Beachtung findet die CPS-Sicherheit seit dem Jahr 2006. Der Begriff „Cyberphysisches System" soll erstmalig von Helen Gill der National Science Foundation (NSF) im Jahr 2006 verwendet worden sein (Ittermann et al., 2018, S. 33-60). In Cardenas et al. (2009) werden Security-Herausforderungen durch den Einsatz von CPS benannt, wie z. B. „Software patching and frequent updates" (Cardenas et al., 2009, S. 2) und „real-time availability" (Cardenas et al., 2009, S. 2). Darüber hinaus werden in demselben wissenschaftlichen Beitrag einzigartige Eigenschaften von CPS im Vergleich zu traditionellen IT-Systemen aufgezeigt. Dazu gehören beispielsweise „network dynamics" (Cardenas et al., 2009, S. 3) und „dynamics of the physical system" (Cardenas et al., 2009, S. 4). Abschließend werden in Cardenas et al. (2009) Mechanismen zur Bedrohungsprävention (inkl. Abschreckung), Detektion und Wiederherstellung (Resilienz) vorgestellt. Ein zentrales Problem beim Design von CPS wird dergestalt beschrieben: „Researchers have not considered how attacks affect the […] control algorithms – and ultimately, how attacks affect the physical world" (Cardenas et al., 2009, S. 3).

Konkrete Anforderungen an ein CPS, insbesondere mit Blick auf unterschiedliche Use Cases, werden in Neuman (2009) dargelegt. In Neuman (2009) wird herausgestellt, dass CPS-Elemente räumlich getrennt und dezentral orchestriert sein können. Dadurch, dass CPS in unterschiedlichen Anwendungen agieren, mit denen verschiedene umweltliche Randbedingungen einhergehen können, bedarf es individueller Anforderungen an die Security: „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, S. 2). Das macht die Sicherheitsbewertung kompliziert (Neuman, 2009). In Ashibani & Mahmoud (2017) werden CPS von IoT-Devices abgegrenzt:

> 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, S. 3).

[17] Standards und Richtlinien für den Bereich Automotive wurden im Rahmen der Tätigkeiten im Fachausschuss 512 „Safety & Security" des VDI erarbeitet. RFID := Radio Frequency Identification.

CPS werden in Ashibani & Mahmoud (2017) in drei Schichten eingeteilt: Application (Use Case), Transmission (Kommunikationsschnittstelle) und Perception (Hardware). Diese Dreiteilung wird als Grundlage für die Durchführung einer CPS-Risikobewertung empfohlen (Ashibani & Mahmoud, 2017). In Möller et al. (2019, S. 356) wird im Gegensatz zu dem Ansatz in Ashibani & Mahmoud (2017) eine fünfgliedrige Einteilung vorgeschlagen. Diese Einteilung besteht aus dem Application Layer, dem Transportation Layer, dem Network Layer, dem Link Layer und dem Physical Layer. Eine detailliertere Unterteilung in insgesamt sieben Kategorien wird z. B. in Alguliyev et al. (2018) vorgenommen: Dazu zählen u. a. die physische Schicht, Protokollschicht, Session-Schicht und Applikationsschicht. Beim Open-Systems-Interconnection-Modell (OSI) der International Telecommunication Union (ITU) aus der ISO/IEC 7498-1:1994 wird ein System insgesamt in sieben Schichten eingeteilt: Bitübertragungsschicht (Physical Layer), Sicherungsschicht (Data Link Layer), Vermittlungsschicht (Network Layer), Transportschicht (Transport Layer), Sitzungsschicht (Session Layer), Darstellungsschicht (Presentation Layer) und Anwendungsschicht (Application Layer) (Kumar et al., 2014).

In dem Modell, wie in Ashinabi & Mahmoud (2017) vorgeschlagen, wird die Security in zwei Bereiche unterteilt, zum einen in die Informations- bzw. Datensicherheit und zum andern in die Steuerungssicherheit. Zur Steuerungssicherheit wird in Ashinabi & Mahmoud (2017) die physische Security gezählt. Die Schnittstellen zwischen den drei Schichten sind in besonderem Maße zu schützen (Ashinabi & Mahmoud, 2017). In Alguliyev et al. (2018) wird vorgeschlagen, zur Sicherung eines CPS geeignete Authentifikationsprotokolle und Verschlüsselungsalgorithmen zu verwenden. Der Fokus in Alguliyev et al. (2018) wird auf die IT-Security und ebenso Privacy-Verletzungen gelegt. Angriffsvektoren werden zwischen außen (externer Angreifer) und innen (böswillige Mitarbeiter) differenziert.

Darüber hinaus werden allgemeine Gegenmaßnahmen, wie beispielsweise Multi-Layer-Security-Lösungen, vorgeschlagen (Alguliyev et al., 2018). Ziel ist es, ein robustes Bewertungsmodell zur Verifizierung aller Bedrohungen und Schwachstellen zu entwickeln, um in einem definierten Kontext (Use Case) dazu beitragen zu können, die Entscheidungsfindung bzgl. des Investments in Sicherungsmaßnahmen zu unterstützen (Alguliyev et al., 2018). In Ashibani & Mahmoud (2017) wird beschrieben, dass es sich bei CPS-Sicherheit um ein neues Gebiet handelt, auf dem bisher nur wenige Arbeiten veröffentlicht wurden. In Lun et al. (2019) werden für das Jahr 2015 insgesamt 57 Veröffentlichungen zum Thema CPS-Security gezählt (siehe Abbildung 7). Abbildung 7 zeigt den Trend auf, dass die Auseinandersetzung mit der CPS-Security aus Sicht der wissenschaftlichen Community zunehmend wichtiger wird.

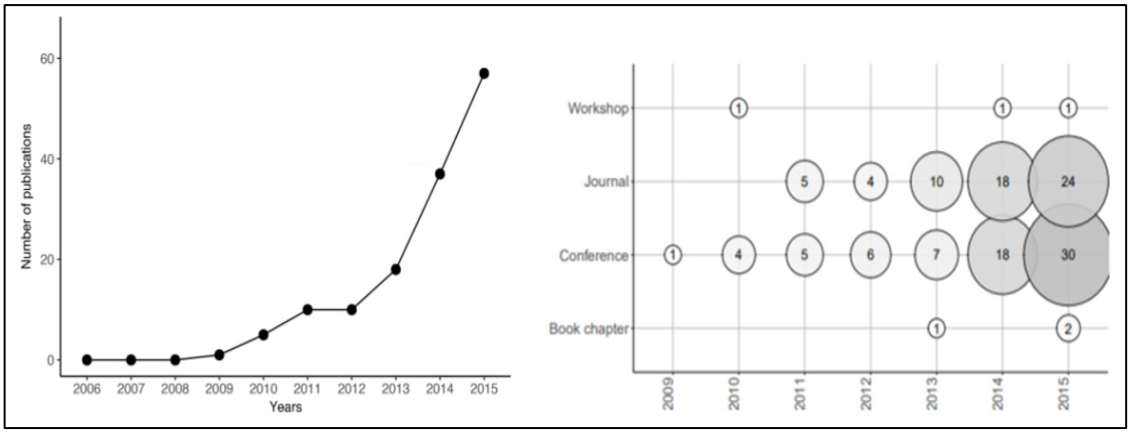


Abbildung 7: Publikationen zur CPS-Security über das Jahr (links) und nach Format und Jahr (rechts). Quelle: Lun et al. (2019).

In Graja et al. (2020) wird analysiert, mit welchen Modellierungssprachen CPS modelliert werden und in welchen Anwendungsgebieten Publikationen in diesem Zusammenhang vorhanden sind. Es werden in Graja et al. (2020) folgende Ansätze identifiziert: 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) und Unified Modeling Language (UML). Für die insgesamt 62 untersuchten Veröffentlichungen werden die Anteile der verwendeten Modellierungssprachen auf folgende Weise zusammengefasst (siehe Abbildung 8):

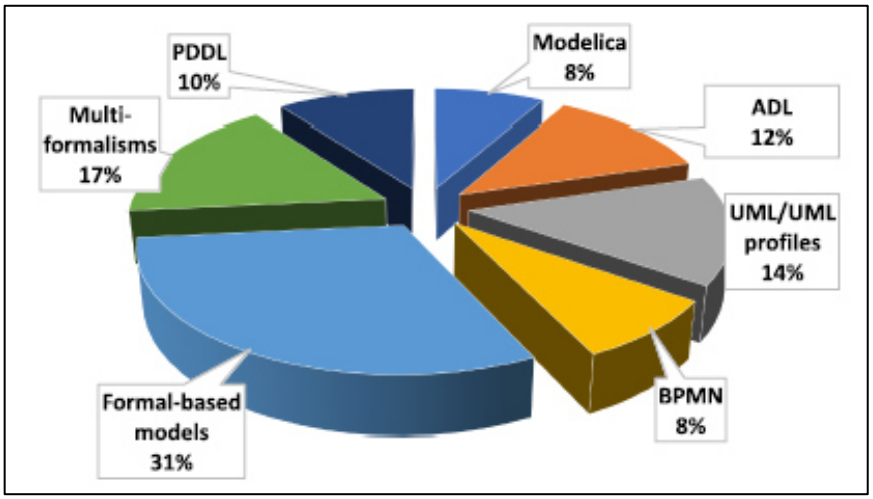


Abbildung 8: Anteil der verwendeten Modellierungssprachen bei der Modellierung von CPS. Quelle: Graja et al. (2020).[18]

CPS-Modellierungsansätze gliedern sich nach Graja et al. (2020) in vier Anwendungsbereiche, den „Transportation Systems", „Emergency Rescue Systems", „Health-Care" sowie „Smart Home/Area" (siehe Abbildung 9). Die Ergebnisse der Recherche von Graja et al. (2020) zeigen auf, dass bei CPS im automobilen Sektor die Architecture Description Languages (ADL), Unified Modeling Language (UML), Multi-Modellierungstechniken und formalbasierte Methoden breite Anwendung finden.

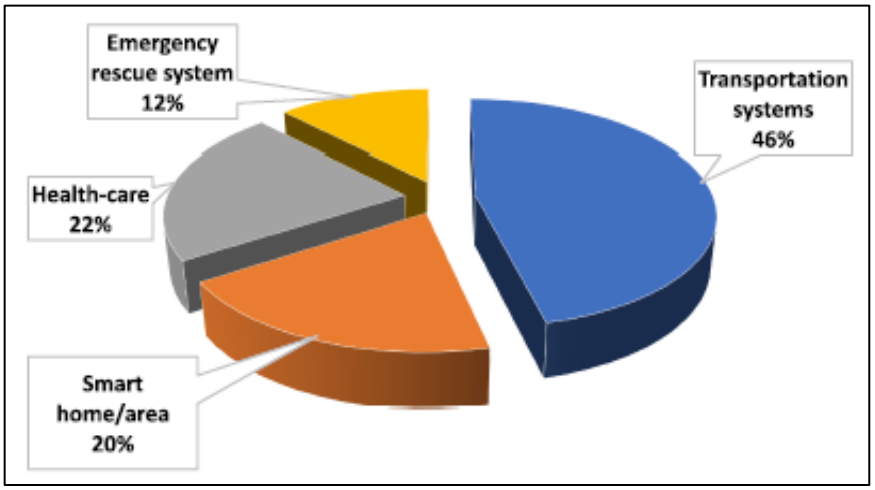


Abbildung 9: Anteil der Anwendungsgebiete in den Modellierungsansätzen für CPS-Anwendungen. Quelle: Graja et al. (2020).[19]

[18] Anzahl an untersuchten Veröffentlichungen: n = 62.
[19] Anzahl an untersuchten Veröffentlichungen: n = 62.

Herausfordernd beim Systemdesign von CPS ist, dass einem Angreifer potenziell unterschiedliche Einsprungpunkte zur Verfügung stehen können, um physische Assets oder Daten-Assets zu manipulieren, zu zerstören oder zu entwenden (Wang et al., 2010; Möller et al., 2019, S. 306, 362-368). Das ist anders als in der rein physischen Betrachtung unter Annahme eines bodengebundenen Angreifers: Dieser Angreifer muss physische Barrieren entlang eines Angriffspfades nacheinander von der ersten bis zur letzten Barriere überwinden (Lichte et al., 2016). Durch die Vernetzung von physischen und logischen Komponenten[20] kann es durch einen Angriff zu Wechselwirkungen mit anderen Komponenten kommen, welche die Funktionalität des Gesamtsystems beeinflussen können (Mo et al., 2011). Sicherheitsmaßnahmen von physischen oder IT-Barrieren können, je nach Angriffsszenario, im Worst Case vollständig ausgehebelt werden und Schlüsseleigenschaften sowie Schlüsselfunktionen des CPS bedrohen (Koscher et al., 2010). Deswegen ist es wichtig, zu verstehen, welche Wege ein Angreifer zu seinem Ziel nehmen kann (Möller et al., 2019, S. 319). Die Vernetzungsproblematik wird in Mo et al. (2011) im Zusammenhang intelligenter Stromnetze (sog. Smart Grids) dargelegt. Systemtheoretische Ansätze werden in Mo et al. (2011) mit Ansätzen zur Modellierung und Bewertung von Cybersecurity-Beiträgen verglichen (siehe Abbildung 10).

	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

Abbildung 10: Ansätze zur Modellierung und Bewertung von CPS.
Quelle: Mo et al. (2011).[21]

Cybersecurity-Modellierungsansätze und systemtheoretische Ansätze werden in Mo et al. (2011) genutzt, um die Detektionsrate von Sensorausfällen unter Berücksichtigung eines Angriffs zu bestimmen. Der in Mo et al. (2011) gewählte Ansatz ist einer fehlertoleranten Regelung ähnlich. In Möller et al. (2019, S. 272-273) werden ferner fünf Security-Konzepte betrachtet, welche Anwender dabei unterstützen können, die erfolgreiche Realisation eines Bedrohungsszenarios für Cybersecurity-relevante Komponenten zu vermeiden. Dazu gehören „Artificial Intelligence", die „Control Theory", die „Epistemic Theory", die „Game Theory" und die „Graph Theory". Eine Auseinandersetzung mit der Detektion und Lokalisation von Angriffen findet in Pasqualetti et al. (2013) statt. Es wird in Pasqualetti et al. (2013) die Unified Modeling Language (UML) als Modellrahmen verwendet. CPS-Sicherheit wird als regelungstechnisches Problem beschrieben. In Konstantinou et al. (2015) werden darüber hinaus Datenschutzbelange auf verschiedenen cyberphysischen Systemebenen untersucht. Die Anwendungsbereiche Smart Home und kritische Infrastrukturen (KRITIS) werden in diesem Zusammenhang betrachtet. Cyberphysische Angriffsmodelle werden in Teixeira et al. (2015) erarbeitet. Ausgangspunkt dafür bildet der cyberphysische Angriffsraum (siehe Abbildung 11).

[20] Die logische Schicht umfasst alle Verarbeitungsmechanismen einer konkreten Anwendung. IT-Komponenten sind zur Ermöglichung der Verarbeitung erforderlich.
[21] WAN := Wide Area Network, NAN := Near Area Network, HAN = Home Area Network, DoS := Denial of Service.

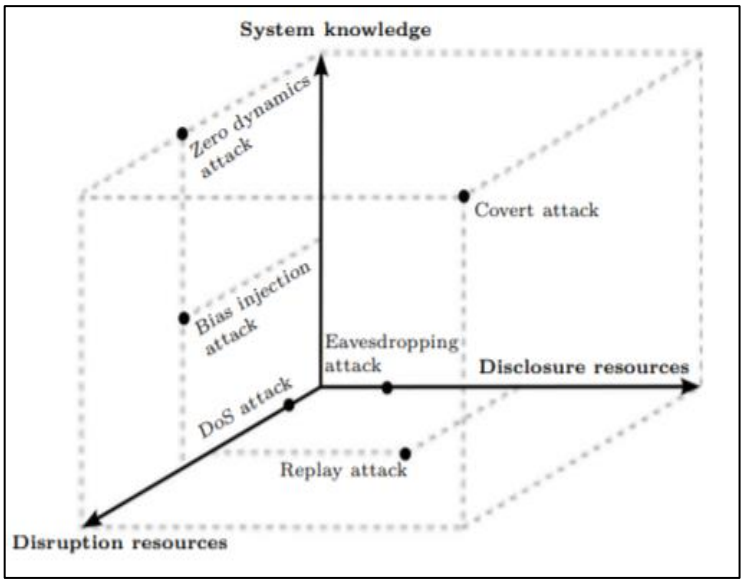


Abbildung 11: Cyberphysischer Angriffsraum.
Quelle: Teixeira et al. (2015).

Im Vergleich zu reinen IT-Infrastrukturen fügen die (zusätzlichen) physischen Komponenten bei CPS eine erhebliche Komplexität hinzu, die eine Sicherheitsbewertung erschwert (Rajkumar et al., 2010): Zum einen bedeutet die Komplexitätssteigerung mehr Aufwand für den Angreifer, das System zu verstehen, zum andern gibt es aber auch mehr Einfallstore für Angreifer und dadurch Echtzeitanforderungen, die beim Systemdesign zu berücksichtigen sind. Das erfordert gem. den Ausführungen in Martins et al. (2015) mehr Aufwand aufseiten der Verteidiger, um sich angemessen schützen zu können. Ein generisches Rahmenwerk zur Bewertung von CPS-Security wird in Humayed et al. (2017) vorgeschlagen (siehe Abbildung 12). CPS werden in diesem Rahmenwerk in Cyber-, cyberphysische und physische Komponenten unterteilt. Die drei Komponenten werden hinsichtlich der Parameter Bedrohungen, Vulnerabilitäten, Angriffe und Kontrollen qualitativ bewertet.

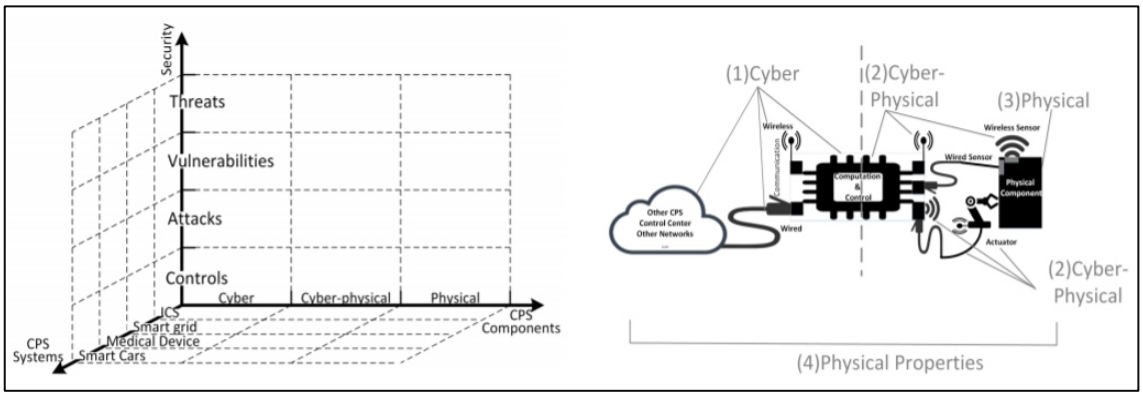


Abbildung 12: CPS-Security-Risikorahmenwerk.
Quelle: Humayed et al. (2017).

In Humayed et al. (2017) werden außerdem potenzielle Bedrohungsquellen in den Anwendungsfeldern Smart Grids, Smart Cars und Medical Devices analysiert. Schwachstellen werden ferner erläutert, und Ursachen für diese Schwachstellen werden anhand konkreter Beispiele erarbeitet. Anschließend werden in Humayed et al. (2017) Sicherheitsmaßnahmen für identifizierte, missbräuchliche Szenarien definiert. Die Zuordnung von Maßnahmen zu Szenarien ist dem Risikoregister nach Harnser (2010, B7, S. 71) aus der physischen Sicherheitsbewertung ähnlich. Im Gegensatz zu vorangegangenen wissenschaftlichen Beiträgen wird in Aigner &

Khelil (2020) die Anwendbarkeit ausgewählter Sicherheitsmetriken für die Risikobewertung von CPS analysiert. Für die Durchführung einer Analyse zur Anwendbarkeit konkreter Sicherheitsmetriken für CPS Use Cases wird in Aigner & Khelil (2020) zunächst eine Reihe von Leitfragen definiert. Ein Beispiel für eine Leitfrage ist: „Can the metric handle the interaction of heterogeneous systems within a CPS environment?“ (Aigner & Khelil, 2020, S. 2). Die Leitfragen werden in Aigner & Khelil (2020) auf die betrachteten Security-Metriken angewendet, das bedeutet, es wird geprüft, ob mittels der Metriken die Leitfragen beantwortet werden können. Insgesamt werden zwölf Security-Metriken betrachtet, wobei zwischen Attack-Detection-Metriken, System-Design-Metriken und Security-Rating-Metriken differenziert wird (siehe Abbildung 13).

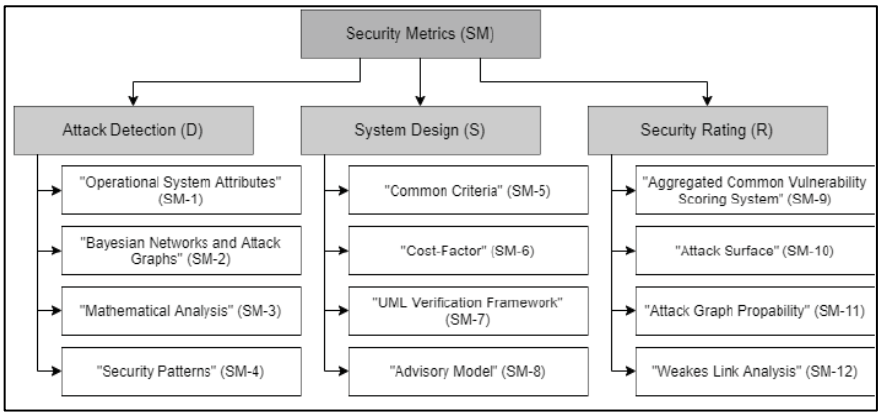


Abbildung 13: Vergleichende Analyse von Security-Metriken für die Eignung zur CPS-Bewertung. Quelle: Aigner & Khelil (2020).

Die Ergebnisse des Benchmarks von Aigner & Khelil (2020) werden in Form einer Matrix dargestellt, nachfolgend am Beispiel der Attack-Detection-Metriken (siehe Tabelle 4): Die Anzahl der beantworteten Fragen wird jeweils gezählt, durch die Gesamtanzahl der gestellten Fragen geteilt. Das Ergebnis wird mit der Zahl 100 multipliziert, um den prozentualen Anteil der beantworteten Fragen zu erhalten. Wie Tabelle 4 entnommen werden kann, können mit der Security-Metrik (SM) „4“ (Security Patterns) alle sieben an die Metrik gestellten Leitfragen beantwortet werden. Im Gegensatz dazu können z. B. mit der SM „1“ (Operational System Attributes) nur 14 % aller gewählten Fragen beantwortet werden. Zu beachten ist, dass nicht jede Frage auf jede Metrik angewendet wird und dass nicht alle dreizehn eingangs definierten Fragen mithilfe der Metriken beantwortet werden können (siehe Abbildung 14). Das zeigt qualitativ punktuelle Stärken, aber auch die Schwächen verfügbarer Security-Metriken auf.

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)

Tabelle 4: Ergebnisse des Benchmarks der Attack-Detection-Metriken. Quelle: Aigner & Khelil (2020).

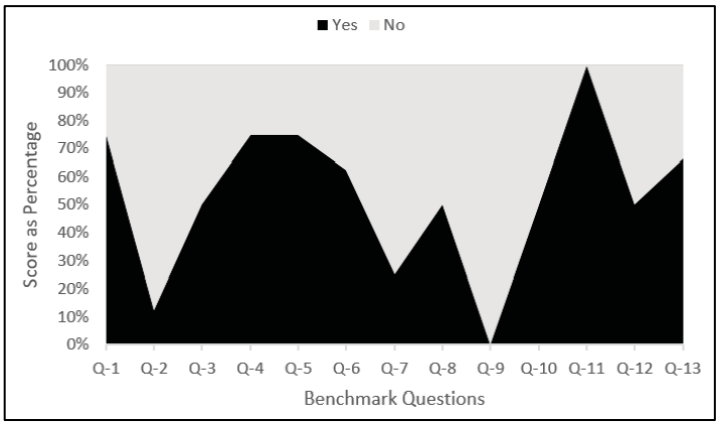


Abbildung 14: Totale Benchmark-Scores nach Fragen.
Quelle: Aigner & Khelil (2020).

Die Sub-Benchmarks nach einzelnen Metrik-Typen werden in einem Gesamt-Benchmark zusammengeführt (Aigner & Khelil, 2020) (siehe Abbildung 15). Das Ergebnis liefert eine Rangliste bezüglich der Anwendbarkeit der betrachteten Metriken für die Risikobewertung von CPS (hier in absteigender Reihenfolge): SM 4, SM 2, (SM 5, SM 7, SM 9, SM 10, SM 11), (SM 6, SM 8, SM 12), SM 3, SM 1.

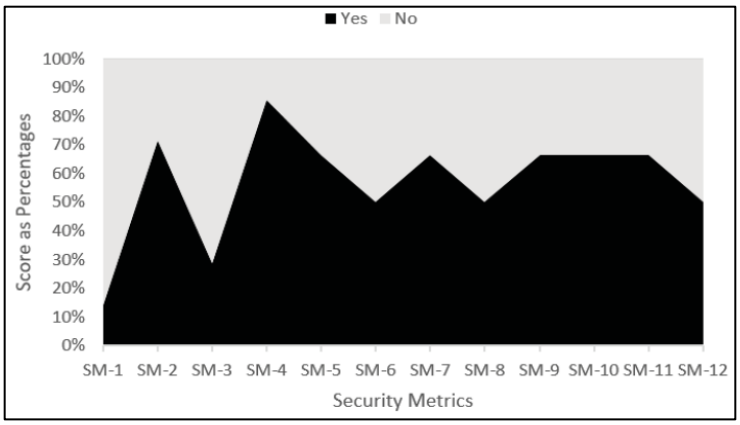


Abbildung 15: Gesamt-Benchmark zu Security-Metriken für CPS.
Quelle: Aigner & Khelil (2020).

Aus den Analyseergebnissen in Aigner & Khelil (2020) wird geschlussfolgert, dass für die Risikobewertung von CPS eine Kombination unterschiedlicher Metriken erforderlich ist. Hierfür wird folgende Option in Aigner & Khelil (2020) genannt: Der Ansatz der aggregierten CVSS-Scores (SM „9“) kann um das Konzept der Attack Surfaces (SM „10“) erweitert und mit Wahrscheinlichkeitsaspekten aus SM „11“ gekoppelt werden (Aigner & Khelil, 2020). Die Notwendigkeit zur Kombination unterschiedlicher Ansätze für die Ermöglichung der Durchführung einer domänenübergreifenden Risikobewertung wird ebenso in Macher et al. (2020a) hervorgehoben. Ein Rahmenwerk zur Quantifizierung von Security in CPS-Anwendungen wird in Aigner & Khelil (2021) vorgeschlagen. Mit dieser Metrik sollen Wechselwirkungen zwischen IT-Assets bewertet werden können. Zunächst werden in Aigner & Khelil (2021) Assets gescort. Einer Score-Kategorie wird ein numerischer Wert zwischen „0“ und „1“, ähnlich dem CVSS-Bewertungsschema, zugewiesen. Nach dem Asset-Scoring (siehe beispielhaft Tabelle 5) folgen u. a. das Scoring der „Impacts“, das Scoring der „Attackers“ und das Scoring der „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

Tabelle 5: Asset Evaluation, Effect Scoring.
Quelle: Aigner & Khelil (2021).

Im Gegensatz zu den bereits vorgestellten Ansätzen werden in Aigner et al. (2021) nicht nur die Auswirkungen eines bestimmten Angriffs auf ein einziges System betrachtet. Es werden auch die vorhandenen Systemtypen innerhalb eines CPS und mehrere Angriffsszenarien (hier: Attack Vectors) analysiert (siehe Abbildung 16).

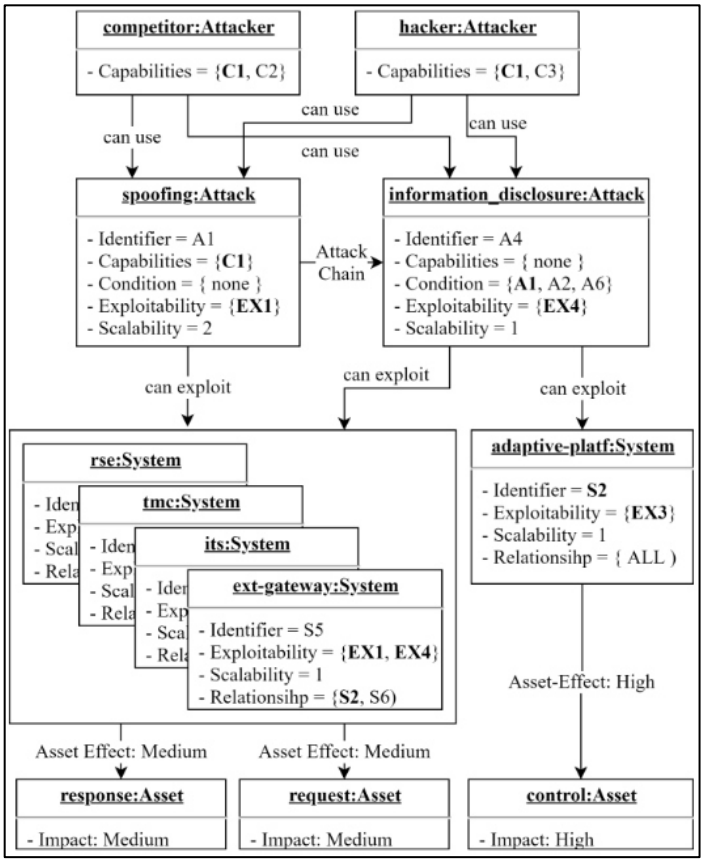


Abbildung 16: Schematische Darstellung des Risikobewertungsprozesses nach Aigner & Khelil (2021).
Quelle: Aigner & Khelil (2021).

Der Kalkulationsmatrix zur Bestimmung des Security-Scores (siehe Abbildung 16 unten) kann entnommen werden, dass numerische Werte, die hinter die Deskriptoren eines Bewertungsparameters geschrieben werden, z. B. addiert und im Zuge des Risikobewertungsprozesses auch multipliziert werden. Bei der in Aigner & Khelil (2021) vorgeschlagenen Metrik handelt es sich um Ordinalwerte (wie z. B. „High“ oder „Medium“). Die Ordinalskala erlaubt aber nur Rangfolgen (größer und kleiner; siehe Kapitel 2.4). Den Deskriptoren werden in Aigner & Khelil (2021) weiterhin numerische Score-Werte zwischen „0“ und „1“ zugewiesen. Hierfür fehlt jedoch in dem Ansatz eine Begründung der Wahl der numerischen Werte.

Die Bewertung von Wechselwirkungen zwischen Bedrohungsszenarien wird ferner in der CVSS-Community diskutiert. In einem Work Item Sheet werden für die „Version 4“ der CVSS-Metriken (aktuell in der Version 3.1 verfügbar, siehe First.org (2022)) Verbesserungsvorschläge

gesammelt (CVSS Work Items, 2022). Sie stammen teils aus der Publikation von Spring et al. (2018). In zwei Beiträgen des Work Item Sheets mit den Titeln „Measure physical "kinetic" outcome of an exploited vulnerability" und „Measure up-stream and/or down-stream "collateral damage" impacts" wird vorgeschlagen, die Wirkung eines erfolgreichen IT-Angriffs auf die physische Domäne bzw. die Wirkung eines physischen Angriffs auf die IT-Domäne durch die Größe „kinetischer Impact" zu beschreiben: „Explore a new metric to measure the direct up and down stream impact of an impacted component" (CVSS Work Items, 2022, S. 9). Ein Lösungsansatz zur konkreten Abbildung des kinetischen Impacts in einer Metrik wird nicht näher dargelegt.

In der IT-Security ist ein klassischer Ansatz zur Identifikation und Kategorisierung von Bedrohungsszenarien STRIDE (S = Spoofing, T = Tampering, R = Repudiation, I = Information Disclosure, D = Denial of Service, E = Elevation of Privilege) (Microsoft Corporation, 2005). STRIDE wurde in den 1990er Jahren von den Ingenieuren Koren Kohnfelder und Praerit Garg bei Microsoft entwickelt. Er wird von Sicherheitsexperten verwendet, um die Frage zu beantworten: „Was kann in dem betrachteten System schiefgehen?". STRIDE ist mit der What-If-Technik vergleichbar, wie sie in der physischen Sicherheitsbewertung nach Harnser (2010, B1, S. 4-6) Anwendung findet. Es wird bei der What-If-Technik gefragt, was für funktionale Auswirkungen entstehen können, wenn ein Systemelement gedanklich aus dem System entfernt wird. Die Bedrohungsmodellierung mit STRIDE kann als ein Sicherheitspendant zum Hazard Analysis and Risk Assessment (HARA) aus der ISO 26262 betrachtet werden (Macher et al., 2015). In Macher et al. (2015) wird vorgeschlagen, STRIDE und HARA zu einem neuen quantitativen Ansatz, der Security-Aware Hazard and Risk Analysis Method (SAHARA), zu kombinieren.

SAHARA sieht vor, Security-Bedrohungen nach den Ressourcen (R) und dem Know-How (K), die für die Durchführung eines Angriffs erforderlich sind, sowie der Kritikalität der Bedrohung (T) zu quantifizieren. R, K und T werden jeweils gescort (siehe Tabelle 6) und in ähnlicher Weise wie bei der Bestimmung des ASIL aus der Safety (ISO 26262-3:2018) in einer Matrix zueinander geordnet (siehe Tabelle 7). Wie Tabelle 6 auf der rechten Seite entnommen werden kann, entspricht die Threat Criticality einer Impact-Kategorie.

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

Tabelle 6: Klassifikation von Know-How und Threat Criticality nach dem SAHARA-Ansatz. Quelle: Macher et al. (2015).

Jede Kombination aus R, K und T stellt ein Security-Level (SecL) zwischen „0" (niedrigstes Level) und „4" (höchstes Level) dar. Bei dem Bewertungsansatz werden Ordinalwerte zueinander in einer Matrix geordnet. Jedes R-K-T-Triplet ergibt im Ergebnis ein Security-Level: „The SecL determination is based on the ASIL determination approach". Und weiter: „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, S. 4). In der Arbeit von Macher et al. (2015) erfolgt demnach eine direkte Zuordnung der SecL zu den ASIL im Verhältnis 1:1: „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, S. 4). Die Bewertung von R, K und T lässt jedoch nur ein Ranking zu. Eine weitere Erkenntnisziehung ist nicht möglich. Weil das so ist, kann nicht gesagt werden, wie viel besser Security-Level „4“ als Security-Level „2“ ist. Das würde ein quantitativer Ansatz aber zulassen. Im Falle eines richtigen quantitativen Ansatzes wäre es möglich, die Bewertungsgrößen und auch die SecL hinsichtlich Größe und Distanz zu vergleichen (siehe auch Kapitel 2.4). Darüber hinaus bleibt im SAHARA-Ansatz die Frage offen, auf welchem Exploitability-Niveau die SecL jeweils basieren und inwieweit sie durch die Anwendung geeigneter Sicherheitsmaßnahmen reduziert werden können.

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

Tabelle 7: Security Level nach SAHARA (links) gegenüber ASIL aus ISO 26262-3:2018 (S. 10) (rechts). Quelle: Macher et al. (2015) (links); eigene Tabelle in Anlehnung an ISO 26262 (rechts).

Zur Anwendung einer TARA liegen bereits durchgeführte Studien für Automotive Networked Embedded Systems vor (Dobaj et al. 2021). In Dürrwang et al. (2021) wird ein Ansatz zur Automatisierung des TARA-Prozesses und des Security-Testings eines Fahrzeugnetzwerks vorgestellt. Dürrwang et al. (2021) führen das Konzept des Attacker Privileges ein, um Zustände zu beschreiben, in welchen Angreifer bestimmte Angriffe durchführen können. Required Privilege Level sind in insgesamt fünf Stufen eingeteilt (siehe Abbildung 17). Jedem identifizierten Angriffspfad aus der TARA wird ein Required Privilege Level (PL) zugewiesen. In Dürrwang et al. (2021) wird argumentiert, dass die Required Privilege Levels als Basis für das Security-Testing dienen können. In Macher et al. (2020a) wird eine TARA am Beispiel eines elektronischen Lenksäulenverriegelungssystems durchgeführt. Im Zuge der TARA in Macher et al. (2020a) wird eine strukturierte Methode zur Integration von Cybersecurity und Functional Safety im Kontext Automotive SPICE angewendet.

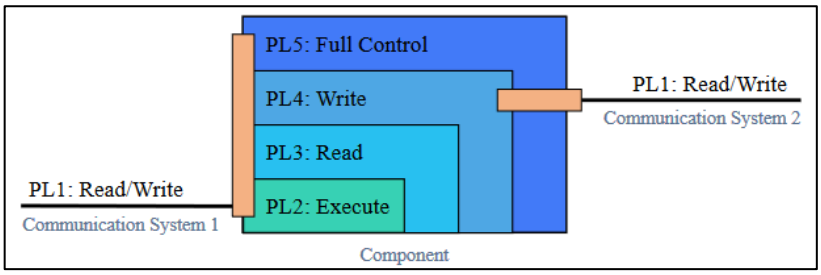


Abbildung 17: Required Privilege Levels. Quelle: Dürrwang et al. (2021).

Zusammenfassend werden verschiedene Ansätze verfolgt, physische Risikobeiträge und IT-Risikobeiträge im Kontext cyberphysischer Anwendungsfälle zu analysieren und zu bewerten. Die Recherche zum aktuellen Stand der wissenschaftlichen Auseinandersetzung mit CPS-Security zeigt jedoch einen Forschungsbedarf bzgl. der Analyse und Bewertung von Wechsel-

wirkungen zwischen beiden Domänen auf. Bisherige CPS-Bewertungsansätze sind weitestgehend qualitativer, deskriptiver Natur und auf einer abstrakten Meta-Ebene, welche die physische Vulnerabilität unberücksichtigt lassen. In Aigner & Khelil (2021) wird sogar ein Rahmenwerk zur Bewertung der Security von CPS definiert, das die IT-Schlüsselcharakteristiken von CPS aufgreift und sich am Industriestandard Common Vulnerability Scoring System (CVSS; First.org, 2022) orientiert. Die Wirksamkeit physischer Sicherungsmechanismen wird jedoch nicht betrachtet. Zudem lassen sich inhärente Verwerfungen bei der Anwendung der vorgeschlagenen semi-quantitativen Metrik identifizieren, wie z. B. das Rechnen mit Werten auf einer Ordinalskala. Schlussfolgernd gibt es bisher keine quantitativen Ansätze zur Synthese von Physical Security und IT Security. Wie im Stand der Forschung zur cyberphysischen Security dargelegt werden kann, liegt ein Forschungsbedarf in der Reduktion von Verwerfungen innerhalb von Metriken sowie in der Reduktion von Inkompatibilitäten zwischen Metriken. Sowohl in der Wissenschaft al auch in der Industrie ist ein Lösungsansatz zur konsistenten Zusammenführung von Metriken aus den Domänen Physical Security und IT Security bzw. Functional Safety und IT Security gefragt. Dieser Forschungsbedarf wird in dieser Forschungsarbeit aufgegriffen. Im Fokus dieser Arbeit liegt die domänenübergreifende Bewertung von Physical Security und IT Security.

2.3 Sicherheit und Risiko

Systemsicherheit kann aus der Benutzer-Perspektive, Betreiber-Perspektive und Versicherer-Perspektive betrachtet werden (Wheeler, 2018, S. 18, 50; Harnser, 2010, S. 1; Gordon et al., 2003). Dabei gibt es eine Dualität von Safety und Security, die das Fundament für die Risikoanalyse bildet. Im deutschen Sprachgebrauch jedoch werden diese unter einem einzigen Begriff, der Sicherheit, zusammengefasst. Im englischsprachigen Raum ist dieser klar differenziert (Newsome, 2013, S. 7; Geiger, 2021). Unter Safety-Gesichtspunkten wird analysiert, wie sich das System auf den Menschen oder die Umwelt auswirkt (Burns et al., 1995). Unfälle werden durch Ereignisse verursacht, die auf gefährliche Systembedingungen zurückzuführen sind. Im Gegensatz zur Safety werden in der Security die Auswirkungen eines Angriffs auf ein System analysiert (Wheeler, 2011, S. 6). Safety meint folglich den Schutz eines Menschen vor einem technischen System, während Security den Schutz eines technischen Systems vor einem Menschen beschreibt (Wurm, 2022, S. 70). Angreifer können dabei sowohl extrinsisch (Hacker, Terroristen, Einbrecher, etc.) als auch intrinsisch (beispielsweise erboste Mitarbeiter) sein (Harnser, 2010, B2, S. 16). Bedrohungsvektoren im Kontext CPS können physisch oder digital auftreten (Kofler et al., 2018, S. 32). Da MAS als CPS kategorisiert sind, gelten beide Bedrohungsvektoren für diese Systeme. Die Folgen von eingetretenen Bedrohungen sind in der Safety und in der Security ähnlich. Eine Ursache für Konsequenzen in der Safety ist beispielsweise technisches Versagen von Hardware (Zio, 2007, S. 1). Dieser Fehlertyp ist stochastisch und die Eintrittswahrscheinlichkeit kann z. B. durch Ermüdungstests bestimmt werden (Bertsche & Lechner, 2006, S. 7 - 8).

Das Ausfallverhalten kann durch Ausfallkurven dargestellt werden (Zio, 2007, S. 50). Menschliche Fehler in Form von Fehlbedienungen sind weitere Ursachen für Ausfälle. Dieser Fehlertyp ist nicht durchgehend stochastisch. In diesem Fall können Experimente verwendet werden, um abzuschätzen, wie wahrscheinlich Fehlbedienungen sind (Ritz, 2015, S. 26, 28, 110). In der Security kommt es dagegen zu vorsätzlichen Angriffen auf ein technisches System oder einen Menschen (Wheeler, 2011, S. 18). Hier ist die Schätzung der Häufigkeiten aufgrund der Willkür eines Angreifers schwieriger (Wheeler, 2011, S. 58, 70). Bei neuartigen Systemen liegen darüber hinaus noch keine historischen Referenzen für Angriffe vor. In der Security findet daher klassischerweise eine prospektive Analyse auf Basis von Szenarien Anwendung (Harnser, 2010, B4, S. 50). Aufgrund vieler unsicherheitsbehafteter Parameter in die Durchführung einer Risikobewertung eine Herausforderung.

Der Risiko-Begriff „is […] a vague notion that carries different meaning under different domain contexts and perspectives." (Wang et al., 2011, S. 1). „Risk is unobservable but we can indirectly measure its realization as losses" (Woods et al., 2021, S. 1). Unter Risiko kann aus Security-Perspektive ein erwarteter Schadensumfang verstanden werden, der durch die Wahrscheinlichkeit des Auftretens und die Schwere eines Schadens beeinflusst wird (Harnser, 2010, B6, S. 64) (siehe Abbildung 18). Bei der Bestimmung von Wahrscheinlichkeit gibt es grundsätzlich zwei Richtungen des statistischen Denkens, die Bayes'sche Perspektive (Grad der Überzeugung) und die frequentistische Perspektive (objektive Wahrscheinlichkeit: zeitliche Häufigkeit) (Vallverdú, 2008).

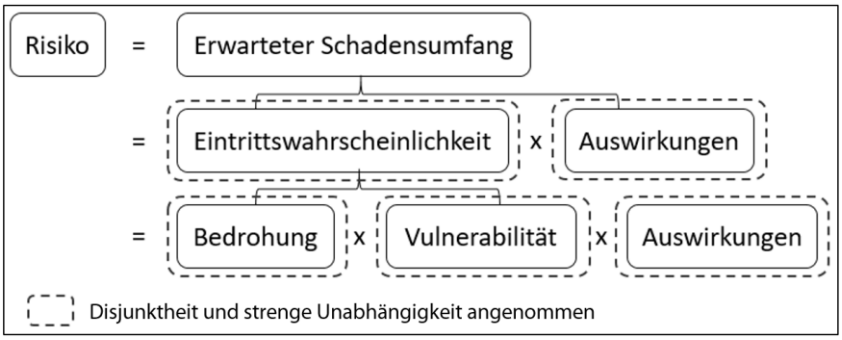


Abbildung 18: Zwei- und dreigliedriges Risikomodell.
Quelle: Eigene Abbildung in Anlehnung an Lichte et al. (2017).

Auswirkungen können auch monetarisiert werden. Das bedeutet, dass sie in geldlichen Werten ausgedrückt werden (Harnser, 2010, B3, S. 39-41). Die Monetarisierung ist notwendig, um unterschiedliche Risiken vergleichbar machen zu können. Bei dieser zweigliedrigen Risikodefinition werden Eintrittswahrscheinlichkeiten mit Auswirkungen verbunden, jedoch muss nicht immer eine Multiplikation die beiden Risikobeiträge[22] miteinander verknüpfen. Sind die Ereignisse der Risikobeiträge disjunkt (unvereinbar), bedeutet das, dass es keine gemeinsame Schnittmenge für die Ereignisse Eintrittswahrscheinlichkeit und Schaden gibt. Eine Kausalität zwischen den Risikobeiträgen wird in dieser Idealisierung ausgeschlossen, d. h. die Eintrittswahrscheinlichkeit und der Schaden sind streng unabhängig voneinander. In solch einem Fall kann das Risiko als Produkt der Einzelwahrscheinlichkeit und des Schadensausmaßes geschrieben werden.

In den Domänen Physical Security und IT Security wird die Eintrittswahrscheinlichkeit weiterhin in die Bedrohung und in die Vulnerabilität aufgeteilt (Lichte et al., 2017; Cheng et al., 2014, S. 4). Die Bedrohung ist die Wahrscheinlichkeit, dass ein Angriff von einem Angreifer mit einem bestimmten Werkzeug stattfindet. In der Security werden vordergründig z. B. Sabotagen oder Attacken analysiert, wohingegen in der Functional Safety Unfälle durch Komponentenversagen oder menschliche Fehler betrachtet werden (siehe Abbildung 19). Für die Bedrohung wird klassischerweise eine frequentistische Sicht eingenommen (beispielsweise 15 Angriffe pro Jahr). Weil im Falle dieser Arbeit Worst-Case-Szenarien für neuartige Systeme betrachtet werden, die noch nicht eingetreten sind, ist eine frequentistische Sicht schwerlich abbildbar. Was jedoch getan werden kann, ist das Einnehmen einer Bayes'schen Sicht (Grad der Überzeugung) (Witte et al., 2020). Im Gegensatz zur physischen Sicherheit oder IT-Security kann die Eintrittswahrscheinlichkeit für eine Bedrohung in der Functional Safety mittels statistischer Methoden quantitativ bewertet werden.

[22] Die Eintrittswahrscheinlichkeit und die Auswirkungen sind z. B. Risikobeiträge. Ein Risikobeitrag gibt in Form eines quantitativen Wertes an, welchen Anteil der jeweilige Risikobeitrag zu einem Risiko leistet. Die Identifikation und Analyse einzelner Risikobeiträge sind wichtig, damit Sicherheitsmaßnahmen erarbeitet werden können, um die Eintrittswahrscheinlichkeit und die Auswirkungen zu reduzieren.

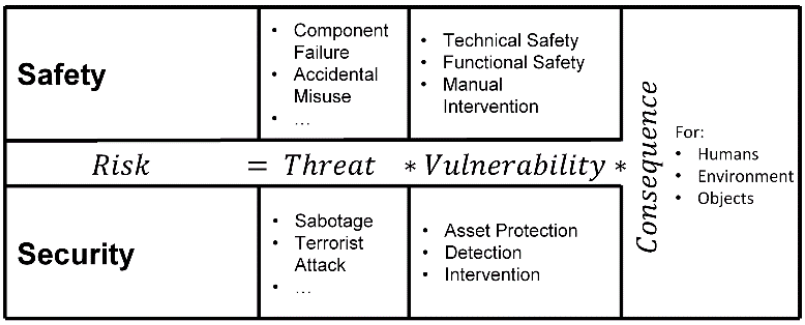


Abbildung 19: Ganzheitliche Risikodefinition von Safety und Security.
Quelle: Lichte et al. (2017).

Die Vulnerabilität umfasst die Wahrscheinlichkeit eines erfolgreichen Angriffs. Disjunktheit und strenge Unabhängigkeit erlauben es hier, dass die einzelnen Risikobeiträge getrennt analysiert und bewertet werden können, z. B. haben dann (aleatorische) Unsicherheiten[23] in der Vulnerabilität keine Ursache-Wirkungs-Zusammenhänge mit der (epistemischen) Unsicherheit[24] in der Bedrohungswahrscheinlichkeit oder den Auswirkungen. Das erleichtert die Risikobewertung, weil unsicherheitsbehaftete Größen, die z. B. stark epistemisch sind, ausgeklammert werden können. Wenn disjunkte Ereignisse vorliegen, dann können Bedrohung, Vulnerabilität und Auswirkungen isoliert bewertet und nach den Einzelbetrachtungen zu einer Risikobewertung zusammengeführt werden. Das Risiko wird üblicherweise als Produkt aus allen drei Risikobeiträgen berechnet. Wenn die Annahmen gemacht werden, dass

a) Bedrohung, Vulnerabilität und Auswirkungen völlig disjunkt sind, und für diesen Idealfall strenge Unabhängigkeit angenommen wird,
b) ein System im Angriffsfall bewertet wird (Worst-Case-Szenario; P(Bedrohung) = 100 % als Grad der Überzeugung),

dann kann die Risikobeschreibung „Risiko = Bedrohung · Vulnerabilität · Auswirkung“ vereinfacht werden (siehe Gl. (1)):

$$\begin{aligned} &\text{Risiko} = \text{Bedrohung} \cdot \text{Vulnerabilität} \cdot \text{Auswirkung} \mid \text{Annahme: Angriffsfall, P(Bedrohung)} = 100\,\% \\ &\text{Risiko} = 100\,\% \cdot \text{Vulnerabilität} \cdot \text{Auswirkung} \\ &\text{Risiko} = 1 \cdot \text{Vulnerabilität} \cdot \text{Auswirkung} \\ &\text{Risiko} = \text{Vulnerabilität} \cdot \text{Auswirkung} \end{aligned} \tag{1}$$

Zu beachten ist, dass die alleinige Multiplikation von der Vulnerabilität und den Auswirkungen ohne Berücksichtigung der Bedrohung nicht gleichbedeutend mit dem Risiko ist. Ohne den Bedrohungsanteil ist Risiko lediglich eine mit der Auswirkung gewichtete Vulnerabilität. Das Risiko aber bemisst, wie wahrscheinlich der Eintritt eines i. d. R. unerwünschten Ereignisses ist (bestehend aus einem Bedrohungsanteil sowie einem Vulnerabilitätsanteil) und wie groß der mögliche Schaden im Falle dieses Ereigniseintritts ist (Lichte et al., 2016). Die Bedrohungswahrscheinlichkeit ist folglich ein essentieller Bestandteil einer Risikobewertung. Für die Entwicklung risikogerechter Metriken müssen folglich alle drei Risikobeiträge, Bedrohung, Vulnerabilität und Auswirkungen, betrachtet werden. Diese Forschungsarbeit konzentriert sich jedoch auf den Vergleich von Metriken zur Bewertung der Vulnerabilität und den Auswirkungen in der physischen Sicherheit und in der IT-Sicherheit. Hierfür wird die Vereinfachung aus Gl. (1) zugrunde gelegt.

[23] Aleatorische Unsicherheiten entstehen durch natürliche und zufällige Schwankungen.
[24] Epistemische Unsicherheiten entstehen durch unvollständiges Wissen.

Je größer die Auswirkung ist, desto größer ist auch das Interesse eines Betreibers, die Bedrohungswahrscheinlichkeit und die Vulnerabilität zu senken (Harnser, 2010, B3, S. 39-41). Bei der physischen Security-Risikobewertung ist es gängige Praxis, den Vulnerabilitätsanteil des dreigliedrigen Risikomodells zu bewerten. Zum einen kann über die Vulnerabilität die Wirkung von Eigenschaften einer Sicherungsmaßnahme im Sinne einer Vulnerabilitätsreduktion bei konkreten Szenarien bewertet werden (Garcia, 2005, S. 20). Zum andern kann ein Betreiber anhand einer Vulnerabilitätsbewertung Cost-Benefit-Analysen durchführen (Wheeler 2011, S. 8). Vulnerabilität ist aus Verteidigersicht das Steuerungsinstrument in der Security-Risikobewertung. Sowohl in der physischen Risikobewertung, z. B. nach Lichte et al. (2016) oder Garcia (2005), als auch in der IT-Risikobewertung, z. B. nach CVSS (First.org, 2022) oder OWASP[25] (Williams, 2022), wird Risiko klassischerweise anhand von Vulnerabilitätsbeiträgen und Auswirkungsbeiträgen bewertet; vorausgesetzt, es gilt die Annahme, dass das System auch angegriffen bzw. eine Schwachstelle ausgebeutet wird (siehe Gl. (1)).

Für die Bewertung von Risiken müssen Metriken für die Bedrohung, Vulnerabilität und Auswirkungen eingeführt werden. Diese beschreiben die einzelnen Risikobeiträge. Es sind ebenso Modelle notwendig, die an bestimmte Randbedingungen und Expertenwissen gebunden sind (Bandow & Holzmüller, 2009, S. IX). Im Gegensatz zu der Risikobewertung von kritischen Infrastrukturen (KRITIS), bei denen umweltliche Randbedingungen weitestgehend statisch sind, muss bei der Security-Risikobewertung von MAS auch die Use-Case-spezifische Dynamik berücksichtigt werden können (Möller et al., 2019, S. 304-306). Use-Case-spezifische Randbedingungen machen die Messung von Risiken sowie die Erfassung von Unsicherheiten zusätzlich kompliziert, weswegen eine gut durchdachte Vorgehensweise zur Durchführung einer Bedrohungsanalyse und Risikobewertung solcher Systeme notwendig ist.

2.4 Metriken

Ausgangspunkt für die Messung von Risiken bilden Metriken (Wheeler, 2011, S. 38, 39, 229). Eine Metrik ist ein Verfahren zur Messung von quantifizierbaren Einheiten oder Größen (Sowa, 2011, S. 4; Stephens, 1946). Sie ist ein Entscheidungshilfsmittel für das Management zur Verbesserung der Sicherheit (Arabsorkhi & Ghaffari, 2018). „Die Hauptaufgabe von Metriken ist es, über Kennzahlen den Stand und die Auswirkung von Einflussfaktoren […] sichtbar, vergleichbar, bewertbar und verfolgbar zu machen" (Broy et al., 2013, S. 334). In Katsikas et al. (2005) wird das Hauptziel von Metriken dergestalt definiert: „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, S. 150). In Cheng et al. (2014) wird das Ziel von Sicherheitsmetriken folgendermaßen beschrieben: „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, S. 3).

Das National Institute of Standards and Technology (NIST) versteht unter Metriken Werkzeuge, um die Entscheidungsfindung durch die Sammlung, Analyse und Berichterstattung relevanter leistungsbezogener Daten zu erleichtern und zu verbessern (Cheng et al., 2014, S. 2-3). Um Produktsicherheit zu verbessern, ist eine Sicherheitsbewertung notwendig, denn „If you can't measure it, you can't manage it" (Drucker, 2015, S. 685). Eine nützliche Bewertung hängt von der Wahl einer geeigneten Metrik ab (Arabsorkhi & Ghaffari, 2018). Nützlich bedeutet, dass das Management gute Entscheidungen bzgl. des Investments von Ressourcen in Sicherheitsmaßnahmen treffen kann. Hierfür ist es erforderlich, zu verstehen, welche Eigenschaften eine Metrik haben muss, um eine gute Entscheidungsgrundlage zu schaffen. In Arabsorkhi & Ghaffari (2018) werden zwei Kategorisierungsmöglichkeiten von erforderlichen Eigenschaften einer

[25] OWASP: Open Web Application Security Project.

guten Security-Metrik dargelegt, CORES und PRAGMATIC. CORES umfasst insgesamt fünf Kriterien:

- **C**larity (Klarheit): Einfach interpretierbar
- **O**bjectiveness (Objektivität): Unbeeinflusst von persönlicher Meinung
- **R**epeatability (Wiederholbarkeit): Erzielung gleicher Ergebnisse bei denselben Bewertungsbedingungen
- **E**asiness (Einfachheit): Leichte Anwendbarkeit der Bewertungsmetrik
- **S**uccinctness (Prägnanz): Genauigkeit der Bewertungsmetrik bzw. Nutzen für die Zielgruppe

PRAGMATIC besteht dagegen aus neun Eigenschaften:

- **P**redictive (Vorhersagbarkeit): Gute Vorhersage von Ergebnissen
- **R**elevant (Bedeutsamkeit): Die Metrik bewertet Security-Aspekte
- **A**ctionable (Verwertbarkeit): Die Metrik unterstützt die Entscheidungsfindung
- **G**enuine (Echtheit): Unzweideutigkeit und Korrektheit der Informationen, die in die Metrik eingespeist werden.
- **M**eaningful (Aussagekraft): Einfache Interpretierbarkeit
- **A**ccurate (Präzision): Genauigkeit der Ergebnisse
- **T**imely (Rechtzeitigkeit): Minimierung der Zeit zwischen Datensammlung und Datenauswertung
- **I**ndependent (Unabhängigkeit): Vollständig, verifizierbar und korrekt
- **C**heap (Kostengünstigkeit): Analyse der Metrik ist mit geringem, kapazitivem Aufwand verbunden.

In Broy et al. (2013, S. 336) werden im Bereich des Software Engineerings insgesamt folgende Prinzipien definiert, die eine gute Metrik zu erfüllen hat: Objektivität, Messgenauigkeit, Aussagekraft und Tauglichkeit, Vergleichbarkeit, Angemessenheit des Aufwands sowie Nützlichkeit. Die erforderlichen Eigenschaften der drei genannten Möglichkeiten zur Beschreibung guter Security-Metriken können einander zugeordnet werden, wie beispielhaft in Tabelle 8 zu sehen.

CORES	PRAGMATIC	Software Engineering
Clarity (Klarheit): Einfach interpretierbar	Actionable (Verwertbarkeit): Die Metrik unterstützt die Entscheidungsfindung; Meaningful (Aussagekraft): Einfache Interpretierbarkeit	Aussagekraft und Tauglichkeit, Nützlichkeit
Objectiveness (Objektivität): Unbeeinflusst von persönlicher Meinung	Independent (Unabhängigkeit): Vollständig, verifizierbar und korrekt	Objektivität
Repeatability (Wiederholbarkeit): Erzielung gleicher Ergebnisse bei denselben Bewertungsbedingungen	Predictive (Vorhersagbarkeit): Gute Vorhersage von Ergebnissen Timely (Rechtzeitigkeit): Minimierung der Zeit zwischen Datensammlung und Datenauswertung	Vergleichbarkeit
Easiness (Einfachheit): Leichte Anwendbarkeit der Bewertungsmetrik	Cheap (Kostengünstigkeit): Analyse der Metrik ist mit geringem, kapazitivem Aufwand verbunden.	Angemessenheit des Aufwands
Succinctness (Prägnanz): Genauigkeit der Bewertungsmetrik bzw. Nutzen für die Zielgruppe	Relevant (Bedeutsamkeit): Die Metrik bewertet Security-Aspekte Genuine (Echtheit): Unzweideutigkeit und Korrektheit der Informationen, die in die Metrik eingespeist werden. Accurate (Präzision): Genauigkeit der Ergebnisse	Messgenauigkeit

Tabelle 8: Zuordnung von metrischen Eigenschaften.
Quelle: Eigene Tabelle in Anlehnung an Broy et al. (2013) und Arabsorkhi & Ghaffari (2018).

Security-Metriken sollen nicht nur die genannten Eigenschaften erfüllen. Sie müssen auch nach gängigen Industriestandards und unternehmerischen Zielen ausgerichtet werden (Cheng et al., 2014, S. 2). Mit Metriken sollen definierte Eigenschaften eines Produkts, eines Entwicklungsprozesses oder eines Projekts erfasst werden können, sodass die Erfüllung von Anforderungen seitens des Kunden oder des internen Managements geprüft werden kann (Broy et al., 2013, S. 335). Dafür ist eine Messung von Einflussgrößen auf die Anforderungskriterien erforderlich. Nach Hubbard et al. (2016) ist in den Entscheidungswissenschaften eine Messung „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, S. 21). „Uncertainty" ist nach Hubbard et al. (2016) „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, S. 29).

Dadurch, dass beim Messen unterschiedliche Größen im Vordergrund stehen, gibt es unterschiedliche Sichten auf Metriken. In Broy et al. (2013, S. 335) wird zwischen der Managementsicht (Kundenzufriedenheit, Kosten, Produktivität), der Entwicklersicht (Effizienz, Wartbarkeit) und der Kundensicht (Termintreue, Kosteneinhaltung, Produktqualität, Sicherheit) differenziert. Um eine geeignete Metrik auszuwählen, müssen die Funktionsweise einer Metrik und ihr jeweiliger Anwendungsumfang verstanden werden (Arabsorkhi & Ghaffari, 2018). Der Anwendungsumfang beschreibt, was wie in welchem Ausmaß (für wen) bewertet wird (Broy et al., 2013, S. 336). Zur Bewertung von Security gibt es eine Vielzahl an Metriken, wie z. B. in Sowa (2011), Wang et al. (2017), Arabsorkhi & Ghaffari (2018) oder Cheng et al. (2014) dargelegt wird. In Broy et al. (2013) wird in Bezug auf die Anwendung von Metriken eine generelle Warnung ausgesprochen: „Auch, wenn eine Metrik komplizierte Formeln verwendet, sagt das nichts über die Gültigkeit der dadurch ermittelten Zahlen im Hinblick auf die Messgröße aus" (Broy et al., 2013, S. 338).

Metriken können qualitativer, semi-quantitativer oder quantitativer Art sein (Newsome, 2013, S. 104 – 106) (siehe Abbildung 20). Die qualitative Bewertung entspricht der Compliance, d. h. es liegt eine Liste an notwendigen Elementen vor, die sukzessive auf Vorhandensein geprüft und abgehakt werden (Harnser, 2010, B4, S. 46). Sie dient dazu, dass bei dem Systemdesign auch keine Sicherheitsmaßnahme vergessen wird.

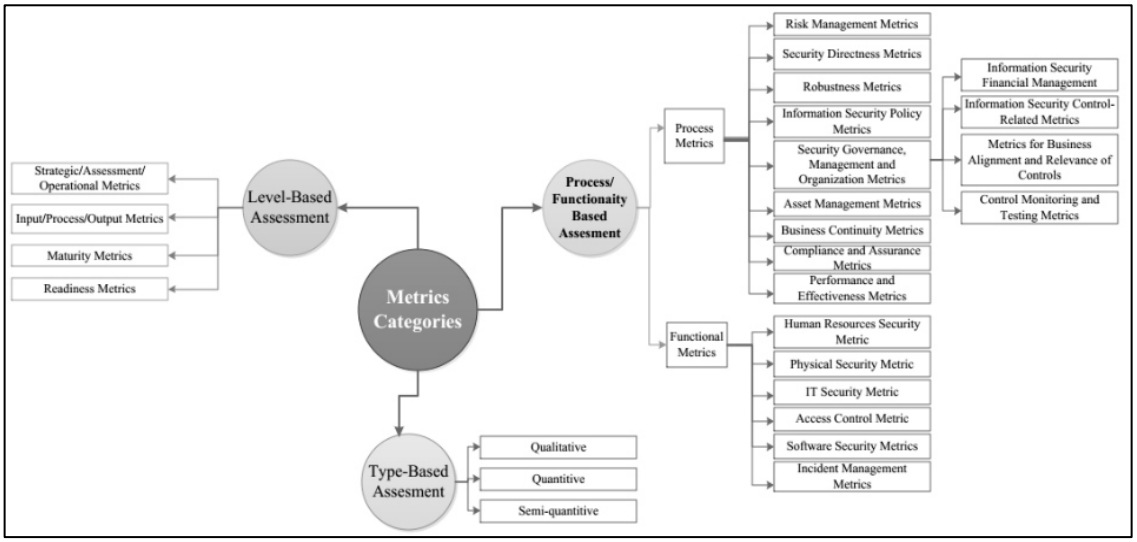


Abbildung 20: Taxonomie von Metriken.
Quelle: Arabsorkhi & Ghaffari (2018).

Im Wesentlichen sagt das Vorliegen z. B. bestimmter Barrieren („ein Zaun und eine Mauer sind vorhanden") jedoch noch nichts darüber aus, wie gut diese im Anwendungsfall dabei sind, einen konkreten Angreifer zu verzögern. Wird eine Messlatte angelegt, die Aussagen wie „etwas ist größer, kleiner oder gleich" erlaubt, dann ist die Bewertung semi-quantitativ (Newsome, 2013, S. 105). Es kann nur gesagt werden, dass beispielsweise bestimmte Maßnahmen effektiver sind als andere, ohne genau in absoluten Zahlenwerten zu benennen, inwiefern („x-mal so viel"). In der IT-Security finden qualitative und semi-quantitative Ansätze breite Anwendung, z. B. beim CVSS (First.org, 2022) oder bei der Open Web Application Security Project (OWASP) Risk Rating Methodology (Williams, 2022). Quantitative Ansätze ermöglichen die Berechnung von Eintrittswahrscheinlichkeiten und monetären Aufwänden. Monetäre Aufwände (z. B. Verluste durch erfolgreiche Angriffe) sind klassischerweise mit der Eintrittswahrscheinlichkeit eines Schadensereignisses verknüpft. In der physischen Security wird ein solcher Ansatz z. B. durch den Einsatz der Vulnerabilitätsmetrik nach Lichte et al. (2016) verfolgt.

Metriken können auch nach dem Applikationstyp unterschieden werden. Security-Bewertungen auf Top-Management-Ebene können strategischer Art sein. Darüber hinaus sind Security-Bewertungen auf mittlerer Management-Ebene und auf der unteren Management-Ebene möglich. Auf der mittleren Ebene kommen klassischerweise exekutive Metriken zum Einsatz. Exekutive Metriken beziehen sich auf die unternehmerische Prozessreife. Auf der unteren Ebene werden operative Metriken verwendet, mit denen beispielsweise die Release Readiness von Hardware und Software bewertet wird (Arabsorkhi & Ghaffari, 2018). Eine dritte Kategorisierung von Metriken ist nach dem zu bewertenden Prozess bzw. der zu bewertenden Funktionalität möglich. Metriken zur Messung von physischer Security und IT-Security können der funktionalen Metrik-Gruppe zugeordnet werden. In Ahmed et al. (2019) werden acht Arten von IT-Security-Metriken unterschieden: Vulnerability Assessment Metric, Red and Blue Teaming Metric, Indicators of Attack Metric, Resilience Metric, Indicators of Compromise, Penetration Testing Metric, Riks Assessment Metric sowie Intelligence Drive Defence Metric.

Beispiele für Metriken sind in verschiedenen Anwendungsfeldern zu finden: Linguistische Maße (wie gesprochen wird), strukturelle Maße (wie was aufgebaut ist) (Sowa, 2011, S. 2), Prozessmaße (wie etwas abläuft) (Torgerson, 2007), Systemmaße (wie etwas bemaßt wird) (Grossert, 1989) und probabilistische bzw. statistische Maße (wie Zufallsereignisse erfasst werden) (Gracia, 2007). Bei letzterem geht es um die Erfassung der Eintrittswahrscheinlichkeit von Ereignissen. Systemmaße und probabilistische bzw. statistische Maße finden im Rahmen der Risikoanalyse besondere Beachtung. Metriken, welche im Security-Kontext zur Bewertung von Situationsbewusstsein (Situational Awareness) verwendet werden, können ferner in objektive Maße, subjektive Maße, Performanz-Maße und Verhaltensmaße eingeteilt werden (Cheng et al., 2014, S. 5-6). Ein zentrales Werkzeug zur Darstellung der Ergebnisse einer Messung sind Skalen (Sowa, 2011, S. 54, 107-111). Ein Skalen- bzw. Messniveau beschreibt eine wichtige Eigenschaft von Merkmalen in der Empirie (Opiera et al., 2016). Empirie umfasst eine methodisch-systematische Sammlung von Daten nach bestimmten Kriterien (Sowa, 2011, S. 58). Das ist ein zentraler Teil in der Risikoanalyse und Risikobewertung von CPS. Skalen können nach DIN EN ISO/IEC 27000:2017-10 systematisiert werden (DIN e.V., 2018). Skalenniveaus werden unterschieden in „nominal-skaliert", „ordinal-skaliert" und „verhältnisskaliert" (Nullpunkt/Referenz gegeben) (Stevens, 1946; Krisper, 2021) (siehe Tabelle 9). Mit nominalen Skalen werden Eigenschaften kategorisiert (Hubbard et al., 2016, S. 22-24). Es ist feststellbar, ob eine Eigenschaft häufiger, weniger oder gleich häufig auftritt. Mess- und damit darstellbar sind nur Häufigkeiten. Es kann keine Aussage darüber getroffen werden, ob etwas im Rang höher oder niedriger, schlechter oder besser ist. Nur einsehbar ist die absolute Häufigkeit.

Wenn Nominalskalen verwendet werden, dann kann über die Ergebnisse ausgesagt werden, ob sie gleich oder ungleich sind. Die Beschreibung der Verhältnismäßigkeit einzelner Kategorien kann über die mathematischen Operatoren „ $= und \neq$ " vorgenommen werden. Die Ordinalskala bildet die Steigerung der Nominalskala, Bei dieser Skala kann sortiert werden (siehe Abbildung 21). Es gibt jedoch keinen Bezugspunkt. Mittels einer Ordinalskala ist die Festlegung einer Reihenfolge möglich (z. B. Bundesligatabelle, wobei der Platz über Punkte und diese über bestimmte Eigenschaften ausgedrückt werden). Mit der Ordinalskala ist mathematisch ein erweitertes Feld gegeben, in dem mit Operatoren Ränge definiert werden können $(=, \neq$ bzw. $> \text{oder} <)$. Neben einer Häufigkeitsangabe kann eine Abstufung gemacht werden. Diese Art Metrik findet in der Vulnerabilitätsanalyse nach Harnser (2010, B4, S. 46) sowie Schwerdtfegers Leifragenkatalog gemäß Common Criteria (CC) Anwendung (Schwerdtfeger, 2018). Weitere mathematische Operationen sind mit Ordinalwerten nicht möglich. Die Anwendung der Ordinalskala ermöglicht keine weitere Erkenntnisziehung. Dafür ist eine Kardinalskala vonnöten. Sie ist einerseits unterteilt in die Intervallskala und andererseits in die Verhältnisskala.

Skalentyp		Messeigenschaft	Mathematische Operatoren	Durchführbare Operation	Lageparameter	Beispiel
Nominal		Häufigkeit	=, ≠	Gruppierung	Modus	Postleitzahl
Ordinal		Häufigkeit, Rangfolge	=, ≠, >, <	Sortierung	Median	Noten
Kardinal	**Intervall**	Häufigkeit, Rangfolge, Abstand	=, ≠, >, <, +, −	Vergleich	Arithmetisches Mittel	Datum
	Verhältnis	Häufigkeit, Rangfolge, Abstand, Nullpunkt	=, ≠, >, <, +, −, x, /	Verhältnis	Geometrisches Mittel	Alter

Tabelle 9: Skalentypen und messbare Eigenschaften innerhalb der Skalentypen.
Quelle: Eigene Tabelle in Anlehnung an DIN e.V. (2018) und Witte (2018, S. 8).

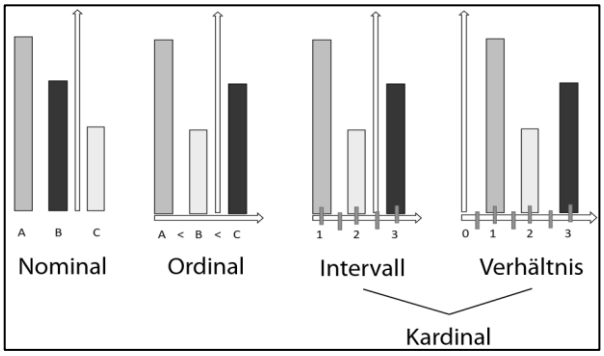


Abbildung 21: Schematische Abstraktion von Skalentypen.
Quelle: Eigene Abbildung in Anlehnung an DIN e.V. (2018, S. 8).

Bei der Intervallskala kann innerhalb der definierten Intervalle addiert und subtrahiert werden (Braband, 2019). Es ist auch feststellbar, wie groß der Abstand zwischen einzelnen Häufigkeiten ist. Der Abstand zwischen zwei Messungen kann selbst bestimmt werden, z. B. durch die Einführung einer definierten Zeitskala, die fortlaufend mit willkürlich festgelegtem Nullpunkt ist, oder durch die Logarithmierung zu einer Basis (Braband, 2008). Dieser künstliche Nullpunkt kann unterschiedlich gesetzt werden, wie z. B. zu sehen bei dem Vergleich des chinesischen Kalenders mit dem islamischen Kalender oder europäischen Kalender. Durch Intervallskalen können Merkmalsdifferenzen festgelegt werden. Über die Addition bzw. Subtraktion ist ersichtlich, wie weit etwas auseinanderliegt. Die übergeordnete Skala ist die Verhältnisskala (Puhani, 2020, S. 9-10). Diese Skala erlaub die Bestimmung der Häufigkeit, des relativen Abstands und der Rangfolge. Zusätzlich zur Intervallskala wird hier ein fester Nullpunkt eingeführt. Über diesen natürlichen Punkt ist der absolute Abstand einer Häufigkeit darstellbar. Wahrscheinlichkeitsrechnung lässt sich insbesondere mit dieser Skalenform realisieren (Lichte et al., 2016). In Newsome (2013, S. 103-107) wird dargelegt, dass verschiedene Behörden und

Institutionen inkompatible Skalen sowie inkompatible quantitative Interpretationen der qualitativen Ausdrücke, wie z. B. „frequent" oder „unlikely", verwenden.

Ein Analyst muss sich demzufolge die Frage stellen, was die Voraussetzungen einer guten Metrik sind und was Schwächen sein können (Krisper, 2021). Eine gute Metrik erlaubt im Allgemeinen die unabhängige Betrachtung von Teilbereichen des Risikos. Zum Beispiel kann auf Basis der Annahmen des dreiteiligen Risikomodells in Kapitel 2.3 eine separate Vulnerabilitätsanalyse durchgeführt werden, ohne dass dies Einfluss auf die Bedrohung oder die Auswirkung hat (Lichte et al., 2016). Eine gute Metrik lässt im Allgemeinen Schlüsse aus Teilbereichen auf das Ganze zu. Ist (mathematisch) eine Trennung der Parameter nicht möglich, so sind die Ergebnisse einer Risikobewertung so unscharf wie die unsicherste Information in dem gesamten Bewertungsprozess (Lichte et al., 2020a; Saltelli et al., 2010, Preface). Eine Metrik muss nicht das ganze Risiko bestimmen können, sondern es erlauben, auf Basis der entkoppelten Analyse und Bewertung von Teilbereichen gut begründete Entscheidungen herbeiführen zu können. Eine Risikobewertung mit einer guten Metrik kann zu einer risikogerechten Verteilung knapper Ressourcen in Maßnahmen führen (Lichte et al., 2019; Cheng et al., 2014, S. 27; Virlics, 2013). Für die Zusammenführung der physischen Security-Bewertung und der IT-Security-Bewertung ist die Wahl einer geeigneten Metrik eine Herausforderung, wie insbesondere in den Kapiteln 2.1 und 2.2 dargelegt wird.

2.5 Bewertungsansätze in der Security

Qualitative und semi-quantitative Risikobewertungsansätze sind sowohl in der physischen Security als auch in der IT-Security weit verbreitet. Physische Sicherheit ist stark standardisiert (Walz, 1992; Charter Global, 2020; Schwerdtfeger, 2018). Modelle und Metriken sind bereits international etabliert und es gibt klare Vorgaben für die Gestaltung sog. physischer Protektionssysteme (PPS) (Garcia, 2005, S. 3). Metriken und Modelle in der IT-Security sind dagegen noch recht neu. Im Gegensatz zur physischen Security zeigen sich größere Herausforderungen bei der Quantifizierung von Vulnerabilität durch Angriffsszenarien (Wang et al., 2017, Preface). Anders als die physische Sicherheit ist die IT-Sicherheit noch unreif:

> 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, S. 1).

In der IT-Security bietet zum Beispiel die Factor Analysis of Information Risk (FAIR) des FAIR Instituts einen Ansatz zur Quantifizierung von Risikovariablen (FAIR 2021). Dieser setzt aber voraus, dass die sog. Loss Event Frequency bestimmt werden kann, also Evidenz vorliegt. „[…] das wesentliche Problem [bei der Bedrohungsanalyse] ist, dass der oder die Angreifer i. d. R. vorab nicht bekannt sind bzw. erst nachdem ein Angriff stattfand und erkannt wurde" (Wurm, 2022, S. 33). Wenn Szenarien betrachtet werden, die noch nicht eingetreten sind, ist die Bestimmung der absoluten Wahrscheinlichkeit schwer abbildbar (Witte et al., 2020). In Hubbard et al. (2016) wird festgestellt:

> 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, S. xii).

In Woods et al. (2021) wird die Herausforderung bei der Quantifizierung in der IT-Security-Domäne folgendermaßen beschrieben:

> 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, S. 12-13).

In Aldasso et al. (2016) wird ferner festgestellt: „However, cyber costs are [also] difficult to quantify" (Aldasso et al., 2016, S. 2). Der Mangel an Daten ist schlussfolgernd eine zentrale Hürde bei der quantitativen Bewertung. In Malavasi et al. (2022) heißt es hierzu: „The scarcity of good quality datasets is a common limitation among the many areas of study on cyber risk" (Malavasi et al., 2022, S. 30). Trotz der Herausforderungen in der Quantifizierung von IT-Risikobeiträgen wird in Hubbard et al. (2016) der Einsatz probabilistischer Ansätze wie folgt verteidigt:

> 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 not need probabilistic models at all. (Hubbard et al., 2016, S. 102).

Aufgrund eines fehlenden, objektiven Wirkmechanismus in der IT-Security, mit dem der Effekt von Maßnahmen zur Reduktion von Vulnerabilität bewertet werden könnte, sind Compliance- und Scoring-basierte Ansätze breit vertreten. Beispiele für Scoring-basierte Metriken sind z. B. das CVSS (First.org, 2022), E-Authentication Guidance for Federal Agencies, kurz OMB M-04-04 (NIST, 2021), oder an OMB M-04-04 angelehnte Bewertungen. Dazu gehören beispielsweise Kantara (Kantara 2021) oder InCommon (2013). Mit den letzten drei Ansätzen werden Spezifikationen des Identitätsmanagements bewertet, wohingegen z. B. CVSS aus unterschiedlichen Metriken besteht, mit denen von der Ausbeutbarkeit einer systeminhärenten Schwachstelle und den Auswirkungen einer ausgebeuteten Schwachstelle auf einen Vulnerabilitäts-Score geschlossen wird: „This score runs from 0.0 to 10.0, in increments of 0.1, giving 101 potential degrees of severity" (Chester, 2021).

In der IT-Security ist das CVSS in der Version 3.1 „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 wird auch in der ISO/SAE 21434 als eine Möglichkeit zur Bewertung der Attack Feasibility (Angriffsdurchführbarkeit) von Bedrohungsszenarien vorgeschlagen (ISO/SAE, 2021b, S. 47). Den CVSS-Metriken ähnlich sind z. B.: 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) und die Open Web Application Security Project (OWASP) Rating Methodology (Williams, 2022).

Insbesondere in der IT-Security ist es gängige Praxis, eine Pseudoquantifizierung vorzunehmen, um Risiken zu bewerten. Beispielsweise werden in Kandasamy et al. (2020) „Risk Likelihood Factors" gewichtet. Gewichtungsgrößen für die Eintrittswahrscheinlichkeit und Gewichtungsgrößen für die Auswirkungen werden in Kandasamy et al. (2020) miteinander multipliziert, um einen Risikowert für ein Bedrohungsszenario zu erhalten. Ein Beispiel für eine solche „Pseudoquantifizierung" aus der physischen Security ist die modular aufgebaute Performance Risk-based Integrated Security Methodology (PRISM). Die Methodologie ist ein wesentlicher Bestandteil des Harnser Reference Security Management Plans (RSMP), der im Auftrag der Europäischen Kommission (EK) entstanden ist und das Sicherheitsmanagement kritischer Infrastrukturen (KRITIS) verbessern soll. Er basiert u. a. auf dem DuPont-Schema aus dem Jahre

1919, einem Kennzahlensystem der Betriebswirtschaftslehre (Weber et al., 1999). Es besteht aus einer Bedrohungs-Metrik, einer Vulnerabilitäts-Metrik und einer Impact-Metrik. Vulnerabilität wird bei der Harnser-Metrik über die Elemente des Schutzes (Protektion), der Beobachtung und Erkennung (Detektion) und der Reaktion (Intervention) bewertet. Über unterschiedliche Arten der Score-Kombination, u. a. Summen-, Mittelwert- und Produktbildung, werden die Ausprägungen die Risikobeiträge, bestehend aus Bedrohungsanteilen, Vulnerabilitätsanteilen und Auswirkungsanteilen, zu einem Risiko-Score aggregiert.

In der IT-Security ist eine wirksamkeitsbasierte Bewertung schwerlich zu finden. Zur Ermöglichung einer wirksamkeitsbasierten Bewertung von Sicherheitsmaßnahmen in der physischen Sicherheit gibt es bereits Metriken: In der physischen Sicherheit wird das Zusammenspiel der Protektion, Observation bzw. Detektion und Intervention z. B. im Vulnerabilitätsmodell nach Garcia (2005) und Lichte et al. (2016) quantitativ durch eine darunterliegende, zeitbasierte Metrik abgebildet. In Garcia (2005) werden diskrete Zeitwerte für die drei Bewertungsgrößen angenommen. In Lichte et al. (2016) werden darüber hinaus Unsicherheiten durch Annahme von Dichtefunktionen für die Bewertungsparameter berücksichtigt. Die Anwendung dieses Ansatzes ermöglicht die Berücksichtigung von scharfen Vulnerabilitätskriterien in der Security-Risikobewertung:

> 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, S. 7).

Ein ebenso zeitbasierter Ansatz wird darüber hinaus beim Estimate of Adversary Sequence Interruption (EASI) Model und seinen Ableitungen verwendet (Garcia, 2007, S. 251-263; Bennett 1977; Bowen et al., 2021). Zu den Ableitungen gehören beispielsweise Analytic System and Software for Evaluating Safeguards and Security (ASSESS), Forcible Entry Safeguards Effectiveness Model (FESEM), Safeguard Effectiveness Model (ISEM), Safeguards Automated Facility Evaluation (SAFE), System Analysis of Vulnerability to Intrusion (SAVI) und Safeguards Network Analysis Procedure (SNAP). In der IT-Security-Bewertung verbreitet sind darüber hinaus die Common Criteria for Information Technology Security Evaluation (kurz: CC) des Common Criteria Recognition Arrangements (CCRA) (Herrmann, 2002). Vertreten werden die CCRA in Deutschland durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es handelt sich um eine international anerkannte Sammlung von Sicherheitsnormen zur Bewertung der Funktionalität sowie der Vertrauenswürdigkeit von IT-Systemen (CC, 2021). Die CC definieren Funktionsklassen, wie beispielsweise die Kommunikation, den Schutz von Benutzerdaten, Kryptografie oder die Identifikation sowie Authentifizierung.

Die CC spezifizieren Anforderungen, welche in Schutzprofilen zusammengefasst werden. Schutzprofile stellen Vulnerabilitätshärtegrade, ähnlich den physischen Widerstandsklassen (Resistance Classes, kurz: RC) gem. DIN EN 1627-1630, dar.[26] Bei den CC werden insgesamt sieben Evaluation Assurance Levels (EAL) unterschieden (CC, 2022). Je höher das Level ist, desto mehr kann ein Anbieter darauf vertrauen, dass die funktionalen Sicherheitsanforderungen aufgrund von Testings, Reviews, etc. erfüllt werden. In Schwerdtfeger (2018) wird auf der Basis der CC, den BSI-Grundschutzkatalogen und Richtlinien für physische Schließsysteme ein

[26] Der physische Härtegrad, der durch eine RC repräsentiert wird, zeigt die jeweilige Wirksamkeit gegenüber definierten Angreiferprofilen an. Er hängt von der Widerstandszeit und den Werkzeugen eines Angreifers ab.

Leifragenkatalog zur Bewertung immobiler Mobile Access Systeme (MAS) abgeleitet. Mithilfe des Compliance-basierten Leitfragenkatalogs kann die Konformität mit der Erfüllung von Anforderungen geprüft werden. Ein hoher Erfüllungsgrad entspricht einem geringen Vulnerabilitätslevel.

Um kritische Systemeinheiten identifizieren und die Wahrscheinlichkeit unerwünschter Schadensereignisse ermitteln zu können, werden die Fehlerbaumanalyse (Fault Tree Analysis, kurz: FTA, Zio, 2007) in der Functional Safety und die Angriffsbaumanalyse (Attack Tree Analysis, kurz: ATA, ISO/SAE, 2021b) in der physischen Security und in der IT-Security verwendet. Eine Verallgemeinerung der Angriffsbaumanalyse ist die Attack Graph Analysis (AGA). Im Safety-Fall wird das Ereignis durch den erkannten Fehler oder das Versagen einer Komponente (d. h. mangelnde Verfügbarkeit gemäß der Aufgabe) beschrieben (Zio, 2007, S. 115). Die ATA wurde von Schneider (1999) eingeführt und konzentriert sich auf die Absicht eines potenziellen Angreifers, ein Ziel zu erreichen (z. B. Beeinträchtigung der Verfügbarkeit einer Einheit gemäß der Aufgabe) (Ingoldsby, 2016, S. 3, 7). Ziel der FTA ist es, eine Fehlerursache herauszufinden, während mittels der ATA (Implementierungs-)Pfade untersucht werden, welche für einen Angreifer attraktiv sein können (ISO/SAE, 2021b, S. 75-76). Die grafische Darstellung der Interaktion von Versagensereignissen (Safety) und Angriffsrealisationen (Security) erfolgt über einen Top-Down-Ansatz (Ostrom & Wilhelmsen, 2019, S. 185 – 187; Harnser, 2010, B4, S. 50).

Die Baumdarstellung beginnt mit dem Top-Event. Dabei handelt es sich um die Formulierung des unerwünschten Ereignisses. Mittels logischer Verknüpfung, sog. Gates oder Gatter auf Basis Boole'scher Operatoren (z. B. „und" sowie „oder"), werden Verzweigungen (ugs. Äste) zu auslösenden (ursächlichen) Ereignissen geschaffen.[27] Dadurch kann die Mannigfaltigkeit des Komponentenversagens im Falle des Fault Trees (FT) und die Mannigfaltigkeit der Implementierung eines Angriffs im Falle des Attack Trees (AT) abgebildet werden. Die Nutzung von AT oder Attack Graphs (AG) in einem bestimmten Kontext kann einer Metrikfamilie zugeordnet werden, wie z. B. den Connectivity Metrics, Exploitability Metrics oder Attack Vector Metrics (Wang et al., 2017, S. 144-167). Bei einer Connectivity Metric beispielswiese wird der AG verwendet, um den Einfluss des Vernetzungsgrades von Komponenten auf die Security zu bewerten (Wang et al. 2017, S. 153). FT und AT bzw. AG zeigen damit implizit auch den Umgang mit Bedrohungen auf (Wheeler, 2011, S. 101). Durch die Baumstruktur lassen sich folglich kausale Abhängigkeiten zwischen Ereignissen abbilden. Werden den unerwünschten Ereignissen z. B. diskrete Wahrscheinlichkeiten zugeordnet, kann mit ihnen die Wahrscheinlichkeit eines Systemausfalls oder eines erfolgreichen Angriffs auf Basis der Bayes'schen Wahrscheinlichkeitstheorie berechnet werden. Eine ATA-basierende Methode zur Risikobewertung ist beispielsweise RISKEE (Krisper et al., 2019).

Eine Erweiterung der Fehlerbäume und Angriffsbäume bilden Bayes'sche Netze. Bayes'sche Netze sind eine Methode zur Repräsentation der Abhängigkeiten von Variablen auf Basis der Bayes'schen Wahrscheinlichkeitsrechnung (Pearl, 2011; Jansen et al., 2006, S. 11-13). Reale Gegebenheiten werden dabei über stochastische Zusammenhänge beschrieben (Jansen et al., 2006, S. 3). Ein Bayes'sches Netz setzt sich aus einem Graphen und bedingten Wahrscheinlichkeitsverteilungen zusammen. Es besteht weiterhin aus Knoten, die Variablen repräsentieren, und Kanten, die kausale Abhängigkeiten zwischen diesen Variablen abbilden. Diese sind gerichtet und verbinden Knoten miteinander (Jansen et al., 2006, S. 6). Sie beschreiben die Wirkung einer Ursache (eines Knotens) auf mindestens einen anderen Knoten. Bayes'sche Netze stellen Ursache-Wirkungs-Zusammenhänge über bedingte Wahrscheinlichkeiten dar (Pearl,

[27] Der Angriffsbaum ist eine besondere Form des Angriffsgraphen. Während bei einem Angriffsbaum Ereignisse eines Implementierungsastes isoliert sind, können bei einem Angriffsgraphen Ereignisse eines Implementierungsastes einen Ursache-Wirkungs-Zusammenhang zu einem anderen Ast haben.

2011). Die Untersuchung von Unsicherheiten ist mit Bayes'schen Netzen ebenso möglich. Bayes'sche Netze werden in beiden Security-Domänen verwendet. Es wird bei der Nutzung dieser Methode davon ausgegangen, dass Wahrscheinlichkeiten relative Größen sind, die durch Informationen bzw. zusätzlichen Informationsgewinn über die Zeit beeinflusst werden können. Damit eignen sich Bayes'sche Netze auch für Anwendungen der Künstlichen Intelligenz (KI) (Niedermayer, 2008). Die Methode erlaubt insbesondere den Transfer von Expertenwissen in subjektive Wahrscheinlichkeiten (Ben-Gal, 2008).

2.6 Erhebung von Expertenwissen

2.6.1 Methoden

Für die Beantwortung von Sicherheitsfragen ist die Befragung von Experten notwendig (EFSA, 2014, S. 35; Hubbard et al., 2016, S. 66). Laut Gabler-Wirtschaftslexikon umfasst Expertenwissen

> Kenntnisse und intellektuelle Fähigkeiten einzelner Personen, deren Leistung auf einem bestimmten Fachgebiet weit über dem Durchschnitt liegen. Expertenwissen besteht i.d.R. aus großen Informationsmengen in Verbindung mit Vereinfachungen, wenig bekannten Fakten, Faustregeln und klugen Verfahrensweisen (Heuristiken), die eine effiziente Problemlösung (in diesem Gebiet) ermöglichen. (Gabler, 2021).

Experten sind demnach Personen, die mehrjährige, einschlägige Berufserfahrung haben. Nach einer Umfrage des Personaldienstleisters Gulp (2022) können Experten zwischen Junior-Experten und Senior-Experten unterschieden werden. Junior-Experten haben den Umfrage-Ergebnissen von Gulp (2022) zufolge eine Berufserfahrung von durchschnittlich 5.7 Jahren. Um Senior-Experte zu sein, bedarf es einer Erfahrung von durchschnittlich 7.6 Jahren.

Damit Expertenwissen für eine Risikobewertung nutzbar gemacht werden kann, muss des erhoben werden (Elias et al., 2018, S. 1-6). Das bedeutet, dass Experten gezielt befragt werden, um daraus Wissen über Sicherheitseigenschaften und -funktionen des Sicherungssystems zu erhalten. Eine Erhebung ist notwendig, weil unsichere Größen geschätzt werden müssen, sodass eine Bewertung überhaupt erst ermöglicht wird (EFSA, 2014, S. 42). Der Transfer von Expertenwissen in z. B. eine Wahrscheinlichkeitsaussage ist dabei wichtig, aber zugleich besonders schwierig, weil Experten unterschiedliche Antworten geben können (EFSA, 2014, S. 11; Elias et al., 2018, S. 28). Expertenwissen als Input einer Sicherheitsmetrik hat einen maßgeblichen Einfluss auf den Output einer Sicherheitsbewertung und demzufolge den Invest in Sicherheitsmaßnahmen (Saltelli et al., 2004, S. 42, 91, S. 152 – 167; Lichte et al., 2020, 1). Es ist die Frage zu stellen, mit welcher Methode dieses Wissen bestmöglich quantifiziert werden kann (Vogl, 2017). Die Herausforderung liegt beim Generierungsprozess von Informationen für ein Modell bzw. eine Metrik (Elias et al., 2018, S. 144). In Shadbolt et al. (2015) wird dieser Prozess unter dem Begriff „Knowledge Engineering" zusammengefasst. Nachfolgend werden in Form eines Auszugs elaborierte Methoden zur Erhebung von Expertenwissen vorgestellt und es werden Vor- sowie Nachteile benannt.

Für Expertenbefragungen gibt es zwei Varianten. Bei der ersten Variante werden die Wahrscheinlichkeitsaussagen der einzelnen Mitglieder einer Expertengruppe ermittelt und danach zusammengeführt (EFSA, 2014, S. 35). Die numerische Aggregation erfolgt aber nicht zu gleichen Teilen. Expertenaussagen können mitunter stark voneinander abweichen. In ihrer getroffenen Aussage können Experten zudem unterschiedlich sicher sein. Um diese Sicherheit in die Ermittlung einer Wahrscheinlichkeitsverteilung einfließen zu lassen, ist eine Gewichtung sinnvoll. Weniger sichere Aussagen haben demnach weniger Einfluss als sicherere Aussagen

auf das Gesamtergebnis. Bei diesem Ansatz wird der Einfluss durch gruppeninterne Dynamiken minimiert, weil Experten ihrer Erfahrung nach einer Gewichtung zugewiesen werden. Zu den gruppeninternen Dynamiken gehören z. B. soziopsychologische Effekte (Dominanz bestimmter Experten, Introvertiertheit anderer Experten). Diese Effekte können durch einen geeigneten Moderator kompensiert werden.

Bei der zweiten Variante erhält die gewählte Expertengruppe die Aufgabe, untereinander Konsens zu finden. Deswegen wird diese Variante als Verhaltensaggregation bezeichnet (EFSA, 2014, S. 35). Der Output dieses Ansatzes hängt von den Teilnehmern der Befragung ab. Der Erheber von Expertenwissen muss darauf vertrauen, dass die Meinung eines jeden Experten angemessen berücksichtigt wird. Bei der Verhaltensaggregation wird die Diskussion angeregt, wenn Meinungen stark auseinandergehen (Randle et al., 2019). Im Gegensatz zur numerischen Aggregation können bei der Verhaltensaggregation Annahmen, welche von Experten getroffen werden und zu Meinungsverschiedenheiten führen, durch eine wirksame Moderation aufgelöst werden. Bei der Verhaltensaggregation wird eine Wahrscheinlichkeitsverteilung durch Diskussion ermittelt, bei der numerischen Aggregation durch eine mathematische Formel (EFSA, 2014, S. 57). Nachfolgend werden gängige Erhebungsverfahren nach Oakley & O'Hagan (2010), Cooke (1994) und der Research and Development Corporation (RAND, 2021) kurz vorgestellt.

Das Sheffield Elicitation Framework (SHELF) ist ein Protokoll zur Erhebung von Expertenwissen und wurde von Oakley & O'Hagan (2010) entwickelt (EFSA, 2014, S. 67). Es umfasst ein Set an Vorgaben zur Unterstützung der Genese von Wahrscheinlichkeitsverteilungen. In Tonyohan (2021) werden Templates zum kostenlosen Download zur Verfügung gestellt. Die Sheffield-Methode basiert auf der Verhaltensaggregation. Für die Erhebung wird die sog. Quartil-Methode verwendet, wie in Abbildung 22 dargestellt.

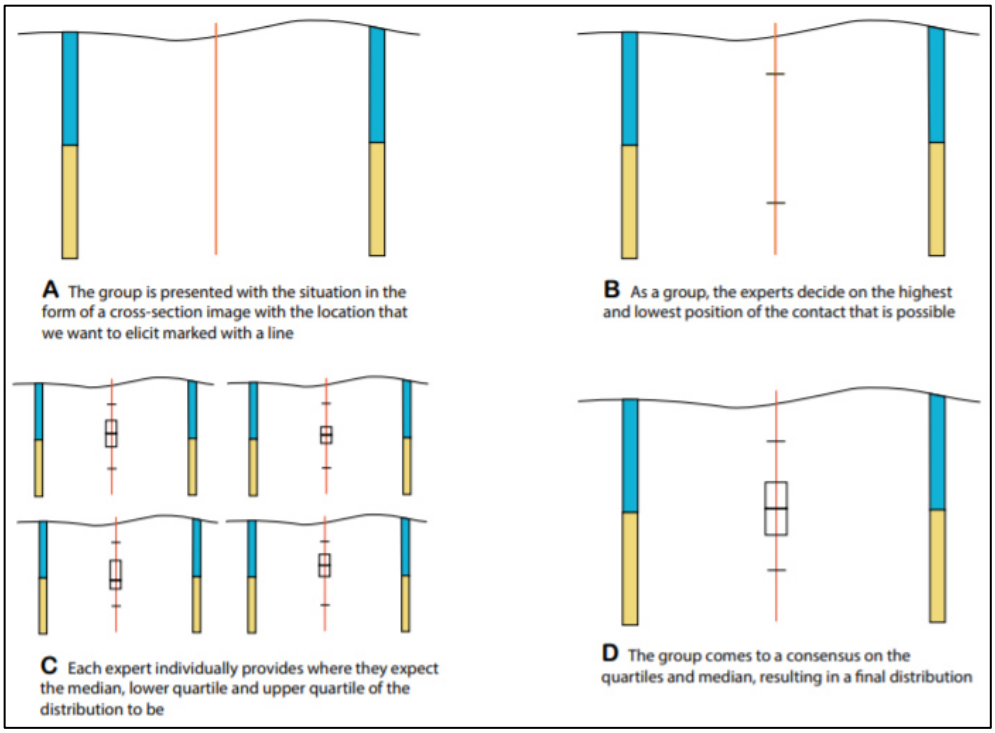


Abbildung 22: Zusammenfassung der Prozessschritte A –D des SHELF.
Quelle: Randle et al. (2019).

Das Modell zur Überführung von Expertenwissen in Wahrscheinlichkeitsverteilungen nach Cooke (1994), auch klassisches Erhebungsmodell genannt (Colson et al., 2020), ist ein Ansatz zur numerischen Aggregation von Expertenwissen (EFSA, 2014, S. 85). Für die Validierung von Expertenurteilen werden zwei Fragentypen gestellt: zum einen Zielfragen und zum andern Kalibrierungsfragen. Zielfragen dienen dazu, Expertenaussagen zu den Unsicherheiten aller Variablen von Interesse, den sog. Zielvariablen, zu erhalten (Colson et al., 2020). Mit Kalibrierungsfragen, auch Seed Questions genannt, sollen Experten Unsicherheiten bei Variablen (Seed-Variablen) angeben, deren wahrer Wert dem Erheber bekannt ist, nicht aber den Experten. Kalibrierungsfragen werden vor den Zielfragen gestellt und haben gem. Colson et al. (2010) drei Zwecke:

- Validierung der Expertenleistung
- Leistungsbasierte Expertengewichtung
- Mechanismus zur Bewertung unterschiedlicher Kombinationen an Experteneinschätzungen

In dem Modell des Cooke'schen Ansatzes wird davon ausgegangen, dass von der Leistung der Experten bei der Beantwortung von Kalibrierungsfragen auf die Leistung bei der Beantwortung von Zielfragen geschlossen werden kann (Cooke 1994). Aus diesem Grund müssen die Seed-Variablen den Zielvariablen möglichst ähnlich sein (EFSA, 2014, S. 85). Nach der Europäischen Behörde für Lebensmittelsicherheit EFSA (2014, S. 85) erfolgt die Bewertung der Güte von Expertenaussagen, Leistungsaggregation genannt, mithilfe zweier Größen, der Kalibrierung und der Information. Die Kalibrierung misst die statistische Wahrscheinlichkeit, dass die Einschätzung eines Experten mit der tatsächlichen Realisierung einer Seed-Variable übereinstimmt (Elias et al., 2018, S. 103-105). Liegen die Wahrscheinlichkeitswerte eines Experten unter einer bestimmten Toleranzschwelle, wird dieser Experte nicht gewichtet. Der Schwellwert wird von einem Prüfer definiert. Die Kalibrierung wird mit Werten zwischen „0" (niedrig) und „1" (hoch) bewertet, wobei „1" hohe statistische Genauigkeit bedeutet und „0" niedrige statistische Genauigkeit (EFSA, 2014, S. 85). Ein Experte liegt mit seinen Antworten bei den Kalibrierungsfragen im Falle einer hohen Kalibrierung nahe bei den wahren Werten der Seed-Variablen.

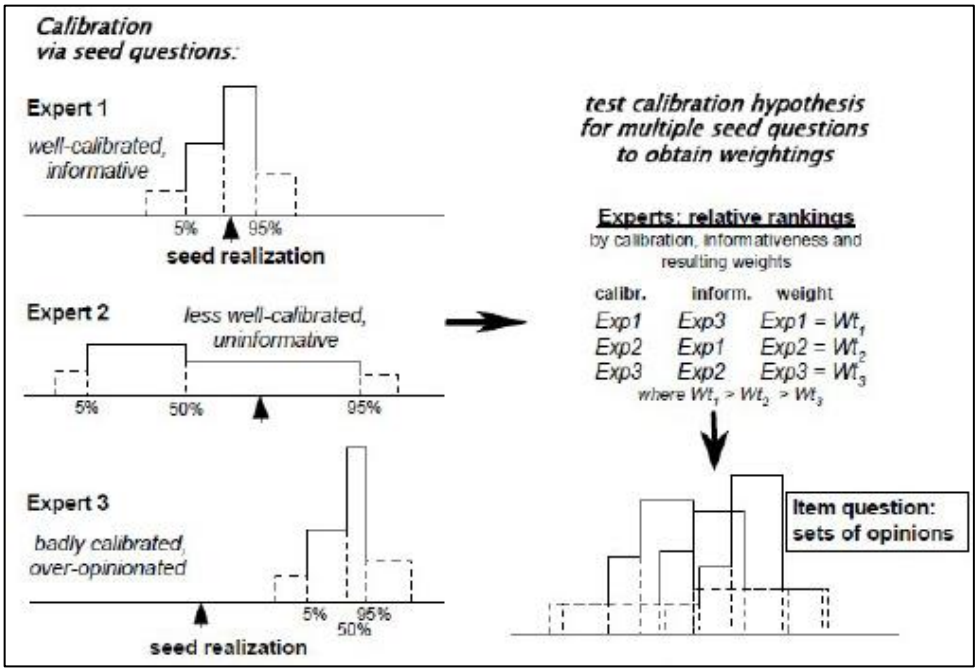


Abbildung 23. Schematische Beschreibung der Leistungsaggregation über Seed Question. Quelle: EFSA (2014, S. 86).

Das Leistungsmaß „Information“ beschreibt zum einen den Grad an Entropie in der Leistung eines Experten (Stichprobenentropie) und zum andern den Grad an Entropie in den Antworten auf Kalibrierungsfragen (Antworten-Entropie) (Elias et al., 2018, S. 105-106). Für jeden Experten wird nach Cooke (1994) ein durchschnittlicher Informationswert berechnet. Es gibt in diesem Kontext unterschiedliche Ansätze, wie die Berechnung durchgeführt werden kann (Elias et al., 2018, S. 102-106). Allgemein entspricht eine gute Expertise einer guten Kalibrierung und einer großen Menge an Informationen. Zusammenfassend gibt die Kalibrierung eine Antwort auf die Frage „Wie nahe liegt der Experte mit seiner Aussage am wahren Wert?“, während die Information eine Antwort auf die Frage „Wie konsistent ist der Experte in seinen Aussagen (über mehrere Kalibrierungsfragen hinweg)?“ repräsentiert. Vereinfachend kann gesagt werden, dass die Kalibrierung ausdrückt, wie nahe der Mittelwert an dem tatsächlichen Wert liegt, während die Information die Streuung um diesen Mittelwert abbildet (siehe Abbildung 23). Experten geben nach dem Cooke’schen Ansatz klassischerweise ein 5 %-Quantil und ein 95 %-Quantil an. Die leistungsbezogenen Gewichte der einzelnen Experten sind laut EFSA (2014, S. 85-86) proportional zum Produkt aus Kalibrierung und Information.

Neben dem SHELF-Ansatz nach Oakley & O'Hagan (2010) und dem klassischen Erhebungsansatz nach Cooke (1994) ist die Delphi-Methode ein verbreiteter Ansatz zur Erhebung von Expertenwissen (EFSA, 2014, S. 8). Die Delphi-Methode wurde von der Research and Development Corporation (RAND) in den 1950er-Jahren entwickelt, um die Auswirkungen von Technologien auf die Kriegsführung vorhersagen zu können (RAND, 2021). Der Zweck der Delphi-Methode besteht darin, den Meinungskonsens einer Gruppe von Experten zu testen (Vernon, 2009). Im Wesentlichen handelt es sich bei Delphi um eine repetitive Umfrage, bei der Fragen so gestellt werden, dass eine Experten-übergreifende Vergleichbarkeit ermöglicht wird (siehe Tabelle 10). Die Delphi-Umfrage kann in mehreren aufeinanderfolgenden Runden erfolgen. Nach jeder Runde wird das Expertenfeedback vom Erheber verwendet, um die Fragen für die nächste Runde nachzubessern. Zusätzlich zu den Fragen können weitere Informationen vom Erheber an die Experten herausgegeben werden. Diese Informationen sollen dazu beitragen, das Vertrauen in die gemachte Expertenmeinung (Konfidenz) zu festigen. Da mit jeder neuen Runde neues Expertenwissen einfließt, ist ein eingeschränktes Maß an Experteninteraktion möglich (EFSA, 2014, S. 101). Darüber hinaus können Expertenaussagen revidiert und auf Basis neu erworbener Informationen nachjustiert werden (Hubbard et al., 2016, S. 72). Ziel weiterer Runden ist es, im Idealfall Konsens zu schaffen.

	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

Tabelle 10: Schritte zur Durchführung einer Delphi-Umfrage.
Quelle: EFSA (2014, S. 101).

Die Anonymität der Teilnehmer ist ein besonderes Merkmal der Delphi-Methode. Diese soll sicherstellen, dass sich eine Expertenmeinung erfragen lässt, welche möglichst nicht direkt von anderen Meinungen beeinflusst wird, wie das bei der typischen Verhaltensaggregation der Fall ist. Jedes Expertenurteil wird klassischerweise gleich gewichtet (Vernon, 2009). Die Antworten werden in einer Endrunde zusammengefasst und analysiert (EFSA, 2014, S. 101). Eine Übersicht und Einordnung weiterer Möglichkeiten zur Erhebung von Expertenwissen wird in Shadbolt et al. (2015) präsentiert.

2.6.2 Anwendungen in der Sicherheitsbewertung

Die Nutzung von Expertenwissen ist in allen vorgestellten Methoden und Modellen bzw. Metriken des Kapitels 2.5 ein Erfordernis, um mit Unsicherheiten aufgrund einer geringen Datenbasis in der Security-Bewertung umzugehen. Nachfolgend werden beispielhaft Anwendungen von Methoden zur Erhebung von Expertenwissen in der Security-Bewertung dargestellt.

In einer Studie über den Einfluss von Unsicherheiten in der physischen Security-Bewertung wird herausgestellt, dass die semi-quantitative Modellierung weit verbreitet ist und die Parametrierung durch Expertenwissen klassischerweise in Form von Scores durchgeführt wird (Lichte et al., 2018). Scoring-basierte Modelle lassen jedoch die Berücksichtigung von Unsicherheiten zu, weswegen in Lichte et al. (2018) ein Ansatz eingeführt wird, mit dem der Transfer von einer semi-quantitativen Modellierung zu einer quantitativen Modellierung möglich gemacht werden kann. Am Beispiel einer fiktiven Produktionsinfrastruktur wird in Lichte et al. (2018) eine vereinfachte semi-quantitative Methode zur Bewertung von Security-Risiken auf Basis eines Rankings der Protektion (P), Observation (O) und Intervention (I) vorgestellt. In Lichte et al. (2018) wird erklärt, dass es notwendig ist, Zeitintervalle hinter die Scores der Bewertungsgrößen zu notieren, z. B. P-Score „1“ = 0 – 90 Sekunden, P-Score „2“ = 90 – 180 Sekunden, usw. „The ranking scale that is chosen depending on the considered infrastructure as well as the corresponding estimations [of experts]” (Lichte et al., 2018, S. 4). Experten geben für jede Barriere ihr Ranking für die Ausprägungen von Protektion, Observation und Intervention ab. Es wird anschließend dargelegt, wie die Rankings in dreieckige probabilistische Dichtefunktionen überführt werden können und wie mit diesem Input für die Protektion, Observation und Intervention ein quantitativer Vulnerabilitätswert bestimmt werden kann.

In Coffey et al. (2016) werden Möglichkeiten zur Erhebung von Expertenwissen im Kontext der konzeptionellen Modellierung in der Entwicklung von Service-orientierten Architekturen untersucht. Es geht im Kern um die Identifizierung von Security- und Vertrauensproblemen bei der Entwicklung von sich kontinuierlich weiterentwickelnden Software-Systemen. In Coffey et al. (2016) werden Möglichkeiten zur Erhebung von Expertenwissen im Kontext der konzeptionellen Modellierung vorgeschlagen: Zunächst wird empfohlen, Concept Maps (zu dt. Konzeptkarten) zu entwickeln, um softwareentwicklungsrelevante Ereignisse sowie ihre Beziehungen zueinander darzustellen (Coffey et al., 2016, S. 44) (siehe Abbildung 24). Die Konzeptkarten bilden die Grundlage für die Durchführung eines zweistufigen Experteninterviews, wobei in Stufe eins das „Desktop and Tool Federation Level“ und in Stufe zwei das „Enterprise Level“ Betrachtungsgegenstand ist. In Coffey et al. (2016, S. 50) wird ein Set an Fragen für die Befragung von Experten in der Software-Entwicklung bereitgestellt. Auf Basis der qualitativen Antworten können dann die Konzeptkarten geschärft werden. Als Ergebnis werden Security und Vertrauen in der Software-Entwicklung durch die Optimierung von Prozessen erhöht.

In dem Beitrag von Luxhøj et al. (2016) wird ein Wissenserhebungsprozess zur Unterstützung der probabilistischen Analyse von Safety-Risiken in der Luftfahrt dargelegt. Es wird darüber hinaus die Anwendung einer verbal-numerischen Skala zur Erhebung bedingter Wahrscheinlichkeiten für ein Bayesian Belief Network (BBN) diskutiert. Der Grundgedanke ist dem Ansatz,

wie er in Lichte et al. (2018) vorgeschlagen wird, ähnlich. In der IT-Security gibt es beispielsweise die Methode „CyberRank". Diese soll das Treffen von sicherheitsrelevanten Entscheidungen mithilfe von Expertenaussagen unterstützen (Grushka-Cohen et al., 2016). In Grushka-Cohen et al. (2016) wird ein Ansatz für die Einstufung von Warnmeldungen über anomale Aktivitäten und Verstöße gegen Richtlinien eingeführt. Es handelt sich bei CyberRank um einen Algorithmus zur automatischen Präferenzierung von Warnmeldungen, sodass Experten diese schneller hinsichtlich ihrer Kritikalität bewerten können. Das wiederum kann eine zügigere Ableitung reaktiver Maßnahmen ermöglichen (Grushka-Cohen et al., 2016).

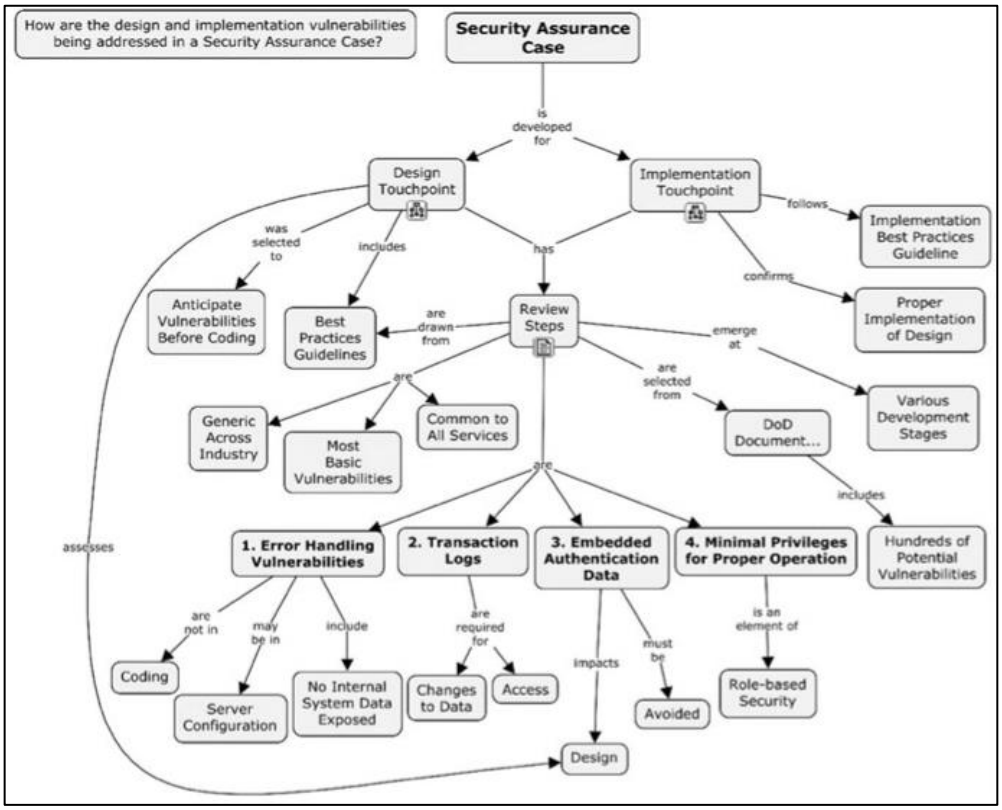


Abbildung 24: Beispielhafte Concept Map.
Quelle: Coffey et al. (2016, S. 47).

In Mézešová et al (2019) wird der Frage nachgegangen, wie von der Ausprägung von CVSS-Scores auf die erforderliche Mindestanforderung an ein bestimmtes Angreiferskill-Level geschlossen werden kann. Es wird eine Kategorisierungsmethode vorgeschlagen, um das erforderliche Qualifikationslevel seitens eines Angreifers für die Ausnutzung einer IT-Schwachstelle bzw. mehrerer IT-Schwachstellen entlang eines Angriffspfads zu bewerten (Mézešová et al., 2019). Aus Sicht der Verteidigung wird auf Basis einer Expertenbefragung ein Rückschluss von den Voraussetzungen zur Durchführung eines Angriffs auf das Skill-Level eines Angreifers geschlossen. Die Expertenbefragung in Mézešová et al (2019) gliedert sich in zwei Runden. In der ersten Runde werden IT-Experten herangezogen, um Auskunft über plausible Angreifertypen und ihre Eigenschaften zu geben. Die drei Skill-Level „Scrypt Kiddie", „Moderate" und „High" resultieren aus der Befragung (siehe Abbildung 25). In einer zweiten Runde werden die Experten anhand konkreter Beispiele gefragt, welches Skill-Level für die Durchführung bestimmter Bedrohungsszenarien erforderlich ist. Für jeden Skill-Typ wird die Durchführbarkeit der beispielhaft gewählten Bedrohungsszenarien gescort. Danach werden die Bedrohungsszenarien auf die Bewertungsgrößen Attack Vector, Attack Complexity, Privileges Required, User Interaction, Authentication, Exploit Maturity Code und Report Confidence nach CVSS (First.org,

2022) zurückgeführt. Danach werden die Mindest-Skill-Level zu den Ausprägungen der CVSS-Bewertungsgrößen geordnet.

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.*

Abbildung 25: Überführung von CVSS-Scores in Angreiferskill-Level.
Quelle: Mézešová et al. (2019).

Aus der Betrachtung aller Ausprägungen des CVSS-Rankings wird der höchste Skill-Level als das Mindestqualitfikationslevel für die Möglichkeit zur erfolgreichen Ausbeutung einer IT-Schwachstelle festgelegt. Zusammenfassend werden in Mézešová et al. (2019) CVSS-Scores mittels Expertenwissen in eine einzige Angreiferkategorie überführt (siehe Abbildung 26). Mithilfe der Methode können für einen Angriffspfad die Mindestanforderung an die Skills eines Angreifers ermittelt werden. Dadurch ist ein Ranking von Angriffspfaden, Schwachstellen und Assets möglich. Die Methode stellt damit eine Entscheidungshilfe für Risikoverantwortliche dar („Was muss zuerst behoben werden?"). CVSS ist ein Kritikalitäts-Grad, der die Ausbeutbarkeit von Schwachstellen bewertet. Die Skill-Kategorisierung auf Basis von (technischen) Mindestanforderungen ist im Prinzip eine andere Interpretation; nicht mit Punkten auf einer semi-quantitativen Skala, wie das bei CVSS der Fall ist, sondern auf einer Skala, welche folgende Frage bewertet: „Welche Mindestfähigkeiten muss ein Angreifer haben?"

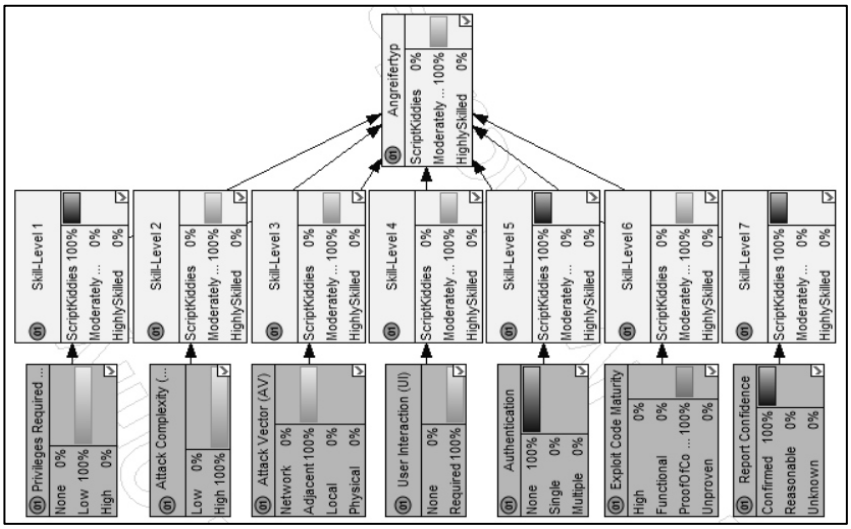


Abbildung 26: Bayes'sches Netz zur Bestimmung der Mindestanforderung an einen Angreifer.
Eigene Abbildung in Anlehnung an Mézešová et al. (2019).

CVSS bildet die Kritikalität von ausgebeuteten Schwachstellen auf einem abstrakten Niveau ab, die Übersetzung von CVSS-Parameter in Skill-Level ermöglicht dagegen den Bezug zwischen Mindestanforderungen und einem konkreten Sachverhalt. „Konkrete Sachverhalte" bedeutet die Möglichkeit einer Use-Case-spezifischen Interpretation. Implizit sind auch mögliche Auswirkungen mit dem Skill-Level verknüpft. Hohe Skill-Level sind allgemein notwendig, um kritischere Assets zu stehlen als im Falle niedrigerer Skill-Level. Mit „kritisch" ist „auswirkungsreich" gemeint. Kritische(re) Assets sind schützenswerte Güter, deren Kompromittierung besonders hohe Auswirkungen mit sich bringen. In Mézešová et al. (2019) wird ein technisch orientierter bzw. technisch gedachter Ansatz aufgezeigt, die Notwendigkeit von technischen Fähigkeiten zur Durchführung eines Angriffs mithilfe von Expertenwissen zu bewerten. Das ist noch nicht die Bedrohungswahrscheinlichkeit für einen bestimmten Angriff. Ein Angreifer muss jeden bewerteten CVSS-Faktor erfüllen, um bestimmte Schwachstellen ausbeuten zu können. Bei einigen Schwachstellen wird nicht jeder Scoring-Faktor berücksichtigt, je nach vorliegender Informationslage. Die vorherigen Beispiele zeigen auf, dass die Erhebung von Expertenwissen für die Beantwortung von Sicherheitsfragen eine wichtige Rolle spielt.

2.7 Zusammenfassung des Stands der Wissenschaft und Technik

Zusammenfassend hat sich die physische Sicherheitsbewertung über lange Zeit entwickelt. Physische Sicherheit wird auf Basis des dreiteiligen Risikomodells Bedrohungswahrscheinlichkeit, Vulnerabilität und Auswirkungen bewertet. Im besonderen Fokus beider Security-Domänen liegt die Bewertung der Vulnerabilität. Physische Vulnerabilität kann mittels einer quantitativen Metrik mit einem hinterlegten, objektiven Wirkmechanismus zur Beschreibung des Effekts von Maßnahmen auf die Vulnerabilitätsreduktion bewertet wird (Lichte et al., 2016). Der dreiteilige Modellierungsansatz aus der physischen Sicherheit ist auch in der IT-Sicherheit vorzufinden. Die Bewertungsgrundlage ist aber eine andere, wie eine Gegenüberstellung von PRISM und CVSS oder FAIR offenlegt. Die IT-Sicherheit unterliegt anderen Paradigmen als in der rein physischen Security, wie z. B. in Wheeler (2011), Anderson (2001) und Kofler et al. (2018) aufgezeigt wird:

Ein Angreifer kann sich in der IT-Domäne von minus unendlich bis vor die Tür beamen und Barrieren durch die Ausnutzung von Schwachstellen außer Kraft setzen. Ebenso existieren nur wenige Mechanismen zur Angreifer-Erkennung (Kofler et al., 2018, S. 37). Architekturen wie das Defense-in-Depth (DiD) sind zwar in der IT-Sicherheit gegeben (Anderson, 2001, S. 513), sie entsprechen aber nicht dem räumlichen topologischen Prinzip aus der physischen Sicherheit. In der IT-Sicherheit bezieht sich DiD vielmehr auf eine Reihe aufeinanderfolgender Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit schützen zu können. „Wie bei Burgen ist auch bei Fahrzeugen die Zielsetzung, dass das Überwinden jeder Stufe dem Angreifer so schwer wie möglich gemacht werden soll", so Wurm (2022, S. 43). Das Prinzip entspricht der Multilateral-Security (Anderson, 2001, S. 276).

Ansätze zur Bewertung von physischen Mobile Access Sicherungsmaßnahmen und IT Mobile Access Sicherungsmaßnahmen werden in Schwerdtfeger (2018) auf Basis von CC (2021) für immobile MAS erarbeitet. Bei dem Ansatz wird ein Soll-Sicherheitsprofil definiert und das Ist-Sicherheitsprofil wird mit dem Soll-Sicherheitsprofil durch die Beantwortung von Leitfragen verglichen. Ein niedriges Soll-Sicherheitsprofil bedeutet allgemein, dass nur ein bestimmter Teil von verfügbaren Fragen aus dem Katalog beantwortet werden muss, z. B. nur zwei von insgesamt fünf Muss-Fragen und zwei Zusatzfragen. Die Auswahl der Fragen liegt aber im Ermessen des Prüfers. Das ist insofern problematisch, als dass sich ein Prüfer die für ihn günstigen Fragen heraussuchen kann, wenn er aufgrund des gewählten Soll-Sicherheitsprofils nicht alle Fragen beantworten muss. Dieser Freiheitsgrad in der Beantwortung der Fragen kann zu

einer Sicherheitsillusion führen: Wenn z. B. nur zwei von fünf Fragen beantwortet werden müssen, kann nach der Erfüllung der Fragen fälschlicherweise angenommen werden, dass das System ausreichend gesichert ist.

Die fehlende Beantwortung der restlichen Fragen, die nicht vom Prüfer ausgesucht werden, kann aber die Ursache für einen (zukünftigen) erfolgreichen Angriff sein. Bei einigen Fragen des Leitfragenkatalogs, wie beispielsweise „Welche Zugangsmöglichkeiten gibt es prinzipiell?“ oder „Werden weitere Dienste für Zugangsmöglichkeiten genutzt?“ (Schwerdtfeger, 2018, S. 127), kann eine Parallele zum CVSS nach First.org (2022) gezogen werden: Die Art der Zugangsmöglichkeiten bzw. die Nutzung weiterer Dienste lässt allgemein einen Rückschluss auf mögliche Angriffsvektoren zu. Bei der Beantwortung von Fragen wie „Werden weitere Dienste für Zugangsmöglichkeiten genutzt?“ ist jedoch zu prüfen, was es konkret für die Sicherheit bedeutet, wenn weitere Dienste für die Bereitstellung eines Service verwendet werden. Im leitfragenbasierten Ansatz, wie in Schwerdtfeger (2018) vorgeschlagen, bleibt die wirksamkeitsbasierte Bewertung außen vor.

Die CPS-Forschung zeigt erste Ansätze zur Bewertung von physischer Sicherheit und von IT-Sicherheit in unterschiedlichen Anwendungsfeldern auf. In den vorgestellten Ansätzen wird die Wechselwirkung zwischen den Domänen Physical Security und IT Security jedoch nur unzureichend berücksichtigt. Die Performance Risk-based Integrated Security Methodology (PRISM) bietet beispielsweise einen ausgearbeiteten Leitfaden für die physische Sicherheit an, nicht aber für die Bewertung von IT-Sicherheit oder von Wechselwirkungen (Harnser, 2010, C4). Mit CVSS können zwar Bedrohungsszenario-beschreibende Charakteristiken aus der IT-Perspektive bewertet werden, jedoch gibt es keinen konkreten Bezug zur Hardware. Bei CVSS wird lediglich zwischen physischem Zugang (Attack Vector = Kontext Physical) und IT-Zugang (z. B. Attack Vector = Kontext Network) unterschieden. Der Einfluss der IT-Ausbeutbarkeit auf die physische Vulnerabilität oder umgekehrt wird nicht bewertet. In bisherigen Standards und Richtlinien sind Lösungsvorschläge zur metrischen Zusammenführung von Physical Security und IT Security nicht gegeben. In Tabelle 11 werden gängige Security-Metriken in den Domänen Physical Security und IT Security aufgeführt. In Tabelle 12 und in Tabelle 13 werden die Vor- und Nachteile ausgewählter Methoden, Modelle bzw. Metriken aus der IT-Sicherheit und der physischen Sicherheit zusammengefasst.

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 Evaluating Safeguards and Security (ASSESS), Safeguards Automated Facility Evaluation (SAFE), System Analysis of Vulnerability to Intrusion (SAVI), Forcible Entry Safeguards Effectiveness Model (FESEM), Safeguard Effectiveness Model (ISEM), Safeguards Network Analysis Procedure (SNAP).

Tabelle 11: Auszug von Security-Metriken.
Quelle: Eigene Abbildung.

IT Security			
Bewertungsansatz	**CVSS**	**FAIR**	**CC, Leitfragenkatalog**
Typ	qualitativ, semi-quantitativ, Scoring-basiert	quantitativ	qualitativ, semi-quantitativ, Scoring-basiert
Vorteile	o Einfache Ergebnisinterpretation, o Mitarbeiter ohne Security-Fachwissen können einbezogen werden, o Klare Handlungsvorschriften und Guidelines, o Erweiterungen möglich, o Bereitstellung eines Kalkulators	o Quantifizierung von Risikovariablen, o Berechnung von IT-Risiken in Bezug zu finanziellen Verlusten, o Klare Definition von Begriffen, o Zunehmende Genauigkeit mit der Zeit (Sammlung von Erfahrung und Evidenz)	o Keine Quantifizierung von Variablen o Einfache Handhabung durch geführten Fragenkatalog
Nachteile	o Keine Abbildung der Wechselwirkung mit der physischen Welt, o Vulnerabilitätsbewertung auf nur auf High-Level Systemebene o Kein Wirkmechanismus hinterlegt o Ordinalwerte werden verrechnet	o Statisches Modell, das keine Editierung/Erweiterung vorsieht, o hohe Kompetenz und Erfahrung notwendig o Evidenz erforderlich	o Wechselwirkung mit der physischen Welt unberücksichtigt, o Ergebnisse sind subjektive Einschätzungen, o Keine Vergleichbarkeit von Risiken
Bewertungsansatz	**OMB M-04-04, NIST 800-63, Kantara, IAFF**	**Angriffsbäume**	**Bayes'sche Netze**
Typ	Qualitativ, semi-quantitativ, Scoring-basiert	qualitativ, semi-quantitativ, quantitativ	quantitativ
Vorteile	o Genormt, o Technische Vorgaben definieren klare Handlungsanweisungen	o Darstellung der Implementierungs-Möglichkeiten eines Angriffs, o Wahrscheinlichkeitstheorie anwendbar	o Abbildung realer Vorgänge, o Probabilistische Konsistenz, o Hinreichende Basis für Kosten-Nutzen-Analyse, o Versatil im Sinne der Einsatzfähigkeit beim Risiko-Assessment
Nachteile	o Keine hinreichende Basis für Kosten-Nutzen-Analyse, o Stark auf Identitätsmanagement fokussiert o Technisches Know-How zur Umsetzung vonnöten	o Erstellung setzt Expertenwissen voraus o Wechselwirkungen zwischen IT und Physik unzureichend abgebildet	o Abhängig von Expertenwissen o Zum Teil sehr komplex

Tabelle 12: Vor- und Nachteile ausgewählter Modelle, Methoden und Metriken, IT Security. Quelle: Eigene Abbildung.

Physische Security			
Bewertungsansatz	**EASI & Ableitungen**	**PRISM**	**Vulnerabilitätsmodell nach Lichte et al. (2016)**
Typ	quantitativ, zeitbasiert	qualitativ, semi-quantitativ, Scoring-basiert	quantitativ, zeitbasiert
Vorteile	o Unterschiedliche Perspektiven abbildbar (externe, interne Angreifer) o Berücksichtigung von topologischen und Einrichtungs-inhärenten Eigenschaften	o Einfache Interpretierbarkeit der Ergebnisse, o Risikoregister gibt Überblick über das gesamte Risiko-Assessment	o Abbildung von Unsicherheiten, o zunehmende Genauigkeit durch Informationsgewinnung über die Jahre, o Bewertung von Risiken nach Geldwerten, o Kosten-Nutzen-Analyse kann unterstützt werden

Nachteile	o z. T. sehr Attribut-lastig, viele Parameter, die subjektiv eingeschätzt werden müssen, o Expertenwissen vonnöten, o z. T. hohe Komplexität, o Herausforderungen bei der Ergebnisinterpretation	o Sehr aufwendig, o Erfordert den Zugang zu sensiblen Daten über eine Infrastruktur, o Keine ausreichende Berücksichtigung scharfer Vulnerabilitätskriterien (Protektion, Observation und Intervention werden trotz Interdependenzen lediglich additiv verrechnet, zudem handelt es sich um Ordinalwerte)	o Hoher Zeitaufwand, um brauchbare Ergebnisse zu erhalten, o Hohe fachliche Kompetenz und Skills vonnöten.
Bewertungsansatz	**Resistance Classes**	**Angriffsbäume**	**Bayes'sche Netze**
Typ	quantitativ, zeitbasiert	qualitativ, semi-quantitativ, quantitativ	quantitativ
Vorteile	o Stark genormt, o Einfache Interpretierbarkeit, o Vergleichbarkeit möglich	o Darstellung der Implementierungs-Möglichkeiten eines Angriffs, o Wahrscheinlichkeitstheorie anwendbar	o Abbildung realer Vorgänge, o probabilistische Konsistenz, o Hinreichende Basis für Kosten-Nutzen-Analyse, o Versatil i. S. Einsatzfähigkeit beim Risiko-Assessment
Nachteile	o Lediglich gängige missbräuchliche Szenarien berücksichtigt, o Use-Case-spezifische Abweichungen bei der Einbruchhemmung werden nicht berücksichtigt, o Lediglich Betrachtung der physischen Security (Wechselwirkungen mit der IT werden nicht erfasst)	o Erstellung setzt Expertenwissen voraus, o Wechselwirkungen zwischen IT und physischer Welt unzureichend abgebildet	o Abhängig von Expertenwissen, o zum Teil sehr komplex

Tabelle 13: Vor- und Nachteile ausgewählter Modelle, Methoden und Metriken, Physical Security. Quelle: Eigene Abbildung.

Der Stand der Erhebung von Expertenwissen legt dar, dass die Festlegung und Abschätzung von schwer quantifizierbaren Risikobeiträgen nur gelingen kann, wenn Expertenwissen mittels geeigneter Methoden erhoben und in Sicherheitsmetriken als Input eingespeist wird. Drei Methoden zur Erhebung von Expertenwissen sind allgemein verbreitet: SHELF, Cooke und Delphi. Vor- und Nachteile der vorgestellten Methoden werden in Tabelle 14 zusammengefasst.

Methode	**Vorteile**	**Nachteile**
SHELF	o Expertenannahmen können sofort reflektiert werden (direktes Feedback). o Schaffung von Konsens im Diskurs.	o Soziopsychologische Effekte können auftreten (Dominanz durch extrovertierte Experten). o Hohe Anforderungen an den Moderator. o Es kann ggf. kein Konsens geschaffen werden.
Cooke	o Gewichtung von Expertenurteilen. o Vorfilterung von Experten über Kalibrierungsfrage. o Quantitative Aggregation über mathematische Formeln. o Moderator bewertet Fachkompetenz des Experten und dieser wiederum den zu untersuchenden Sachverhalt.	o Kalibrierungsfragen nicht leicht zu finden. o Erhebungsaufwand hoch. o Gewichtung von Expertenaussagen nicht trivial. o Für die Wahl von Zielvariablen hohe fachliche Kompetenz vonnöten. o Mathematische Expertise an Moderator vonnöten.
Delphi	o Anonyme Angabe von Ergebnissen, dadurch keine gegenseitige Beeinflussung. o Befragung mehrerer, unabhängiger Experten. o Skalierung der Umfrage von einigen bis zu hunderten Experten möglich.	o Vorbereitung der Sitzungen aufwendig. o Zusammenführung der Ergebnisse aufwendig. o Qualität der Schätzung von den Kompetenzen der Experten abhängig. o Auswahl der Experten erfolgt subjektiv. o Wiederholbarkeit muss hinterfragt werden, wenn Experten nach einer Runde über die Meinungen der anderen dazulernen

Tabelle 14: Vor- und Nachteile elaborierter Methoden zur Erhebung von Expertenwissen. Quelle: Eigene Abbildung.

Die wesentliche Funktion aller drei genannten Methoden ist es, den subjektiven Grad an Überzeugung eines oder mehrerer Experten durch Leitfragen und ggf. mehrere Befragungsrunden in einen quantitativen Ausdruck zu überführen. Der Output einer Expertenbefragung kann in einem nächsten Schritt z. B. als Input für eine Bewertungsmetrik oder die Optimierung von Modellen verwendet werden. Folgenden Herausforderung muss im Zuge der Erhebung von Expertenwissen begegnet werden: 1) Wahl eines oder mehrerer Experten; 2) Wahl eines Moderators, welcher insbesondere mit soziopsychologischen Effekten (z. B. Dominanz von Individuen) umgehen kann; 3) Formulierung der richtigen Fragen in Bezug auf das Ziel der Erhebung; 4) Analyse und Auswertung der Expertenaussagen. Den Überlegungen in Aigner & Khelil (2020) folgend könnten Erhebungsmethoden kombiniert werden, um eine bestmögliche Erhebung und Verwertung von Expertenwissen zu ermöglichen.

3 Ansatz zur domänenübergreifenden Risikobewertung

Die Vorgehensweise zur Bewertung der cyberphysischen Vulnerabilität lehnt in Teilen an die bestehenden Ansätze nach Lichte et al. (2016), Braband (2019), Harnser (2010) und CVSS (First.org, 2022) an. Die physische Vulnerabilität von Mobile Access Sicherungssystemen soll wirksamkeitsbasiert bewertet werden können. Die Bestandteile des physischen Wirkmechanismus, Protektion, Observation und Intervention, sollen die physischen Sicherungsfähigkeiten beschreiben, einen physischen Angreifer an seinem Vorhaben zu hindern, erfolgreich das Fahrzeug bzw. das Mobile-Access-Produkt zu stehlen. Darüber hinaus sollen Unsicherheiten bei der Bewertung der Sicherungsfähigkeiten aufgrund unterschiedlicher Angreiferprofile berücksichtigt werden können. Der physikalische Angriffsprozess und die dem Prozess zugrundeliegende, zeitliche Abfolge bei der Überwindung von Systembarrieren werden auf Grundlage der Vulnerabilitätsmetrik nach Lichte et al. (2016), in dieser Arbeit als Interventionsfähigkeitsmetrik bezeichnet, quantitativ abgebildet. In einer metrischen Analyse werden Maßnahmen erarbeitet, sodass die Ergebnisse der Scoring-basierten Metrik nach Harnser (2010) an die Ergebnisse der Interventionsfähigkeitsmetrik nach Lichte et al. (2016) angeglichen werden können. Dadurch wird mit beiden Vulnerabilitätsmetriken eine vergleichbare Vulnerabilitätseinstufung erzielt. Das ist erforderlich, damit mit dem Harnser-Scoring reale Vulnerabilitätsstufen abgebildet werden können. Zudem wird erklärt, wie Verwerfungen innerhalb der Harnser-Metrik reduziert werden können.

In der IT-Security soll die Vulnerabilität über die Ausbeutbarkeit systeminhärenter IT-Schwachstellen, die insbesondere die Integrität, Vertraulichkeit und Verfügbarkeit des MAS betreffen, bewertet werden können. Die Ausbeutbarkeit wird über die Bedrohungsszenario-beschreibenden Parameter aus dem CVSS (First.org, 2022) ermittelt. In dieser Arbeit werden Verwerfungen in den CVSS-Exploitability-Metriken und dem Barriere-basierten CVSS-Ansatz, wie in Braband (2019) vorgeschlagen, analysiert. Anschließend werden Verbesserungsvorschläge entwickelt, um die aufgedeckten Verwerfungen zu reduzieren, z. B. die Anwendung einer log-Transformation, logische Inkonsistenzen bezogen auf die Bezeichnung oder die Ausprägungen von Bewertungsparametern. Die Reduktion von Verwerfungen trägt dazu bei, Widersprüche innerhalb der Scoring-Systeme abzubauen und die Bewertungsparameter eines Scorings hinsichtlich des Abstraktionsgrades respektive Informationsgehalts zu harmonisieren. Die definierten Forderungen und Maßnahmen aus der metrischen Analyse der Harnser-Metrik und der Interventionsfähigkeitsmetrik werden als Ausgangspunkt für die Angleichung der Beschreibung und Bewertung von Vulnerabilität bzw. von Risiken in beiden Security-Domänen verwendet. In dieser Arbeit wird untersucht, welche Forderungen an die Vulnerabilitätsbeschreibungen zu definieren sind, sodass sowohl in der physischen Sicherheit als auch in der IT-Sicherheit ein Barriere-basiertes Pfadmodell als Ausgangspunkt für eine Vulnerabilitätsbewertung genutzt werden kann.

In einem weiteren Schritt soll gezeigt werden, wie die Risikobeschreibungen und Risikobewertungen in beiden Security-Domänen zusammengebracht werden können, sowie welche Voraussetzungen dafür erforderlich sind. Für die Bewertung der physischen Vulnerabilität wird die Harnser-Metrik verwendet. Für die Bewertung der IT-Vulnerabilität wird die CVSS-Metrik benutzt. In dieser Arbeit werden Maßnahmen erarbeitet, um (auf Verfahrensebene) die Bewertung von Bedrohungsszenarien in beiden Domänen konsistent aufzustellen. Ebenso wird ergründet, wie Wechselwirkungen bewertet und Sicherheitslevel in beiden Domänen im Falle einer Wechselwirkung aufeinander abgestimmt werden können. Da in der IT-Security aufgrund des fehlenden objektiven Wirkmechanismus unzureichende Möglichkeiten der Quantifizierung von Vulnerabilität bestehen, wird vorgeschlagen, nur Wechselwirkungen von IT-Szenarien auf physische Szenarien abzubilden. Die Wahl liegt auch darin begründet, dass die

Ergebnisse der Scoring-basierten, physischen Vulnerabilitätsbewertung quantitativ nachgerechnet werden können.

Basis der Bewertung von cyberphysischen Wechselwirkungen durch Experteneinschätzungen sind die topologischen Verbindungen der cyberphysischen Strukturen, welche durch das Server-Client-Modell beschrieben werden können (siehe Kapitel 8.2.1 im Anhang). Gemäß dem Server-Client-Konzept kann eine kompromittierte Einheit zur Kompromittierung subordinierter Einheiten führen. Die Schnittstellen zwischen physischen Barrieren zu IT-Einheiten bilden in diesem Zusammenhang Möglichkeiten ab, die ein Angreifer ausnutzen kann, um physische Sicherheitsfunktionen zu beeinträchtigen. Zur Abbildung der Wechselwirkung wird der IT Impact on Physical Vulnerability (ITIPV) eingeführt. Die Größe ITIPV beschreibt den Kompromittierungsgrad physischer Sicherheitsfunktionen durch ein IT-Szenario. Für die Ermittlung des ITIPV wird die physische Vulnerabilität zweimal ermittelt: einmal unter der Voraussetzung, dass nur ein physisches Szenario vorliegt, und einmal unter der Voraussetzung, dass vor dem physischen Szenario ein IT-Szenario physische Sicherheitsfunktionen beeinflusst. Die Bewertung der Beeinträchtigung erfolgt durch Experteneinschätzungen.

Für die Herleitung und Angleichung von physischen und IT-Sicherheitslevels werden Vorgaben aus den Standards ISO/SAE 21434 (Cybersecurity Assurance Level, CAL) und ISO 26262 (Automotive Safety Integrity Level, ASIL) herangezogen. Es werden Unterschiede in der Festlegung von CAL und ASIL herausgearbeitet und Möglichkeiten dargelegt, physische Sicherheitslevels und IT-Sicherheitslevels nach derselben Systematik herzuleiten. Weiterhin wird diskutiert, wie Sicherheitslevels bei Vorliegen einer Wechselwirkung in Abhängigkeit des ITIPV gesetzt werden können. Eine Harmonisierung der Auswirkungsskala beider Domänen wird vorgenommen, sodass sich Auswirkungen von physischen Angriffen und Auswirkungen von IT-Angriffen wiederfinden lassen. Die Vereinheitlichung der Auswirkungsskala bildet eine wichtige Voraussetzung dafür, dass eine domänenübergreifende Bewertung gelingen kann. Zur Ermöglichung der Durchführung einer ganzheitlichen Risikoanalyse wird gezeigt, wie die erarbeiteten metrischen Ansätze zur Vulnerabilitätsbewertung in der physischen Security und IT-Security in die TARA nach ISO/SAE 21434 eingefügt und damit zum cyberphysischen TARA (CPTARA) im Sinne einer prospektiven Risikobewertung für CPS erweitert werden kann.[28] Für die Sub-Schritte zur Durchführung eines CPTARA werden Methoden vorgeschlagen, wie z. B. die What-If-Technik bei der Bewertung der Assets oder die Angriffsbaumanalyse bei der Bewertung der Angriffspfade. Die Zusammenführung der vorgeschlagenen Bedrohungsanalyse und Risikobewertung wird über die Methode Bayes'scher Netze vorgenommen, um das Expertenwissen über die Sicherheitsfähigkeit in der physischen Security und in der IT-Security probabilistisch konsistent zu verknüpfen.

Die Wahl Bayes'scher Netze erlaubt es, Expertenwissen über die topologischen Verknüpfungen innerhalb des Systems und Fähigkeiten der eingesetzten Sicherungsmaßnahmen zu berücksichtigen. Hierfür wird ein Erhebungsverfahren auf Basis der Delphi-Methode und dem Cooke'schen Erhebungsansatz vorgeschlagen, um Expertenwissen zu quantifizieren und in das Modell als Input zu überführen. Durch die generische Vorgehensweise des Mixed-Metric- und Mixed-Methods-Ansatzes können domänenspezifische und domänenübergreifende Risikoanalysen durchgeführt werden. Arbeitsschritte im Zuge der Entwicklung eines Ansatzes zur Ermöglichung einer domänenübergreifenden Sicherheitsbewertung werden nachfolgend auf einer übergeordneten Ebene beschrieben:

[28] Abgrenzung nach Morr et al. (2019): Prädiktiv: „Was wird passieren?", diagnostisch: „Warum ist es passiert?", deskriptiv: „Was passierte?", preskriptiv: „Was sollte getan werden?". Bei einer prospektiven Analyse werden Daten gesammelt und analysiert, um z. B. die Wirksamkeit der Sicherheitsmaßnahmen eines Systems zu überprüfen. Bei der prädiktiven Analyse werden (historische) Daten genutzt, um zukünftige Ereignisse vorherzusagen.

1. Durchführung einer metrischen Analyse zu Möglichkeiten zur Reduktion der Inkompatibilität zwischen semi-quantitativen und quantitativen Metriken am Beispiel der physischen Sicherheit: Die semi-quantitative Vulnerabilitätsmetrik nach Harnser (2010) wird mit der quantitativen Interventionsfähigkeitsmetrik nach Lichte et al. (2016) verglichen. Vorschläge zur Reduktion von Verwerfungen innerhalb der Harnser-Metrik werden vorgeschlagen.
2. Analyse der Verwerfungen beim Common Vulnerability Scoring System (CVSS) nach First.org (2022) und beim Barriere-basierten CVSS: Untersuchung der Schwächen der Basismetrik und Diskussion möglicher Verbesserungen, z. B. Reduktion von Verwerfungen.
3. Definition von Randbedingung, sodass die ungleichen Bewertungen in den Domänen physische Sicherheit und IT-Sicherheit in gleiche Vulnerabilitäts- bzw. Risikoeinstufungen und Sicherheitslevels resultieren: Am Beispiel CVSS (IT Security) sowie der Harnser-Metrik (Physical Security).
4. Aufbau der Risikoanalyse, in Anlehnung an ISO/SAE 21434: Erweiterung des Threat Analysis and Risk Assessment (TARA) zum Cyber-Physical Threat Analysis and Risk Assessment (CPTARA).
5. Implementierung der Risikoanalyseschritte in ein Bayes'sches Netz, um das Expertenwissen über die Sicherheitsfähigkeit für die Domänen Physical Security und IT Security probabilistisch konsistent zu verknüpfen.

Die Arbeit schließt mit einer Zusammenfassung der Ergebnisse und einer Beschreibung möglicher Anschlussforschungen ab.

3.1 Analyse der Harnser-Metrik und Interventionsfähigkeitsmetrik

Das Problem bei der Anwendung semi-quantitativer Metriken wird in Krisper (2021) wie folgt dargelegt:

> 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, S. 5).

Den Harnser-Scores liegt keine dahinterliegende Metrik auf Basis der Zeit zugrunde, wie das bei der ICM nach Lichte et al. (2016) der Fall ist. Beispielsweise wird für den Harnser-Score „5" definiert: „There is no capability to prevent this scenario from occurring and causing worst-case consequences" (Harnser, 2010, S. 109). Ein scharfes Vulnerabilitätskriterium kann mit der Interventionsfähigkeitsmetrik (Intervention Capability Metric, ICM) nach Lichte et al. (2016) objektiv abgebildet werden. Mit der Harnser-Metrik ist dergleichen nicht möglich, weil hinter den Vulnerabilitäts-Scores keine konkreten Wahrscheinlichkeiten stehen. In Krisper (2021) wird in diesem Zusammenhang geschrieben: „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, S. 10). In der Problemstellung aus Kapitel 1.1 wird in qualitativer Form bereits auf die Inkompatibilität zwischen dem additiven Ansatz nach Harnser und dem probabilistischen Ansatz nach Lichte et al. (2016) hingewiesen. Bei beiden Vulnerabilitätsbewertungen wird die physische Sicherheitsfähigkeit eines Systems im Angriffsfall betrachtet, das bedeutet, es wird in der Vulnerabilitätsbewertung davon ausgegangen, dass ein Angreifer tatsächlich das System auf physischem Wege angreift (siehe dazu auch Kapitel 1.2).

Wenn die Vulnerabilitätsskala der Harnser-Metrik kompatibel zu den Vulnerabilitätsergebnissen der ICM wäre, dann könnten mit der Harnser-Metrik reale Vulnerabilitätsniveaus ermittelt werden. Das würde den Vorteil mit sich bringen, dass in einer physischen Bedrohungsanalyse

und Risikobewertung Szenarien durch Experten Scoring-basiert bewertet werden könnten und anhand der Vulnerabilitäts-Scores eine realistische Einschätzung in Bezug auf die Vulnerabilität erfolgen könnte. Experten aus der Produktentwicklung können folglich ein einfaches Scoring für die physische Sicherheitsbewertung verwenden, für welches kein fundiertes mathematisches Wissen notwendig ist. Die Anpassung der Harnser-Metrik an objektive Vulnerabilitätsniveaus schafft auch Vorteile für eine domänenübergreifende Sicherheitsbewertung. Angenommen, es gibt IT-Szenarien, die Auswirkungen auf physische Sicherheitsfunktionen haben können. Die IT-Bedrohungswahrscheinlichkeit und die IT-Vulnerabilität sind aber nicht näher bekannt. Ein Experte kann, wenn er ein IT-Szenario mit einer Auswirkung auf physische Sicherheitsmaßnahmen identifiziert hat, die an die ICM angepasste Harnser-Metrik heranziehen, um folgenden Sachverhalt zu bewerten: Wie hoch ist die physische Sicherheitsfähigkeit des Systems im physischen Angriffsfall, wenn zuvor ein IT-Szenario die physische Sicherheitsfähigkeit beeinträchtigt hat? Physische Vulnerabilität wird dieser Idee folgend unter Annahme eines physischen Angriffsfalls unter Berücksichtigung eines davor stattgefundenen IT-Angriffsfall bewertet. Das Resultat des Harnser-Scorings liefert dann einen Vulnerabilität-Score, hinter dem eine objektive Vulnerabilitätsstufe steht. Weitere Ausführungen zur domänenübergreifenden Bewertung sind in Kapitel 3.2 zu finden.

Aus wissenschaftlicher Sicht stellen sich die Fragen, wie groß die Inkompatibilitäten zwischen beiden Metriken unter bestimmten Annahmen tatsächlich sind und welche Möglichkeiten es geben kann, diese zu reduzieren. In dieser Arbeit wird eine mathematische Analyse durchgeführt, um diese Fragen zu beantworten. In Krisper (2021) beispielsweise wird vorgeschlagen, quantitative Metriken als Werkzeug zu benutzen, um qualitative und semi-quantitative Bewertungsschemata in ihrer Güte zu bewerten. Dabei kann es sich grundsätzlich um quantitative Safety- oder quantitative Security-Metriken handeln. In Krisper (2021) wird im Rahmen eines Vergleichs von semi-quantitativen und quantitativen Metriken festgestellt: „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, S. 3). Die Differenzen zwischen den Vulnerabilitätsergebnissen der Harnser-Metrik und den Vulnerabilitätsergebnissen der ICM werden anhand verschiedener Arten des Bewertungsschemas in der Harnser-Metrik und anhand der Variation der Mittelwerte und Streuungen in der ICM berechnet. Anschließend werden Maßnahmen zur Verringerung der metrischen Differenzen untersucht. Es werden bei der ICM z. B. in einem Analysedurchlauf diskrete Werte für die Protektion, Observation und Intervention gewählt. Im Ergebnis soll sich eine Vulnerabilitätsfunktion in Abhängigkeit der Fähigkeiten eines Sicherungssystems ergeben, die mathematisch begründet zeigt, welche Differenzen zustande kommen und wie groß diese sind, wenn semi-quantitativ nach Harnser – im Vergleich zu quantitativ nach der ICM – gearbeitet wird. Dadurch kann objektiv nachgewiesen werden, an welchen Stellen der quantitative Ansatz nach der ICM andere Ergebnisse liefert als der semi-quantitative Ansatz nach Harnser. Um Vergleichbarkeit zu gewährleisten, wird folgendes Referenzszenario gewählt:

Betrachtet wird ein System, das aus einer Barriere und einem Asset besteht. Die Barriere muss überwunden werden, um an das Asset zu gelangen. Sie besitzt Eigenschaften der Protektion, Observation und Intervention. Es wird die Wirksamkeit von Maßnahmen im Falle eines Angriffs in Bezug auf die Vulnerabilität bewertet. Die Bewertungsgrößen Protektion, Detektion und Intervention werden bei Harnser jeweils zwischen „1" (Minimum) und „5" (Maximum) gescort. Der Detektions-Score wird hier durch den Observations-Score ersetzt. Grund dafür ist, dass die Detektion ein Ereignis ist, welches sich aus dem Zusammenspiel von Protektion und Observation ergibt. Auf Basis der fünf Scores für je Protektion (P), Observation (O) und Intervention (I) werden dann gem. der festgelegten Rechenvorschriften nach Harnser (2010) die Permutationen aller möglichen Ausprägungen (5 x 5 x 5 = 125) durchgerechnet. Folgende Analysen wer-

den durchgeführt: 1) Bildung des Vulnerabilitäts-Scores über die Summe der Scores von Protektion, Observation und Intervention; 2) Bildung des Vulnerabilitäts-Scores über die Summe der logarithmierten Scores von Protektion, Observation und Intervention. Für die Bestimmung der Vulnerabilität mit der ICM werden zu jedem Harnser-Score quantitative Gegenstücke formuliert. Mit diesen werden ebenso die Permutationen aller möglichen Ausprägungen (5 x 5 x 5 = 125) durchgerechnet. Es wird angenommen, dass die Zeiten für Protektion, Observation und Intervention normalverteilte Größen sind. Steuerungsgrößen sind der Mittelwert und die Standardabweichung, d. h. es handelt sich jeweils um eine Zuordnung eines P-Scores, O-Scores bzw. I-Scores zu einem Mittelwert und einer Standardabweichung einer Normalverteilung (siehe Tabelle 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	$\mu = 15, \sigma = 30$

Tabelle 15: Mapping der Harnser-Scores zu Mittelwerten und Standardabweichungen in der ICM.
Quelle: Eigene Tabelle.

Die Standardabweichungen werden bei allen Scores auf 30 Sekunden festgesetzt. Die Protektionszeit wird mit zunehmendem Score größer, wohingegen die Observationszeit und Interventionszeit jeweils mit zunehmendem Score kürzer werden. ICM 1 steht für die ICM-Variante Nummer eins. Eine ICM-Variante ist eine Konvention bzgl. der Festlegung von den Mittelwerten und Standardabweichungen für die Stufen „1" bis „5". Im Falle der ICM werden insgesamt 37 Varianten durchgerechnet, wobei eine Variante (ICM discrete) die Berücksichtigung diskreter Zeitwerte für die Protektion, Observation und Intervention betrachtet. Die Konfigurationen ICM 1, …, ICM 36 basieren dagegen auf Dichtefunktionen für die Protektion, Observation und Intervention. In Tabelle 16 werden die Werte der Standardabweichungen durch Buchstaben substituiert: A_x steht für die Standardabweichung der Protektion. B_x steht für die Standardabweichung der Observation, und C_x steht für die Standardabweichung der Intervention. Der Index „x" bezeichnet die jeweilige ICM-Variante (siehe Tabelle 16 und Tabelle 17).

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

Tabelle 16: Verallgemeinerung der Zuordnung der Harnser-Scores zu Mittelwerten und Standardabweichungen in der ICM.
Quelle: Eigene Tabelle.[29]

[29] „x" steht hier für die ICM-Variante. A_x := Standardabweichung der Protektion, B_x := Standardabweichung der Observation, C_x := Standardabweichung der Intervention.

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

Tabelle 17: Auszug der ICM-Varianten.
Quelle: Eigene Tabelle.[30]

Als Beispiel dafür, wie Tabelle 17 zu lesen ist, wird in Tabelle 18 ein Beispiel für die ICM-Variante 30 gegeben.

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

Tabelle 18: Harnser-Score-Zuordnung zu den Mittelwerten und Standardabweichungen von ICM 30.
Quelle: Eigene Tabelle.

Je höher die Nummer der Variante bis einschließlich Nr. 27, desto höher sind die verwendeten Standardabweichungen. Die verwendeten Mittelwerte bleiben, wie in Tabelle 15 definiert, gleich. Eine Ausnahme bildet die ICM 36 aus Tabelle 17. Die Varianten 28 bis 36 stellen Konfigurationen dar, bei denen weitere Modifikationen getestet werden. Im Ergebnis ergibt sich für jede Permutation ein quantitativer Vulnerabilitätswert zwischen 0 (minimal) und 1 (maximal), der zu den Vulnerabilitäts-Ergebnissen nach Harnser geordnet werden kann. In der ersten Harnser-Scoring-Variante werden Protektion (P), Observation (O) und Intervention (I) jeweils zwischen „1“ und „5“ gescort und addiert. Im Ergebnis ist ein Score-Umfang von „3“ bis „15“ möglich. Die Score-Range von „0“ bis „2“ ist aufgrund der Rechenvorschrift nicht in der Bewertungsskala enthalten. „15“ bedeutet eine geringe Vulnerabilität und „3“ bedeutet eine hohe Vulnerabilität. Das Bewertungssystem nach Harnser ist in dieser Form nicht mit der ICM vergleichbar. Für die Ermöglichung des Vergleichs ist die Erweiterung des Harnser-Bewertungsschemas durch eine Skala mit probabilistischen Werten erforderlich.

[30] Da in der Metrik mit Normalverteilungen gerechnet wird, wird die Abbildung von diskreten Werten durch kleine Standardabweichungen approximiert.

Die Transformation von qualitativen Deskriptoren (respektive Scores) in quantitative Ausdrücke ist erforderlich, weil die Harnser-Ergebnisse mit den Ergebnissen nach der ICM verglichen werden sollen. Weil gem. Krisper (2021) und Newsome (2013, S. 105) Unsicherheiten Score-inhärent sind, sind die Scores bzw. die Kategorien auf der Bewertungsskala, in welche die Scores einsortiert werden, nicht mit diskreten Werten zu versehen, sondern mit einer „Approximate Range" an probabilistischen Werten (Newsome, 2013, S. 104-105). Die Umwandlung von Scores in andere Bewertungsgrößen wird auch „Konversion" genannt (Howard, 1958). Initial wird hinter jedem Vulnerabilitäts-Score jeweils ein gleich großes Wahrscheinlichkeitsintervall vermutetet, d. h. 0 % bis 100 % an möglicher Wahrscheinlichkeit für die Vulnerabilität wird zu gleichen Teilen auf die Vulnerabilitäts-Scores von „3" bis „15" verteilt (siehe Tabelle 19). Die Wahrscheinlichkeitsintervalle werden in ihrer Breite äquidistant gewählt, weil noch nicht bekannt ist, wie weit die semi-quantitativen Ergebnisse nach Harnser an den quantitativen Ergebnissen der ICM liegen. Eine solche Einteilung ist gängige Praxis bei Behörden und Institutionen (Newsome, 2013, S. 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

Tabelle 19: Harnser-Skala-Setup zur Ermöglichung eines metrischen Vergleichs.
Quelle: Eigene Tabelle.[31]

In dieser Arbeit werden nicht alle berechneten ICM-Varianten und unternommenen Vergleiche zwischen der Harnser-Metrik und der ICM dargelegt. Auszughaft werden nachfolgend ausgewählte ICM-Varianten betrachtet, um den wissenschaftlichen Mehrwert darzustellen. Für den ersten Vergleich zwischen der Harnser-Metrik und der ICM wird die Konfiguration eins aus Tabelle 17 herangezogen (ICM 1). Es werden drei Varianten betrachtet: Bei Variante eins bleiben die Scores der Protektion und Observation konstant, während der Interventions-Score erhöht wird (siehe Tabelle 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

[31] V := Vulnerability. Mu := Mittelwert, sig := Standardabweichung, V := Vulnerability, Upper := obere Grenze des vermuteten Wahrscheinlichkeitsinterballs, Lower := untere Grenze des vermuteten Wahrscheinlichkeitsintervalls.

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

Tabelle 20: Variantenrechnung I zum Vergleich Harnser-Metrik – ICM.
Quelle: Eigene Tabelle.[32]

Da hinter jedem Score Mittelwerte und Standardabweichungen in der ICM-Konfiguration eins stehen, kann eine Score-Kombination, z. B. P = „1“, O = „1“ und I = „1“, quantitativ nachgerechnet werden. Bei Variante zwei werden die Protektion und Intervention konstant gehalten, während die Observation zunehmend betont wird. Bei Variante drei wird die Protektion als einziger der drei Bewertungsparameter variiert. Bei allen drei Varianten ist zu sehen, dass die Differenz zwischen den Ergebnissen der Harnser-Metrik und den Ergebnissen der ICM mit zunehmender Score-Summe größer wird. Das Abfallen der Vulnerabilitätswerte nach Harnser ist durch die Definition der Skalenkategorien in Tabelle 19 zu erklären. Hinter jedem Vulnerabilitäts-Score nach Harnser steht jeweils ein vermutetes Wahrscheinlichkeitsintervall, das eindeutig unterscheidbar von den anderen Intervallen ist: Je niedriger der Vulnerabilitäts-Score, desto höher die vermutete Wahrscheinlichkeit. Wird folglich einer der drei Bewertungsparameter variiert, dann wird die Score-Summe größer und die vermutete Wahrscheinlichkeit kleiner. Die Vulnerabilitätsergebnisse nach der ICM bleiben dagegen konstant hoch.

Aufschluss dafür gibt ein näherer Blick auf die Verrechnung der Bewertungsgrößen in der ICM: Ein niedriger Protektions-Score bedeutet eine geringe Zeit in der Überwindungshemmung. Ein geringer Observations-Score bezeichnet eine lange Observationszeit. Trotz dessen, dass die Intervention mit zunehmendem Score besser, also aus Sicht der quantitativen Metrik kürzer wird, bleibt die Vulnerabilität hoch. Der Grund für diesen Verlauf der Vulnerabilitätskurve nach der ICM liegt an der schlechten Observationszeit. Eine kurze Observationszeit ist eine Voraussetzung, dass die Intervention erfolgreich sein kann. Eine gute Interventionszeit bringt nichts, wenn ein Angreifer im Zuge seines Angriffs nicht oder zu spät als solcher erkannt wird. An dem dargelegten Beispiel zeigt sich das Zusammenspiel zwischen der Eindring- und Reaktionszeit, wie sie durch die ICM abgebildet wird. Die Berechnungen der drei Varianten verdeutlichen die Differenzen zwischen der Harnser-Metrik und der ICM.

Bei einer Minimalauslegung jeweils zweier Bewertungsparameter ist es unerheblich, ob der dritte Bewertungsparameter, sei es Protektion, Observation oder Intervention, betont wird: Die Vulnerabilität, so zeigt die quantitative Rechnung mittels der Parameterkombination in der ICM 1, bleibt über 99 %. Die Berechnung über das Scoring-System suggeriert jedoch, dass die Score-Erhöhung eine Besserung bringen würde. Ein weiterer Untersuchungsgegenstand kann sein, zu berechnen, wie sich die Vulnerabilität verändert, wenn folgendes Setup definiert wird: Zwei Bewertungsparameter sind besonders betont, während der dritte Wirkmechanismus zunehmen soll. In gleicher Weise wie in Tabelle 20 werden drei Varianten berechnet. Zuallererst werden Protektion und Observation jedoch konstant hoch festgehalten, während die Intervention variiert wird. Nach demselben Prinzip wird in Variante zwei die Observation variiert und in Variante drei die Protektion, während die anderen beiden Bewertungsparameter besonders ausgeprägt bleiben. Die berechneten Permutationen sind in Tabelle 21 aufgeführt. Die Ergebnisse der ICM offenbaren, dass mit der ersten Variante die beste Vulnerabilitätsreduktion erzielt werden kann. Variante zwei und drei sind hinsichtlich der Vulnerabilitätsreduktion identisch und geringer als Variante eins.

[32] V := Vulnerability.

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

Tabelle 21: Variantenrechnung II zum Vergleich Harnser-Metrik – ICM.
Quelle: Eigene Tabelle.[33]

Unter Annahme der gewählten Parameterkombinationen sollte allgemein auf viel Observation und viel Protektion gesetzt werden. Letztlich hängt dies von der Kostenfunktion, welche hinter den Parametern hinterlegt ist, ab. Dieser Effekt wird durch die Harnser-Metrik nicht abgebildet. Es ist dennoch zu sehen, dass bei den drei betrachteten Analysedurchläufen die Ergebnisse von Variante eins am besten mit dem Scoring-Bewertungssystem angenähert werden können. Die Differenz zwischen dem Harnser-Mittelwert und dem Ergebnis nach der ICM beträgt für die erste Permutation, P = „5“, O = „5“ und I = „1“, nahezu 27 %. Für die zweite Permutation ist die Differenz bei ca. 12 %, bei der dritten Permutation liegt sie bei 0.26 %, bei der vierten Permutation bei 4 % und bei der vierten Permutation bei 1.5 %. In einem weiteren Schritt werden alle möglichen Kombinationen, so z. B. auch die Permutationen P = „2“, O = „3“, I = „5“ oder P = „4“, O = „2“, I = „4“, mittels der Harnser-Metrik und der ICM 1 durchgerechnet und verglichen. Die vermuteten Wahrscheinlichkeitsintervalle können in einem ersten Schritt mit der Skala aus Tabelle 19 für jede der (5 x 5 x 5 =) 125 Score-Kombinationen ermittelt werden. Diese werden in einem zweiten Schritt permutationsweise zu den ICM-Ergebnissen geordnet. Anschließend werden die Ergebnisse der Harnser-Metrik und die Ergebnisse der ICM der Größe der Harnser-Werte nach sortiert (siehe Abbildung 27).

[33] V := Vulnerability.

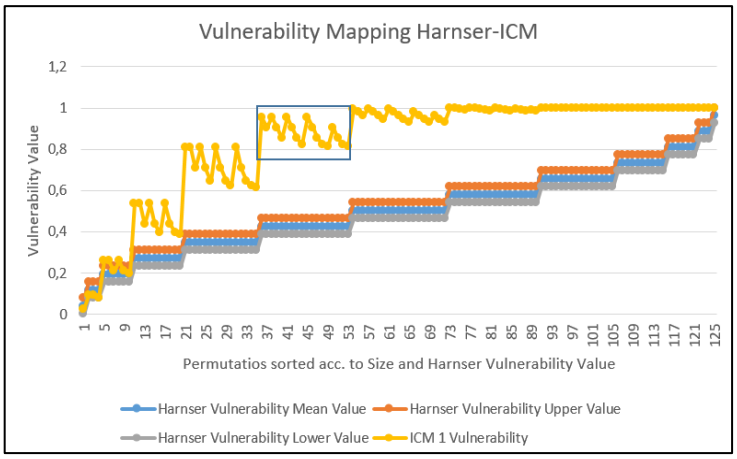


Abbildung 27: Sortierte Ergebnisse der Permutationen, ICM 1 – Harnser.
Quelle: Eigene Abbildung.

Dadurch ergibt sich eine objektive ICM-Vulnerabilitätsfunktion. Die Ergebnisse nach Harnser bilden eine quasi-kontinuierliche Zuordnung bezogen auf eine diskrete Basis der Harnser-Werte. Der Verlauf der Zuordnung enthält Sprünge (Plateaus), ist also nicht „kontinuierlich". Die Wahrscheinlichkeitsintervalle pro Plateau werden durch den „Lower Vulnerability Value" und den „Upper Vulnerability Value" aufgespannt. Die zu den Harnser-Werten zugeordneten Vulnerabilitätsergebnisse nach der ICM springen dagegen. Die ICM-Ergebnisse bilden einen diskontinuierlichen Kurvenverlauf beschränkten Wachstums. Bei der Betrachtung der Abbildung 27 wird eine Frage aufgeworfen: Weshalb springen die Werte der ICM-Vulnerabilitätsfunktion? Zur Beantwortung der Frage nach dem Springen der ICM-Funktionswerte wird beispielhaft eine Reihe an Permutationen, in Abbildung 27 durch ein blaues Rechteck markiert, näher betrachtet. Auszughaft aus dem in Abbildung 27 eingezeichneten Bereich sind in Tabelle 22 die Berechnungsergebnisse der permutierten Varianten aufgelistet. Markiert sind beispielhaft ein hoher Wert (rot) ein mittlerer Wert (orange) und ein tiefer Wert (gelb). Die Bezeichnungen hoher Wert, mittlerer Wert und niedriger Wert beziehen sich auf die betrachtete Range an den vorliegenden quantitativen Ergebnissen. Bei diesen drei Varianten ist die Score-Summe dieselbe.

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
2	3	5	10	0.385	0.462	0.4235	45.0	75.0	15.0	30.0	30.0	30.0	0.95367115
2	4	4	10	0.385	0.462	0.4235	45.0	45.0	45.0	30.0	30.0	30.0	0.90338094
2	5	3	10	0.385	0.462	0.4235	45.0	15.0	75.0	30.0	30.0	30.0	0.85309073
3	2	5	10	0.385	0.462	0.4235	75.0	105.0	15.0	30.0	30.0	30.0	0.95367115
3	3	4	10	0.385	0.462	0.4235	75.0	75.0	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
4	4	2	10	0.385	0.462	0.4235	105.0	45.0	105.0	30.0	30.0	30.0	0.82195999

Tabelle 22: Auszug aus den berechneten Permutationen, sortiert nach den Harnser-Ergebnissen.
Quelle: Eigene Tabelle.[34]

[34] V := Vulnerability.

Zwar ist das vermutete Wahrscheinlichkeitsintervall in allen drei Fällen aus Sicht der Harnser-Metrik gleich, es liegt jedoch einmal P = „1“, O = „4“, I = „5“, einmal P = „3“, O = „4“, I = „3“ und einmal P = „4“, O = „2“, I = „4“ vor. Aus Sicht der quantitativen Metrik gibt es daher Unterschiede. Die Score-Summe von „10“ kann als Menge verfügbarer Ressourcen interpretiert werden, welche auf die Slots von Protektion, Observation und Intervention aufgeteilt wird. Die berechneten Vulnerabilitätsergebnisse auf Basis der ICM belegen quantitativ, dass das Zusammenspiel der Bewertungsparameter bei P = „3“, O = „4“, I = „3“ besser ist als bei P = „1“, O = „4“, I = „5“. An diesem Beispiel kann mittels der ICM gezeigt werden, dass bestimmte Konfigurationen, bei denen aus Harnser-Sicht dasselbe Vulnerabilitätsniveau vermutet wird, wirksamer sind als andere. Das ist der Grund warum es hier zu Differenzen in den Vulnerabilitätsergebnissen zwischen der ICM und der Harnser-Metrik kommt. Daraus resultieren die Sprünge in der Vulnerabilitätsfunktion der ICM.

Die Wahrscheinlichkeitsintervalle, die hinter den Score-Summen der Harnser-Metrik vermutet werden, sind nachweislich suboptimal gewählt, weil sie die Ergebnisse der ICM 1 nicht spiegeln. Am Beispiel der Gegenüberstellung von Harnser-Vulnerabilitätswerten und ICM 1-Vulnerabilitätswerten kann verdeutlicht werden, dass in bestimmten Teilen große Differenzen vorliegen. Aus Anwendersicht wäre es nutzbringend, eine Skaleneinteilung im Scoring-System vorliegen zu haben, mittels derer Einstufungen möglich sind, die mit den quantitativ errechneten Vulnerabilitätswerten besser übereinstimmen. Hierzu werden zunächst die Verläufe beider Vulnerabilitätskurven qualitativ analysiert: Die Sprünge der ICM-Vulnerabilitätswerte sind je nach zugeordnetem Harnser-Plateau unterschiedlich stark ausgeprägt. Während die Schwankung der Vulnerabilitätswerte zu Beginn und zum Ende der ICM-Vulnerabilitätskurve gering ist, ist sie im Mittelfeld deutlich größer (siehe Abbildung 28).

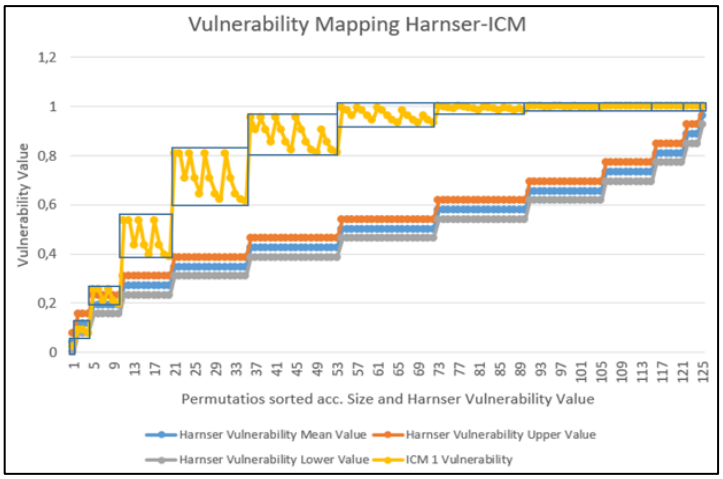


Abbildung 28: Zu ändernde Wahrscheinlichkeitsintervalle bei den berechneten Permutationen. Quelle: Eigene Abbildung.[35]

Um folglich alle ICM-Vulnerabilitätswerte innerhalb eines Harnser-Plateaus durch ein vermutetes Wahrscheinlichkeitsintervall erfassen zu können, ist die Wahl unterschiedlicher Breiten an vermuteten Wahrscheinlichkeitsintervallen pro Harnser-Score erforderlich. Eine weitere Erkenntnis ist, dass die vermuteten Wahrscheinlichkeitsintervalle überlappen können, beispielsweise Score „10“ := 0.98 – 1.00, und Score „15“ := 0.99 – 1.00. Damit die Skalenanpassung auch gelingen kann, bedarf es einer Analyse der Vulnerabilitätswerte der nach Harnser sortierten Permutationen. Der kleinste ICM-Vulnerabilitätswert innerhalb der Länge eines Harnser-Plateaus ist als neue untere Intervallgrenze der dazugehörigen Score-Summe zu wählen. Der

[35] Durch die blauen Rechtecke werden die Sprünge der ICM-Vulnerabilitätswerte pro Plateaulänge erfasst.

größte ICM-Vulnerabilitätswert ist entsprechend als neue obere Intervallgrenze zu setzen (siehe beispielhaft Tabelle 23).

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

Tabelle 23: Auszug aus den Ergebnissen der sortierten Permutationen mit Score-Summe „14“ nach Harnser und ICM 1.
Quelle: Eigene Tabelle.[36]

Nach demselben Prinzip wird jedes vermutete Wahrscheinlichkeitsintervall der 15-Punkte-Skala angepasst. Die Resultate sind in Tabelle 24 aufgeführt:[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

Tabelle 24: An ICM 1 angepasste Harnser-Vulnerabilitätsskala.
Quelle: Eigene Tabelle.

Der Plot der Vulnerabilitätswerte aller 125 Permutationen nach der Größe der Harnser-Mittelwerte zeigt eine erfolgreiche Angleichung des Harnser-Scoring-Systems an die ICM-Variante 1 (siehe Abbildung 29).

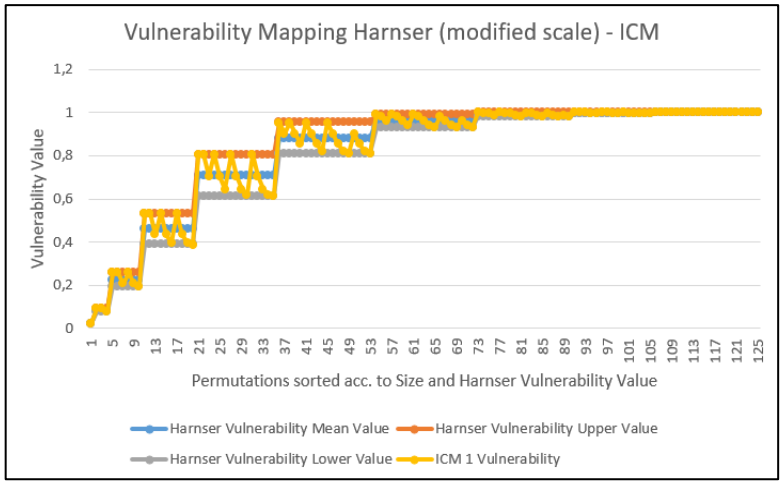


Abbildung 29: Sortierte Ergebnisse der Permutationen, ICM 1 – Harnser mit modifizierter Skala.
Quelle: Eigene Abbildung.

Wenn innerhalb der Harnser-Plateaus nach den ICM-1-Werten sortiert wird, dann ergibt sich ein nahezu stetiger Verlauf beschränkten Wachstums (siehe gelbe Kurve in Abbildung 30).

[36] Neue obere Intervallgrenze: gelb markiert; neue untere Intervallgrenze: blau markiert.
[37] Die Mittelwerte der neuen vermuteten Wahrscheinlichkeitsintervalle sind nachgetragen.

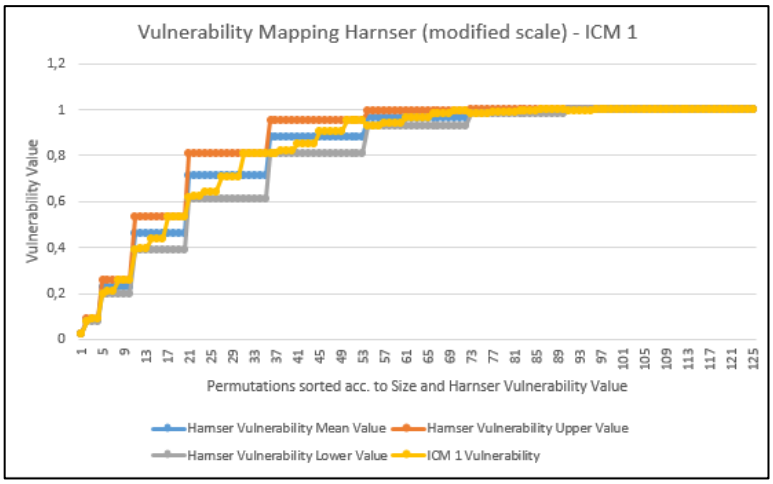


Abbildung 30: ICM 1 in etwa gleichverteilt innerhalb der Harnser-Plateaus sortiert.
Quelle: Eigene Abbildung.

Bei der gelben Kurve handelt es sich um eine Funktion der drei Parameter Protektion, Observation und Intervention. Diese werden über die willkürliche Reihung der betrachteten Permutationen diskret verändert (siehe Tabelle 25). Weil die Skala der Harnser-Metrik an die ICM 1 so angepasst wird, dass mit ihr objektive Vulnerabilitätseinstufungen vorgenommen werden können, können mit dieser modifizierten Harnser-Metrik risikogerechter Entscheidungen bzgl. des Invests in Sicherheitsmaßnahmen getroffen werden. Dies alles mit der Einschränkung des willkürlich gewählten ICM-Modelles einer Barriere und eines Assets. Es kann gezeigt werden, dass die Harnser-Metrik grundsätzlich nicht unerheblich verbessert werden kann.

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**

Tabelle 25: Auszug der berechneten Permutationen, ICM-Werte pro Plateau der Größe nach sortiert.
Quelle: Eigene Tabelle.[38]

Wie Abbildung 30 zeigt, weisen die ICM-Vulnerabilitätswerte bei den Übergängen zwischen zwei betrachteten Plateaus nicht nur Knicke nach oben, sondern auch Knicke nach unten auf.

[38] V := Vulnerability. Alle Tabellenwerte wurden nach der Spalte „ICM 1 V Value" aufsteigend sortiert. In oranger, grüner und blauer Farbe sind jeweils Permutationen markiert, welche für eine konkrete Score-Summe dieselben Vulnerabilitätswerte auf quantitativem Wege erzeugen. In roter Farbe ist ein Übergang der ICM-Vulnerabilitätswerte von einem Plateau zum nächsten Plateau mit einem Knick nach unten markiert.

Der niedrigste ICM-Vulnerabilitätswert des „höheren" Plateaus ist geringer als der höchste Wert des „niedrigeren" Plateaus. In Tabelle 25 rot markiert ist ein Beispiel dafür: Mit der ICM 1 wird bei der Permutation P = „4", O = „1" und I = „5" (Score-Summe „10") eine Vulnerabilität von 95.4 % berechnet. Bei der Permutation P = „3", O = „5" und I = „1" (Score-Summe „9") ergibt sich auf Basis der ICM 1 eine Vulnerabilität von 93.1 %. Schlussfolgernd ist die Konfiguration P = „3", O = „5" und I = „1" besser als die Konfiguration P = „4", O = „1" und I = „5". Das Harnser-Scoring lässt jedoch aufgrund der unterschiedlichen Score-Summen vermuten, dass es andersherum ist.

Es kann bei konkreten Anwendungen jedoch die Regel sein, dass die Mittelwerte und Standardabweichungen von Protektion, Observation und Intervention andere Ausprägungen als im Falle ICM 1 annehmen. Eine Möglichkeit kann sein, dass ein Benutzer des Scoring-Systems zuallererst wählen muss, wie hoch die Streuung bei den Parametern Protektion, Observation und Intervention qualitativ eingeschätzt wird. Diese Einschätzung kann in Stufen erfolgen, indem festgelegt wird: Es gibt z. B. die Stufe A, B und C. Hinter jeder dieser Stufen steht eine klar definierte ICM-Variante mit bestimmten Mittelwerten und Standardabweichungen für die Scorings von „1" bis „5". Für jede ICM-Variante könnte es dann ein Harnser-Scoring mit angepassten Skalen geben. Diese Skala ist so definiert, dass die Harnser-Ergebnisse die ICM-Ergebnisse einer ICM-Variante replizieren können. Das bedeutet, dass ICM-Vulnerabilitätswerte in den Plateaus der vermuteten Wahrscheinlichkeitsintervalle nach Harnser liegen.

Denkbar wäre, dass im Falle dieser Arbeit für den Sonderfall mit einer Barriere und einem Asset ein Nachschlagewerk erarbeitet werden könnte, in dem es angepasste Harnser-Skalen gibt, die eine Entsprechung in einer ICM-Variante finden, so z. B.:

- Wenn Stufe A vorliegt, entspricht das einer ICM-Variante X, und es ist das Scoring-System mit der Skaleneinteilung I zu wählen.
- Wenn Stufe B vorliegt, entspricht das einer ICM-Variante Y, und es ist das Scoring-System mit der Skaleneinteilung II zu wählen.
- Wenn Stufe C vorliegt, entspricht das einer ICM-Variante Z, und es ist das Scoring-System mit der Skaleneinteilung III zu wählen.
- Usw.

Nachfolgend ein Beispiel zur Veranschaulichung: Die vorgeschlagene Skala aus Tabelle 24 zur Scoring-basierten Bewertung von Vulnerabilität bildet den Ergebnisraum der ICM-Variante 1 ab. Werden die Ergebnisse aller Permutationen der ICM-Variante 30 aus Tabelle 17 ebenso in Abbildung 29 eingetragen, dann kann aufgedeckt werden, dass die Skala aus Tabelle 24 ICM 30-Ergebnisse nur in Teilen replizieren kann (siehe z. B. die rote Markierung in Abbildung 31). Die Ergebnisse des Scorings auf Basis der modifizierten Skala für ICM 1 sind in vielen Bereichen nicht quantitativ konform mit ICM 30. Die Harnser-Metrik wird als quantitativ konform definiert, wenn sie hinsichtlich der Kombination der Bewertungsparameter und der Bewertungsskala so kalibriert ist, dass Ergebnisse erzeugt werden können, die den Resultaten aus der quantitativen ICM entsprechen. Die Bewertungen beider Metriken (Harnser und ICM) führen im Falle quantitativer Konformität der Scoring-basierten Metrik zu gleichen Einstufungen von Vulnerabilität. In diesem betrachteten Fall (ICM 30 gegenüber Harnser) sind die Ergebnisse nach Harnser in vielen Teilen nicht in Übereinstimmung mit den quantitativ berechneten ICM 30-Ergebnissen. Hier sollte die Skala des Scorings andere obere und untere Intervallgrenzen für die vermutete Wahrscheinlichkeit pro Score-Summe haben.

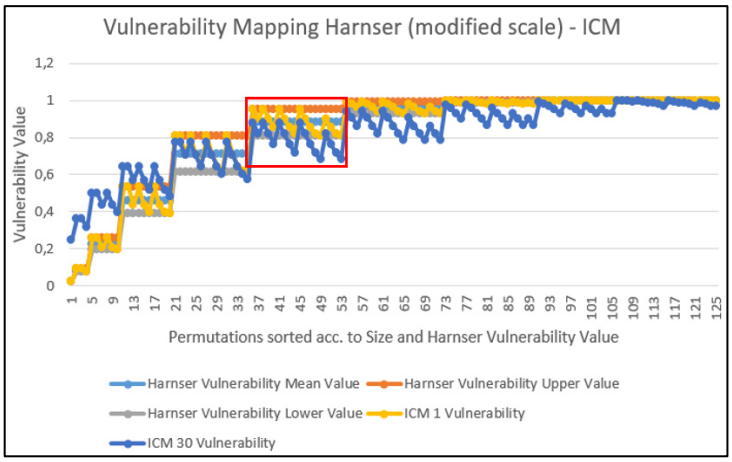


Abbildung 31: Sortierte Permutationen ICM 1, ICM 30 und Harnser mit modifizierter Skala für ICM 1. Quelle: Eigene Abbildung.

Für die Anpassung des Scorings an ICM 30 wird wie bei der vorangegangenen Skalenanpassung vorgegangen: Es werden jeweils die berechneten Einträge, welche zu jedem einzelnen Plateau gehören, analysiert. Daraufhin werden der minimale ICM 30-Wert sowie der maximale ICM 30-Wert pro Plateau ermittelt. Der maximale ICM 30-Wert wird als neue obere Intervallgrenze des vermuteten Wahrscheinlichkeitsintervalls definiert, der minimale ICM 30-Wert als neue untere Intervallgrenze. In Tabelle 26 werden jeweils die Skalen der Harnser-Metrik zur Abbildung der Variante ICM 1 und zur Abbildung der Variante ICM 30 aufgeführt. Im Rahmen eines spaltenweisen Vergleichs zwischen der quantitativ konformen Harnser-Skala zu ICM 1 und der quantitativ konformen Harnser-Skala zu ICM 30 kann verdeutlicht werden, dass jedes vermutete Wahrscheinlichkeitsintervall anders ist.

Harnser-Skala, die ICM 1 replizieren kann													
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-Skala, die ICM 30 replizieren kann													
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

Tabelle 26: Gegenüberstellung der quantitativ konformen Harnser-Skala für ICM 1 und ICM 30. Quelle: Eigene Tabelle.

Der Plot der Vulnerabilitätsergebnisse nach Harnser mit modifizierter Skala für die Variante ICM 30 und nach ICM 1 sowie ICM 30 in Abbildung 32 belegt, dass eine erfolgreiche Anpassung des Harnser-Scorings an ICM 30 vorgenommen werden kann. Gleichzeitig geht mit dieser Skalenanpassung einher, dass sie nicht mehr quantitativ konform mit ICM 1-Ergebnissen ist.

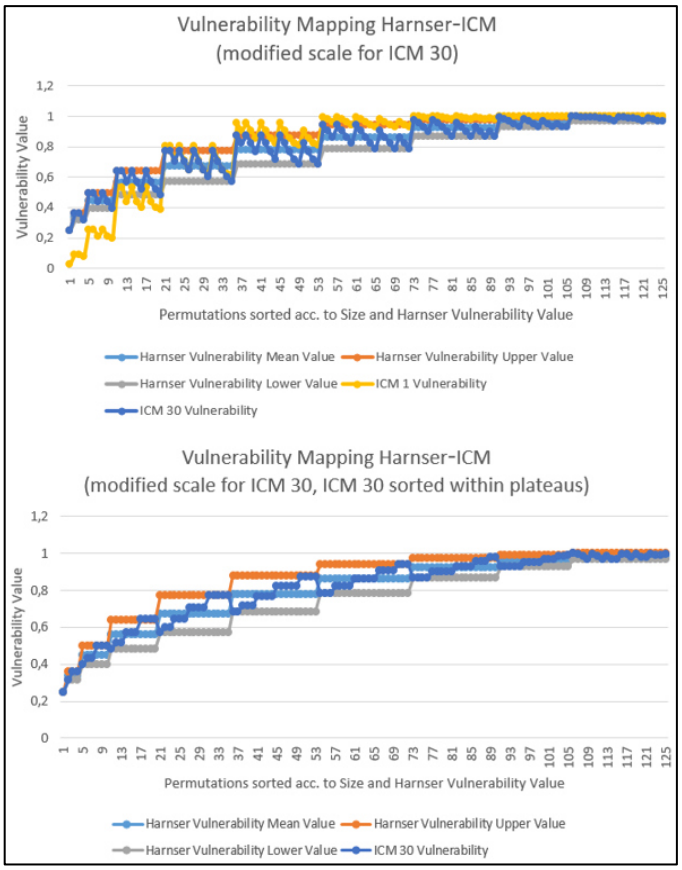


Abbildung 32: Sortierte Permutationen ICM 1, ICM 30 und Harnser mit modifizierter Skala für ICM 30.
Quelle: Eigene Abbildung.

Eine Harnser-Skala, die beide Varianten kombiniert, also Ergebnisse von ICM 1 und ICM 30 über entsprechende Plateaus abdeckt, ist in Tabelle 27 dargestellt. Für jedes Harnser-Plateau ist jeweils der minimale und maximale ICM-Wert über die Varianten ICM 1 und ICM 30 zu ermitteln. Diese beiden Werte werden als untere bzw. obere Intervallgrenze des vermuteten Wahrscheinlichkeitsintervalls nach Harnser definiert. Durch die Anpassung der Harnser-Skala an zwei ICM-Varianten kann ein Security Margin abgebildet werden. Die Mittelwerte und Standardabweichungen, welche hinter einem jeden Score stehen, haben demzufolge eine Range, welche hier von den Varianten ICM 1 und ICM 30 aufgespannt wird. Die Intervallgrenzen überlappen sich. Die Ergebnisse sind in Abbildung 33 geplottet. Wenn zwei ICM-Varianten bei der Überführung in Harnser-Scores Berücksichtigung finden, dann werden die vermuteten Wahrscheinlichkeitsintervalle pro Plateau größer, wie beim Vergleich zwischen Abbildung 31 und Abbildung 33 sowie zwischen Abbildung 32 und Abbildung 33 deutlich wird. Die Anpassung der Harnser-Skala an weitere ICM-Varianten kann nach derselben dargelegten Vorgehensweise erfolgen. Wie in der Abbildung 33 zu sehen, überschneiden sich die Intervallgrenzen.

Harnser-Skala, die ICM 1 und ICM 30 replizieren kann													
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

Tabelle 27: Quantitativ konforme Harnser-Skala für ICM 1 und ICM 30.
Quelle: Eigene Tabelle.

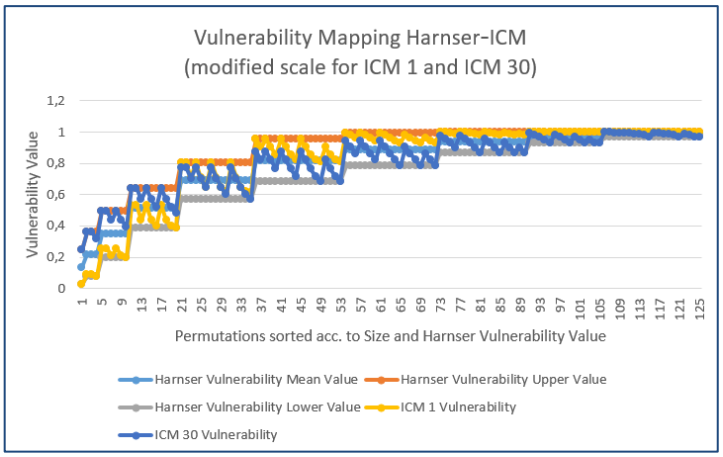


Abbildung 33: Sortierte Permutationen ICM 1, ICM 30 und Harnser mit „kombinierter" Skala. Quelle: Eigene Abbildung.

3.2 Analyse der Common-Vulnerability-Scoring-System-Metriken

Das Common Vulnerability Scoring System (CVSS) der FIRST.org[39] ist ein Industriestandard. Er wurde von der Special Interest Group (SIG) entwickelt (Cheng et al., 2014, S. 11). Es erfasst technische Merkmale von Software, Hardware und Firmware von IT-Systemen (First.org, 2022). CVSS wird weltweit genutzt und ist Stand Mai 2022 in der Version 3.1 verfügbar (Risk-based Security, 2017). CVSS ist ein offenes, anbieter- und plattformunabhängiges Rahmenwerk zur Bewertung des Schweregrads von Sicherheitslücken anhand der Ausbeutbarkeit von Schwachstellen und den mit einer Ausbeutung verbundenen Auswirkungen. In der IT-Security wird Vulnerabilität anhand systeminhärenter Schwachstellen bewertet (First.org, 2022; ISO/SAE, 2021b; Kumar et al., 2017). Eine Schwachstelle ist eine notwendige Bedingung, um einen Angriff ausführen zu können, aber keine hinreichende Bedingung. Die hinreichende Bedingung dafür ist, dass es einen Angriffsvektor (Attack Vector) gibt, der auch zu einem sog. Exploit führt. Exploitability (Ausbeutung) meint, dass eine theoretische Schwachstelle erfolgreich ausgenutzt werden kann. Das Maß zur Bewertung von Schwachstellen ist somit die Exploitability. In der ISO/SAE 21434 wird der Exploitability-Grad über eine Attack-Feasibility-Skala eingeordnet (ISO/SAE, 2021b, S. 1).

Mit der erfolgreichen Ausbeutung einer Schwachstelle geht ein Schaden einher. Das ist z. B. eine Kompromittierung von Vertraulichkeit, Verfügbarkeit oder Integrität oder einer Kombination aus den dreien. Eine Schwachstelle kann gem. ISO/SAE 21434 als Abwesenheit einer Maßnahme oder einer Anforderung oder als eine nicht ausreichende Konfiguration aufgefasst werden (ISO/SAE, 2021b, S. 5). Sie ist ausbeutbar, wenn es mindestens einen Angriffsvektor gibt, der zu einem Schaden führt. Deswegen wird auch die Größe Attack Vector bei CVSS zur Schwachstellenbewertung herangezogen (siehe Abbildung 34). Ein Angriffsvektor fasst nach ISO/SAE 21434 mehrere Sub-Handlungsschritte zusammen, um erfolgreich an ein Ziel zu kommen (ISO/SAE, 2021b, S. 2). Angriffsvektoren bezeichnen gem. der CVSS-Spezifikation v.3.1 „the context by which vulnerability exploitation is possible" (First.org, 2022). Der Attack Vector beschreibt somit den Aufwand, der erforderlich ist, um eine Schwachstelle erfolgreich ausbeuten zu können. Der Aufwand gliedert sich beim CVSS in „Physical", „Local", „Adjacent" und „Network". Für den Attack Vector „Physical" heißt es beispielsweise „The attack requires the attacker to physically touch or manipulate the vulnerable component" (First.org, 2022). Ein

[39] FIRST bedeutet „Forum of Incident Response and Security Teams" (First.org, 2022), eine Non-Profit-Organisation.

Angriffspfad (Attack Path) kann demzufolge potenziell aus mehreren Angriffsvektoren (Kontexten) bestehen. Ein Angriffspfad ist nach ISO/SAE 21434 „a set of deliberate actions to realize a threat scenario" (ISO/SAE, 2021b, S. 2). Bei einem Bedrohungsszenario (threat scenario) handelt es sich dabei um ein „potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario" (ISO/SAE, 2021b, S. 4).

Durch Angriffspfade wird allgemein eine Kombination von möglichen Informationsbeschaffungsquellen abgebildet. Angriffspfade können über die Applikationsebene (Software und Hardware eines Produkts), die Systemebene (Web-Applikations-Server, virtuelle Maschinen), die Netzwerkebene (Kommunikationsverbindungen und Anbindungsformen, z. B. Switches, Firewalls, Virtual Private Network oder Router, und die physische Infrastrukturebene (Gebäudezutritt, Serverräume) hinweg beliebig komplex sein (Nguyen et al., 2020). Bei CVSS wird die Kompromittierung eines bestimmten Assets einem einzigen Attack Vector (Kontext) zugeordnet (First.org, 2022). Die Ergebnisse einer CVSS-Bewertung sind Vulnerability-Scores von „0" bis „10", mit deren Hilfe Sicherheitsmaßnahmen priorisiert werden können. Da beim CVSS die Exploitability (Vulnerabilität) und die Impacts (Auswirkungen) miteinander verknüpft werden, wäre eine Umbenennung des „Vulnerability-Scores" zum „Risk Score" sinniger. Das kann auch durch die Definition von „Risiko" in der ISO/SAE 21434 begründet werden: „[Risk describes the] effect of uncertainty on road vehicle cybersecurity expressed in terms of attack feasibility and impact" (ISO/SAE, 2021b, S. 4). Eine Möglichkeit, die Attack Feasibility nach ISO/SAE 21434 zu bestimmen, ist die Anwendung des CVSS-Scorings (ISO/SAE, 2021b, S. 47).

CVSS besteht aus drei metrischen Gruppen, der Base Metric, der Temporal Metric und der Environmental Metric (siehe Abbildung 34). Die Base Metric, im Folgenden Basis-Metrik genannt, wird für die Ermittlung einer zeitlich konstanten Vulnerabilität verwendet, die für alle Konfigurationen eines IT-Systems gültig ist. Es wird grundsätzlich, u. a. mangels Evidenz, von den schwersten Auswirkungen (Worst-Case-Szenarien) ausgegangen. Die Ergebnisse der Basis-Metriken werden generell veröffentlicht, z. B. unter Common Vulnerabilities and Exposures (CVE, 2021), da sich diese über die Zeit nicht ändern und für alle betroffenen IT-Systeme gelten. Es wird von der SIG vorgeschlagen, den Basis-Score durch zeitliche und umgebungsspezifische Scores zu ergänzen, um einen Schweregrad zu erhalten, der die Vulnerabilität für konkrete Use Cases eines Anbieters abbildet. Die Temporal Metrics (temporale Metriken) ergänzen den Basisschweregrad einer Vulnerabilität durch zeitlich variable Faktoren. Ein Beispiel dafür ist die Bewertung der Verfügbarkeit von ausnutzbarem Code. Die Environmental Metrics (umweltliche Metriken), auch Umgebungsmetriken genannt, passen die Basis- und Temporalmetriken Vulnerabilität an einen bestimmten Use Case und seine umweltlichen Randbedingungen an. Monetäre Verluste durch erfolgreiche Angriffe werden bei CVSS nicht explizit berücksichtigt, können aber, je nach Bedarf, entsprechend ergänzt werden (First.org, 2022).

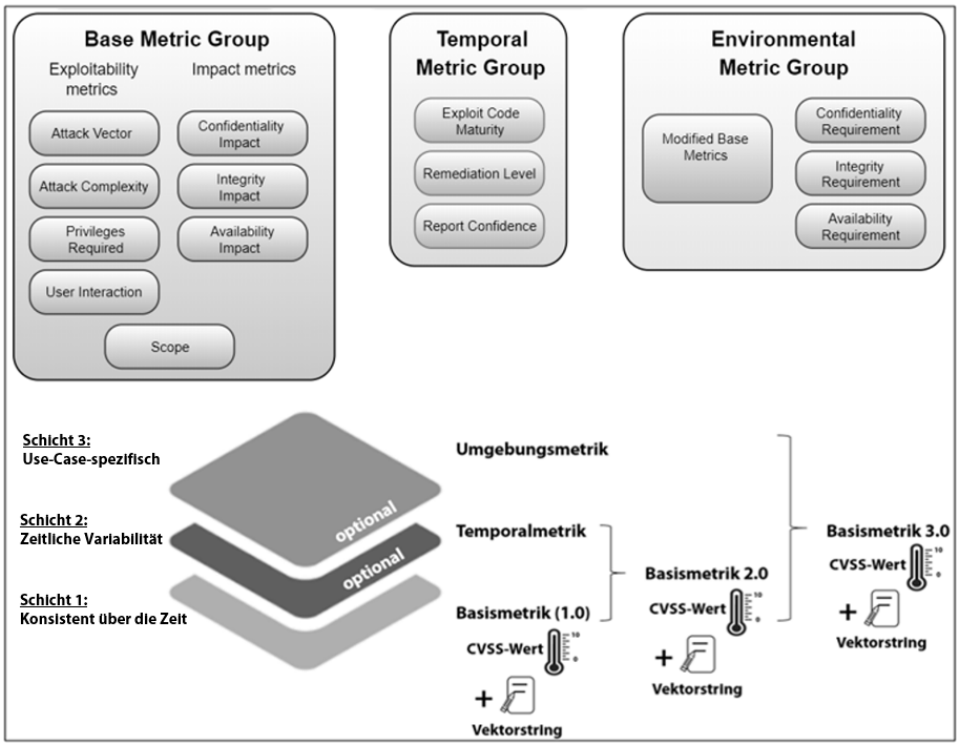
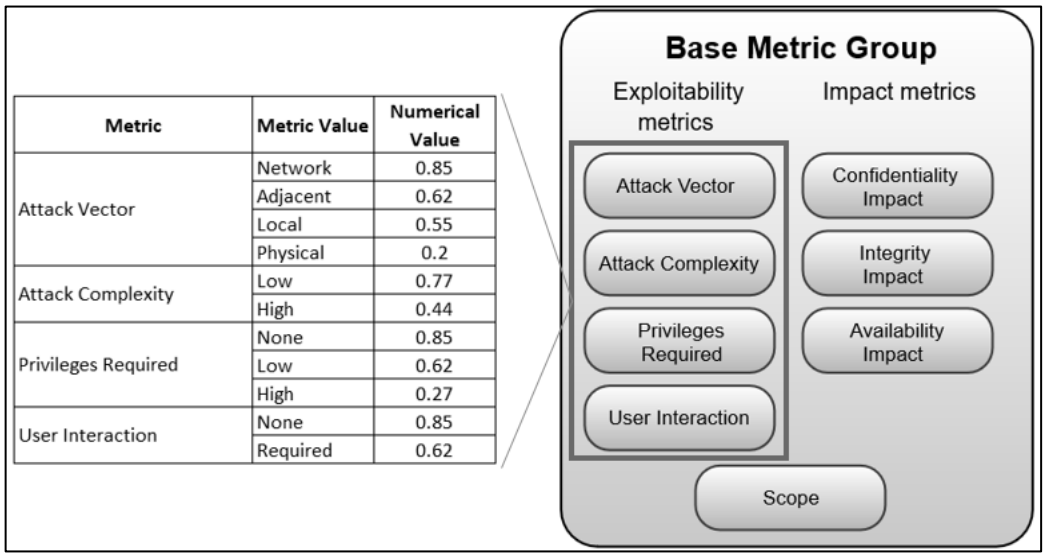


Abbildung 34: Metrische Gruppen des Common-Vulnerability-Scoring-Systems.
Quelle: Eigene Abbildung in Anlehnung an First.org (2022). Bildquelle: flaticon.com (2021).

Im Zuge der Bewertung nach dem CVSS wird zusätzlich eine textuelle Darstellung der Bewertungen nach den drei Metriken erzeugt. Sie wird Vektorstring genannt und enthält neben der Bezeichnung der Metrik auch den gesetzten Score-Wert. Für die Analyse der CVSS-Metrik wird die Basis-Metrik-Gruppe in der Version 3.1 herangezogen (siehe Abbildung 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

Abbildung 35: Zusammensetzung des CVSS-Basis-Scores.
Quelle: Eigene Abbildung in Anlehnung an First.org (2022) und Ghani et al. (2013).[40]

In der Basis-Metrik gibt es Exploitability-Metriken und Impact-Metriken. Die Exploitability-Metriken bestehen aus den Parametern (bei CVSS „Metriken" genannt) Attack Vector (AV), Attack

[40] Die Exploitability E wird in CVSS v.3.1 über $E = 8.22 \cdot AV \cdot AC \cdot PR \cdot UI$ berechnet. Der Scope Change ist in der tabellarischen Darstellung nicht abgebildet.

Complexity (AC), Privileges Required (PR) und User Interaction (UI). Mit dem AV wird der Kontext eines Angriffs festgelegt: „Kann ein Angreifer aus der Ferne angreifen oder muss er z. B. physisch vor Ort sein?“. Die AC beschreibt „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). Mit PR wird nach CVSS „the level of privileges an attacker must possess before successfully exploiting the vulnerability” bewertet. UI wiederum umfasst „the level of privileges an attacker must possess before successfully exploiting the vulnerability” (First.org, 2022). Jeder dieser Parameter bewertet andere Aspekte einer Schwachstelle. Die Impact-Metriken setzen sich aus dem Impact der Schutzziele Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) zusammen. Darüber hinaus gibt es den Scope, mit dem ein Geltungsbereichswechsel durch einen Angriff abgebildet wird:

> 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).

Jede der CVSS-Metriken besteht aus Deskriptoren, z. B. für AC „Low“ und „High“. Diesen wird ein diskreter, numerischer Wert zwischen null und eins zugewiesen. Diese Zahlenwerte können als Beiträge zur Exploitability interpretiert werden, die von Experten abzuschätzen sind. In einem ersten Schritt wird die Häufigkeit der Vulnerabilitäts-Scores für alle möglichen Kombinationen untersucht. Beim CVSS wird aufgrund der möglichen Score-Kombinationen nicht der gesamte Ergebnisraum zwischen 0 und 10 abgedeckt: „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).

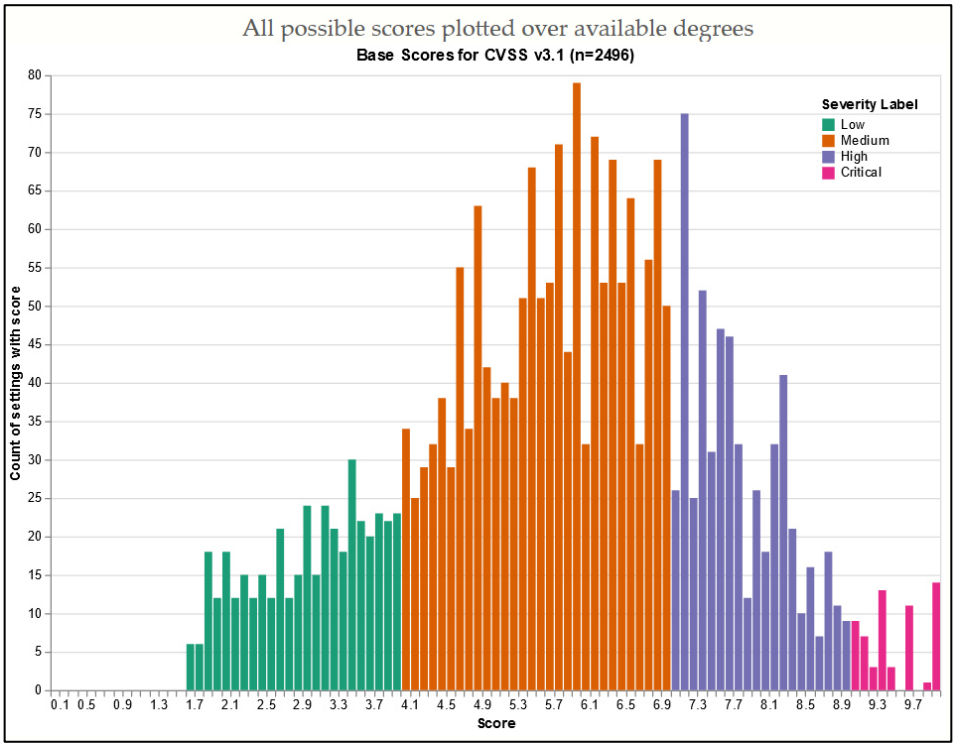


Abbildung 36: Plot aller möglichen CVSS-Vulnerabilitäts-Scores.
Quelle: Chester (2022).

Der Darstellung der Häufigkeiten der Vulnerabilitäts-Scores in Abbildung 36 ist zu entnehmen, dass der nächstniedrigere Score zu 1.6 den Wert Null hat (siehe Abbildung 37). Dieser liegt nur dann vor, wenn es keinen Impact gibt, d. h. Vertraulichkeit, Verfügbarkeit und Integrität sind auf „None“ gesetzt.

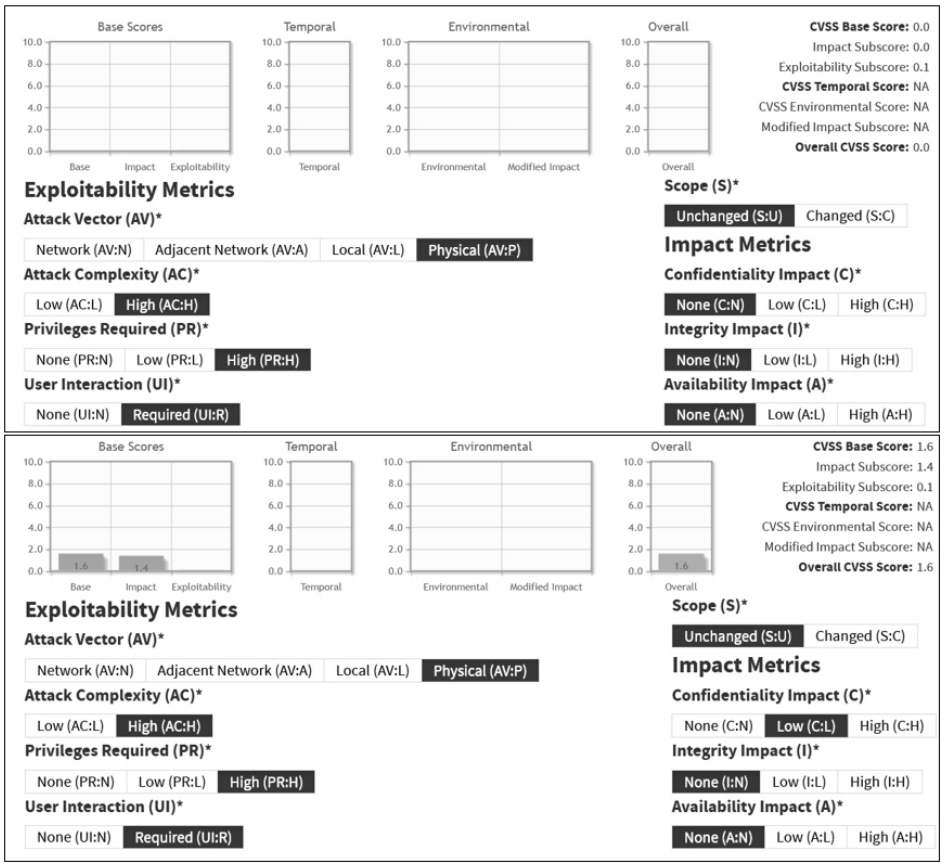


Abbildung 37: CVSS-Vulnerabilitäts-Scores, Vergleich von Konfigurationen.
Quelle: NIST CVSS (2022).

Darüber hinaus geht aus dem CVSS hervor, dass mit physischen Angriffen nie dasselbe Vulnerabilitätsniveau wie bei Netzwerk-Angriffen erreicht werden kann. Das liegt zum einen darin begründet, dass Physical den numerischen Wert 0.2 besitzt und Network den numerischen Wert 0.85. Zum andern liegt in der CVSS-Metrik zur Ermittlung des Vulnerabilitäts-Scores keine Gewichtung von physischen Angriffen und Netzwerkangriffen vor. Das bedeutet, dass z. B. nicht berücksichtigt werden kann, wie groß der Anteil an physischer Infrastruktur und IT-Infrastruktur in konkreten Anwendungsfällen ist. Die Annahme „Physical = 0.2“ und „Network = 0.85“ setzt Annahmen voraus. Eine solche Annahme kann nach Wurm (2022) sein:

> Physische Angriffe sind […] nicht weniger wahrscheinlich [als Netzwerkangriffe], sie erfordern allerdings den zumindest zeitlich beschränkten Zugriff. Das Gelegenheitsfenster ist bei Angriffen auf Internetverbindungen praktisch unendlich und zudem leicht skalierbar, indem weltweit verteilte Ressourcen (und Komplizen) eingebunden werden können.
> (Wurm, 2022, S. 49)

Aus den CVSS-Spezifikationen der First.org (2022) gehen alle Annahmen zur Festlegung der numerischen Werte, die hinter den Ausprägungen der Bewertungsparameter stehen, nicht klar hervor. Die Bewertung mittels der CVSS-Metriken zur Bestimmung des Vulnerability-Scores ist „not justified, either formally or empirically“ (Spring et al., 2018, S. 1). Eine Infrastruktur könnte beispielsweise physisch stärker ausgeprägt sein als informationstechnisch. Das

müsste sich in CVSS widerspiegeln, tut es aber nicht. CVSS-Kritik aus Berichten der IT-Community seit dem Jahre 2007 wird z. B. in Spring et al. (2018, S. 3) folgendermaßen zusammengefasst: Unzureichende Berücksichtigung des Kontexts (sowohl technisch als auch menschlich-organisatorisch); Nichtberücksichtigung der materiellen Folgen einer Bedrohung (ob Leben oder Eigentum bedroht ist); Probleme bei der operativen Bewertung (inkonsistente oder gebündelte Bewertungen, Schwächen im Algorithmus-Design).

In Braband (2004) wird grundsätzlich davor gewarnt, mit Scores auf einer Ordinalskala wie mit quantitativen Werten z. B. auf einer Kardinalskala zu rechnen. In Allodi et al. (2018) wird hervorgehoben, dass die CVSS-Metrik mathematisch keinen Sinn ergibt, weil es sich bei den Expertenangaben zu den Exploitability-Beiträgen um Ordinalwerte handelt. Auf der Webseite TheoryOf von Chester (2021) wird das Problem anschaulich wie folgt erklärt:

> 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).

In Krisper (2021) wird das Problem derart erläutert:

> 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, S. 5).

Die Problematik bei der Rechnung mit Ordinalwerten wird auch in Petr et al. (2022) aufgezeigt.

3.2.1 Reduktion von metrischen Verwerfungen durch Logarithmierung

Zur Bestimmung der Exploitability werden im CVSS nach First.org (2022) vier Parameter bewertet: Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) und User Interaction (UI). In Braband (2019) wird nun vorgeschlagen, die CVSS-Exploitability-Parameter als in Reihe geschaltete Barrieren zu interpretieren. Das soll dem Prinzip der Defense in Depth (DiD) entsprechen. Folgende Klassifizierungen werden verwendet: AV steht für den Ort des IT-Angriffs (physische Barriere), AC für die Komplexität des Angriffs aus technischer Sicht (technische Barriere) und PR für die erforderlichen Rechte auf Seiten des Nutzers bzw. UI für die Notwendigkeit der Nutzerinteraktion (organisatorische Barriere). Die einzelnen Barrieren werden als unabhängig voneinander interpretiert, das bedeutet beispielsweise, dass die PR-Barriere keinen Einfluss auf die UI-Barriere hat. Liegt Unabhängigkeit zwischen den Barrieren vor, können die Exploitability-Beiträge von AV, AC, PR und UI multiplikativ verknüpft werden.

In dem Barriere-basierten CVSS-Ansatz wird ein Likelihood of Exploitability (LoE) Score ermittelt, indem die einzelnen Exploitability-Beiträge addiert und auf einer Bewertungsskala einsortiert werden. Damit die Addition der Exploitability-Beiträge ermöglicht werden kann, wird in Braband (2019) die log-Transformation der numerischen CVSS-Werte vorgeschlagen. Der Ansatz in Braband (2019) beruht auf der Feststellung, dass ein quantitativer Risikoansatz in einen semi-quantitativen Ansatz (Addition von CVSS-Scores) umgewandelt werden kann, indem ein Logarithmus auf das quantitative Modell angewendet wird. Die Anwendbarkeit dieser Idee gilt unter der Voraussetzung, dass die Exploitability-Beiträge quantitativ multipliziert werden müssen. Das wird beim CVSS vermutet ($E = 8.22 \cdot AV \cdot AC \cdot PR \cdot UI$) (First.org, 2022). Darüber hinaus ist die log-Transformation nur durchführbar, wenn die Werte, die transformiert werden

sollen, positiv sind. Für die Zahlenwerte, die hinter den Ausprägungen der CVSS-Bewertungsparameter stehen, ist dies zutreffend. Die log-Transformation bringt den Vorzug mit sich, dass sich die einzelnen Exploitability-Beiträge potenziell auf einer Skala von mehreren Größenordnungen bewegen können, so z. B. über mehrere Dekaden hinweg (Braband, 2008). Die Skalierung von Exploitability- bzw. Risiko-Beiträgen kann mit der Bewertung nach CVSS weder additiv noch multiplikativ dargestellt werden, weswegen das Logarithmieren verwendet wird.

Die Basis b des Logarithmus kann entsprechend der „Auflösung" der semi-quantitativen Skala gewählt werden (Braband, 2019). Im Prinzip kann jedoch jede beliebige Basis b gewählt werden, da der Logarithmus eine mathematische Funktion ist, die unabhängig von der Basis die gleichen mathematischen Eigenschaften besitzt: Wenn Daten logarithmiert werden, ändern sich ihre mathematischen Eigenschaften nicht, unabhängig davon, welche Basis gewählt wird. Der Logarithmus zur Basis 10 hat z. B. den Vorteil, dass er leicht verständlich ist. Das insbesondere im Kontext von Messungen und Skalen, die auf ein Dezimalsystem verwenden. Folgende Eigenschaften besitzt gem. Braband (2008) ein log-transformierter Bewertungsansatz: Kontinuität der Skala, rationale Skalierung, Monotonie, Vergleichbarkeit und Sensitivität. Nachfolgend wird am Beispiel des CVSS analytisch gezeigt, dass das Logarithmieren Verwerfungen innerhalb einer multiplikativen Scoring-Metrik reduziert:

Risiko wird in der IT-Security als ein zusammengesetztes Ereignis betrachtet, bestehend aus Bedrohung, Vulnerabilität (Exploitability) und Auswirkungen. Die Einzelbeiträge des Risikos (Elementarereignisse) werden klassischerweise multiplikativ verknüpft, sodass sich ein IT-Risiko unter Annahme der Gl. (1) (P(Bedrohung) = 1) aus der Exploitability E und dem Impact I zusammensetzt (siehe Gl. (2)):

$$\text{R} = \text{Exploitability x Impact} \tag{2}$$

Beeinflussen sich die Ereignisse E und I nicht gegenseitig, kann das IT-Risiko als Multiplikation aus E und I geschrieben werden (siehe Gl. (3)):

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

In der IT-Security werden Risiken durch Scoring-basierte Metriken beschrieben. Den Stufen der Einzelbeiträge entsprechend, werden Zahlen auf einer Bewertungsskala eingeordnet. Wenn E und I linear skaliert wären, ließen sich IT-Risikobewerte berechnen, die proportional zum wahren Risiko sind (siehe Gl. (4)):

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

Wenn die Zusammenhänge zwischen den Zahlenwerten und Risikobeiträgen nichtlinear sind, kann es zu Verwerfungen kommen: Eine auf Zahlenwerten beruhende Risikobewertung entspricht unterschiedlichen realen Risikowerten. Diese Verwerfungen sollen am Beispiel CVSS demonstriert werden. Die CVSS-Bewertungsparameter AV, AC, PR und UI haben unterschiedlich viele Stufen:

1. AV: vier Stufen
2. AC: drei Stufen
3. PR: drei Stufen
4. UI: zwei Stufen

Mithilfe von Experten können für die Bewertungsparameter von CVSS zunächst gleich viele Stufen definiert werden, so die Annahme, z. B. vier Stufen pro Bewertungsparameter (siehe als

Beispiel Tabelle 28). Dies Stufen werden hier als wahre Beiträge für die Exploitability aufgefasst, auch wenn es sich strenggenommen um subjektive Experteneinschätzungen (Ordinalwerte) handelt.

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

Tabelle 28: Exploitability-Stufen und Exploitability-Beiträge.
Quelle: Eigene Tabelle in Anlehnung an First.org (2022).[41]

Die Stufenwerte werden der Größe nach geplottet. Anschließend werden die Kurvenverläufe jeweils durch eine Regressionsfunktion dargestellt (siehe Abbildung 38). Hinter den einzelnen Exploitability-Beiträgen werden annähernd lineare Zusammenhänge vermutet.

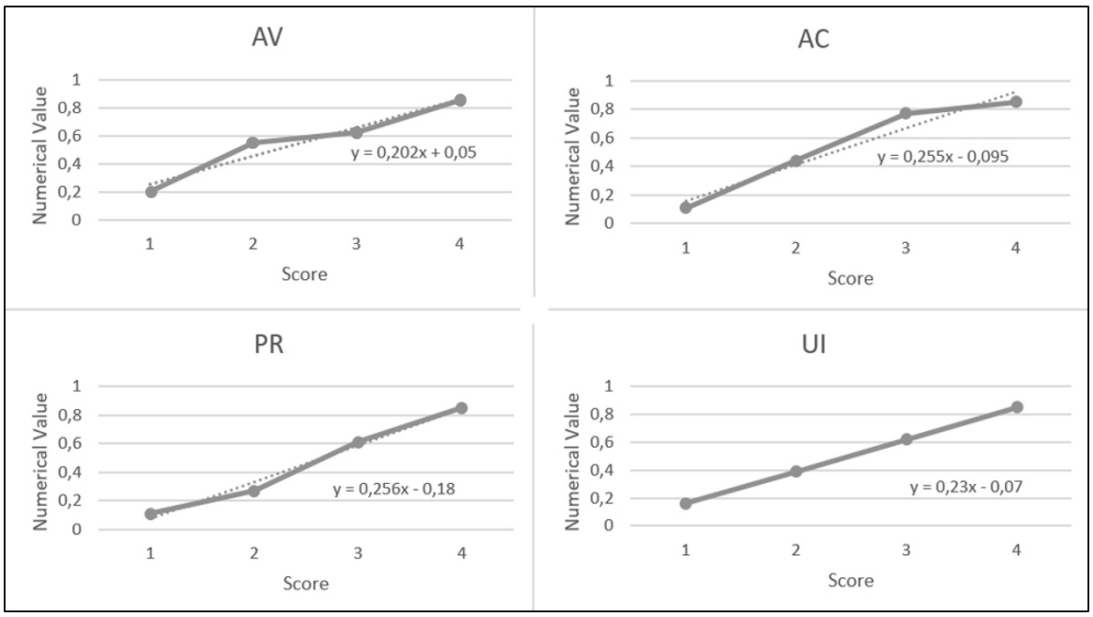


Abbildung 38: Plot der Exploitability-Beiträge von CVSS.
Quelle: Eigene Abbildung.

In die Risikobewertung fließen die Exploitability-Beiträge AV, AC, PR und UI und der Impact I ein. Das Produkt aus AV, AC, PR und UI wird als Wahrscheinlichkeit für die Exploitability angenommen (Lyu et al. 2020).[42] Für den Impact I wird der Zusammenhang $I = 10^i$ [Euro] angenommen (siehe Tabelle 29).

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

Tabelle 29: Impact-Stufen und monetäre Verlustwerte.
Quelle: Eigene Abbildung.

Für die Exploitability-Beiträge werden auf Basis der Tabelle 28 und der Abbildung 38 folgende Zusammenhänge angenommen (siehe Gl. (5)):

[41] Kursiv markiert werden Ergänzungen beispielhaft vorgenommen.
[42] Die Multiplikation der Beiträge von AV bis UI macht Sinn, wenn wie z. B. in Braband (2019) angenommen wird, dass es sich bei AV bis UI um Barrieren einer Schwachstelle in Reihenschaltung handelt.

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)

Für die Parameterkombinationen „av = 1, ac = 2, pr = 3, ui = 4, i = 1“ und „av = 4, ac = 3, pr = 2, ui = 1, i = 1“ ergibt sich, der semi-quantitativen Metrik folgend, derselbe Risikowert ($r_1 = r_2 =$ 24). Das reale Risiko ist aber für beide Fälle unterschiedlich, wie die nachfolgende Rechnung zeigt (siehe Gl. (6)):

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

$$\begin{aligned} &R_1 \\ &= (0.202 \cdot 1 + 0.05) \cdot (0.255 \cdot 2 - 0.095) \cdot (0.256 \cdot 3 - 0.18) \cdot (0.23 \cdot 4 - 0.07) \cdot 10^1 \\ &= 0.52 \text{ [Euro]} \\ &R_2 \\ &= (0.202 \cdot 4 + 0.05) \cdot (0.255 \cdot 3 - 0.095) \cdot (0.256 \cdot 2 - 0.18) \cdot (0.23 \cdot 1 - 0.07) \cdot 10^1 \\ &= 0.31 \text{ [Euro]} \end{aligned} \tag{6}$$

Bei unterschiedlicher Skalierung der Risikobeiträge lässt sich durch eine Transformation wieder ein proportionaler Zusammenhang zwischen den Stufenwerten der Risikobeiträge und dem logarithmierten Risiko herstellen. Das soll am Beispiel der fünfteiligen IT-Risikobewertung „$R = AV \cdot AC \cdot PR \cdot UI \cdot I$" bzw. „$r = av \cdot ac \cdot pr \cdot ui \cdot i$" gezeigt werden. Die Konstante (8.22), wie sie bei der CVSS-Berechnungsformel für die Exploitability verwendet wird[43], wird hier weggelassen, da sie lediglich den Exploitability-Wert skaliert. Die Reihenfolge der Risikowerte bleibt unverändert. Durch Logarithmieren der IT-Risiko-Funktion R mit dem Zusammenhang in Gl. (7):

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

kann für die einzelnen Risikobeiträge AV, AC, PR, UI und I der Logarithmus gebildet werden. Für den Bewertungsparameter Impact wird die Basis 10 gewählt (siehe Gl. (8)).

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

Die Zahlenwerte für av, ac, pr, ui und i eingesetzt ergibt (siehe Gl. (9)):

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

Das führt für die Parameterkombinationen „av = 1, ac = 2, pr = 3, ui = 4, i = 1“ zu ln(r) = - 0.648 und für „av = 4, ac = 3, pr = 2, ui = 1, i = 1“ zu ln(r) = - 1.186. Die realen IT-Risikobeiträge ergeben sich durch Anwendung der Umkehrfunktion zu $e^{-0.648} = 0.52$ [Euro] bzw. $e^{-1.186} = 0.31$ [Euro]. Diese entsprechen den Risikowerten R_1 bzw. R_2 aus Gl. (6). Wenn folglich die Risikobe-

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

schreibung multiplikative Zusammenhänge beinhaltet, das Scoring jedoch durch additive Zusammenhänge gekennzeichnet ist, dann ist die log-Transformation ein sinnvoller Schritt, um Verwerfungen zu reduzieren, wie sie in der multiplikativen Scoring-Metrik vorzufinden sind. Zu beachten ist, dass ein Anwender in die Funktionen der Risikobeiträge auch Werte wie z. B. „3.5“ oder „5“ einsetzen könnte. Um das zu vermeiden, ist die strenge Annahme zu definieren, dass für die Funktion eines Risikobeitrags in diesem Fall nur die Scores „1“, „2“, „3“ und „4“ eingesetzt werden dürfen.

3.2.2 Analyse des Barriere-basierten CVSS-Ansatzes

In Braband (2019) wird eine Transformation der Zahlenwerte der Exploitability-Beiträge aus dem CVSS in log-Scores vorgenommen. Die Basis, zu welcher beispielsweise in Braband (2019) logarithmiert wird, wird zu 0.6 gesetzt: Die Wahl dieser Basis wird darin begründet, dass die Zahlenwerte der Exploitability-Beiträge einen Wertebereich von 0.2 bis 0.85 (≈ 0.6) aufspannen. In Braband (2019) werden die resultierenden log-Scores zu ganzzahligen Werten aufgerundet, um die Ergebnisse einfacher darzustellen.[44] Als Beispiel wird in Gl. (10) die Transformation für das Merkmal "Physical" des Parameters AV durchgeführt:

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

Alle CVSS-Ausprägungen von AV bis UI können nach der Formel in Gl. (10) mit dem Logarithmus in neue Zahlenwerte respektive log-Scores transformiert werden. Die zu den Ausprägungen der Bewertungsparameter gehörenden log-Scores sind in Tabelle 30 zu sehen.

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		

Tabelle 30: log-transformierte CVSS-Scores.
Quelle: Braband (2019).[45]

Die Wahl der Basis, zu der ein Datensatz log-transformiert wird, beeinflusst die Skalierung und damit auch die Interpretation der transformierten Werte. Sie hat jedoch keinen Einfluss auf die Berechnung eines wahren Risikowerts. Nachfolgend wird ein Beispiel zur Veranschaulichung gezeigt: Die AV-Skala wird einmal zur Basis 0.6 (wie in Braband vorgeschlagen) und einmal beispielhaft zur Basis 3 logarithmiert (siehe Gl. (11) und Gl. (12)):

$$\log - \text{Transformation von } AV \; zur \; Basis \; 0.6 = \ln 0.6 \frac{\ln AV}{\ln 0.6} = \; ln \; 0.6 \cdot \log_{0.6} AV \tag{11}$$

[44] Rundungsregel: Ist die erste Dezimalstelle der Ziffer eine 0, 1, 2, 3 oder 4, dann wird abgerundet. Ist die erste Dezimalstelle der Ziffer eine 5, 6, 7, 8 oder 9, dann wird aufgerundet.

[45] Können Angreifer aus der Ferne (Kontext: Network) potenzielle Angriffe ausführen, so ist dies aus Betreibersicht gravierender als die Durchführung von Angriffen mit dem Kontext Physical. Gründe dafür können z. B. sein, dass es eine Vielfalt von möglichen Einsprungpunkten auf Netzwerkebene geben und der Aufwand für Angreifer geringer sein kann als im Falle eines physischen Angriffs.

Für AV = Physical (0.2) ergibt sich in Gl. (11) eingesetzt der Wert -1.6. Eine Rücktransformation mittels $e^{-1.6}$ ergibt 0.2.

$$\log - \text{Transformation von } AV \; zur \; Basis \; 3 = \ln 3 \frac{\ln AV}{\ln 3} = ln\, 3 \cdot \log_3 AV \tag{12}$$

Für AV = Physical (0.2) ergibt sich in Gl. (12) eingesetzt der Wert -1.6. Eine Rücktransformation mittels $e^{-1.6}$ ergibt 0.2. In beiden Fällen ist das Ergebnis identisch. Der Liklihood-of-Exploitability-Score (LoE) wird berechnet, indem die Summe der log-transformierten Exploitability-Beiträge gebildet wird (siehe Gl. (13))[46]:

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

Der Ergebnisraum der LoE-Werte wird anschließend in Skalenkategorien einsortiert (Braband 2019). Die niedrigste Wertesumme „0" entspricht einem sehr hohen Wahrscheinlichkeitslevel, die Werte „1-3" einem hohen Wahrscheinlichkeitslevel, usw. (siehe Tabelle 31). Ein Set an LoE-Werten wird somit einer bestimmten Likelihood-Kategorie zugeordnet. Über die log-Transformation der Zahlenwerte der Exploitability-Beiträge hinaus wird vorgeschlagen, die Kategorien, die hinter LoE-Score-Ergebnisse geschrieben werden können, einer Reihe von Barrieren zuzuordnen (siehe Tabelle 31 dritte Zeile).

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

Tabelle 31: LoE- Skala basierend auf dem CVSS-Barriere-Modell.
Quelle: Braband (2019).[47]

In Braband (2019) wird anstelle von „$ln\ 0.6 \cdot \log_{0.6} AV$" nur mit „$log_{0.6}(AV)$" gerechnet, so ist die naheliegende Vermutung, weil mit „$log_{0.6}(AV)$" positive log-Werte erzeugt werden. Durch Anwendung von „$ln\ 0.6 \cdot \log_{0.6} AV$" resultieren dagegen negative log-Werte (siehe Gl. (14):

$$\begin{aligned} &1.\ log_{0.6}(AV = 0.2) = 3.15 \\ &2.\ ln\ 0.6 \cdot \log_{0.6}(AV = 0.2) = \text{-}1.6 \end{aligned} \tag{14}$$

Neben der spezifischen Schutzwirkung (dem LoE-Score) wird auch die Barriere-Tiefe in die Bewertung einbezogen. Das Hinzufügen einer weiteren Barriere würde keinen Einfluss auf die LoE haben, wenn für die neue Barriere ein Score „0" gesetzt werden würde. Es gibt dem Ansatz zufolge eine Reduktion der LoE, wenn bei der neuen Barriere ein Score größer „0" gesetzt wird. Mit jeder hinzukommenden Barriere wird die LoE kleiner. Unter der Annahme, dass beispielhaft die Variable „System Check" (SC) als fiktive prozedurale Barriere mit den exemplarischen Ausprägungen niedrig (log-Score "0") und hoch (log-Score „1") in dem Barriere-basierten CVSS-Schema berücksichtigt wird, ergibt sich der LoE-Score (hier LoEmod) mittels Gl. (15):

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

Auf Basis LoEmod würde es eine weitere Kategorie auf der Exploitability-Skala geben, z. B. "Sehr sehr unwahrscheinlich := Very very unlikely (VVUL)" Eine Rücktransformation der LoE-Scores kann mit Gl. (16) gelingen (siehe Tabelle 32 vierte und fünfte Zeile).[48]

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

[46] Der Scope Change wird hier nicht berücksichtigt.
[47] „Sehr wahrscheinlich = Very Likely (VL)", „Wahrscheinlich = Likely (L)", „Möglich = Possible (P)", „Unwahrscheinlich = Unlikely (UL)", „Sehr unwahrscheinlich = Very Unlikely (VUL)".
[48] Das „e" auf der linken Seite der Gleichung bezeichnet die Exploitability. Das „e" auf der rechten Seite meint die Euler'sche Zahl.

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

Tabelle 32: LoE-Einstufungen auf Basis der Barriere-basierten CVSS-Metrik.
Quelle: Eigene Tabelle in Anlehnung an Braband (2019).

Wenn angenommen wird, dass die Zahlenwerte von CVSS realen Beiträgen zur Exploitability entsprechen (wie z. B. in Lyu et al. (2020) interpretiert), dann können die rücktransformierten log-Score-Summen als Wahrscheinlichkeit für die Exploitability aufgefasst werden. Wie Tabelle 32 entnommen werden kann, gibt es Lücken im Exploitability-Wertebereich von 0 % bis 100 %. Das liegt in den ganzzahligen Sprüngen zwischen den einzelnen LoE-Scores begründet. Gäbe es beispielsweise einen LoE-Score „3.5“, dann würde sich die Wahrscheinlichkeit für die Exploitability zu $\mathrm{e} = e^{\ln(0.6) \cdot 3.5} = 0.167$ ergeben. Folgende Punkte können in diesem Zusammenhang festgestellt werden:

1. Eine Exploitability von „e = 1“ kann gem. der quantitativen Risikobeschreibung von CVSS nie erreicht werden, da das größte Produkt aus „AV · AC · PR · UI“ (0.85^4 =) 0.522 beträgt.
2. Das kleinste Produkt, das über den multiplikativen Zusammenhang von CVSS darstellbar ist, beträgt (E = 0.2 · 0.44 · 0.27 · 0.62 =) 0.0147. Nach der Barriere-basierten CVSS-Bewertung, wie in Braband (2019) vorgeschlagen, sind jedoch auch niedrigere Exploitability-Werte abbildbar (siehe Tabelle 32).

Worin liegt diese Differenz begründet? In Braband (2019) werden die Zahlenwerte der Exploitability-Beiträge mittels $log_{0.6}(Exploitability\_Beitrag)$ transformiert und anschließend auf ganzzahlige Werte gerundet: Aus dem Exploitability-Beitrag $log_{0.6}(0.85)$ = 0.318 wird beispielsweise $log_{0.6}(0.85) \approx 0$. Dabei handelt es sich um einen von insgesamt vier Beiträgen, die aufsummiert werden. Die log-Score-Summe für die nicht gerundeten log-transformierten Werte ergibt sich unter Berücksichtigung der maximalen CVSS-Ausprägungen zu (0.318 + 0.318 + 0.318 + 0.318 =) 1.272. Dem Bewertungsschema in Braband (2019) folgend ergibt sich dagegen für dieselben CVSS-Ausprägungen eine log-Score-Summe von (0 + 0 + 0 + 0 =) 0. Bei einer Rücktransformation ergibt sich zwischen beiden Varianten eine Differenz von $|e^{\ln(0.6) \cdot 0} - e^{\ln(0.6) \cdot 1.272}|$ = 1 – 0.522 = 0.478(!) (siehe obigen Feststellungspunkt eins). Wenn das Produkt aus den Exploitability-Beiträgen tatsächlich einer Wahrscheinlichkeit (in %) entspräche, dann würde der Ansatz in Braband (2019) aufgrund der Rundung der log-Scores zu mitunter großen Fehleinschätzungen führen. Ein wichtiger offener Punkt, welcher im Barriere-basierten CVSS-Ansatz angemerkt wird, ist die Zuordnung der LoE-Skalenkategorien zu Wahrscheinlichkeiten (Braband 2019).

Da die Exploitability-Beiträge der quantitativen CVSS-Metrik bisher empirisch nicht belegt sind (Spring et al., 2018), ist infrage zu stellen, inwiefern die Anwendung der LoE-Skala tatsächlich bessere Ergebnisse liefert als der klassische CVSS-Ansatz. Ob die Berücksichtigung der Barriere-Tiefe im Rahmen der Exploitability-Bewertung nach CVSS Besserungen mit sich bringt, lässt sich schlussfolgernd mit den CVSS-Metriken nur schwer verifizieren oder falsifizieren. Das ist anders als in der physischen Sicherheitsbewertung. Hier kann auf Basis des Zeitspiels zwischen der Eindringzeit eines Angreifers und der Reaktionszeit eines Verteidigers entlang eines Pfades die Sicherheitsfähigkeit eines Systems objektiv gemessen werden. Der Pfad kann dabei selbst aus mehreren Barrieren bestehen. Es wird folglich eine quantitative Metrik benötigt, um den postulierten DiD-Effekt systematisch zu analysieren.

Weil in der IT-Sicherheitsbewertung eine Metrik mit objektivem Wirkmechanismus zur objektiven Bewertung der Sicherheitsfähigkeit schwerlich zu finden ist, damit die Effizienz des CVSS-Weges nachgerechnet werden kann, wird in Termin et al. (2022) vorgeschlagen, architekturellen und metrische Überlegungen aus dem Barriere-basierten CVSS-Ansatz in der physischen Sicherheitsbewertung zu emulieren.[49] Es wird in Termin et al. (2022) die Problematik bei der Anwendung semi-quantitativer Metriken aus der IT-Perspektive beleuchtet. In der Analyse nach Termin et al. (2022) wurde die Architektur des physischen Systems so umgestaltet, dass sie den postulierten DiD-Effekt, wie er in der IT-Sicherheitsbewertung vorgeschlagen wird, nachbildet. Zu diesem Zweck werden die Protektion (P), Observation (O) und Intervention (I) als Performanz-lastige Barrieren interpretiert: Die Protektions-lastige Barriere, die Observations-lastige Barriere und die Interventions-lastige Barriere besitzen jeweils Eigenschaften der Protektion, Observation und Intervention. Eine der drei Bewertungsgrößen ist bei einer Barriere jeweils betont, während die anderen weniger stark ausgeprägt sind.

Das bedeutet, dass es für jede Barriere ein bestimmtes Zusammenspiel aller drei Bewertungsparameter gibt. Die Protektions-lastige Barriere hat beispielsweise eine betonte Protektion, jedoch auch geringe Observations- und Interventionsanteile; ansonsten wäre die Vulnerabilität an der Barriere maximal. Zur Abbildung des Prinzips der Performanz-lastigkeit werden in der Interventionsfähigkeitsmetrik (ICM) nach Lichte et al. (2016) Mittelwerte und Standardabweichungen der normalverteilten Parameter so definiert, dass das vermutete Wahrscheinlichkeitsintervall, welches sich aus der Summe der integralen Parameter Protektion, Observation und Intervention ergibt, quantitativ nachgerechnet werden kann. Es wird eine Kostenfunktion eingeführt, um die Vulnerabilitätsergebnisse über die Summe der integralen Parameter und über die ICM zu vergleichen. Die Ergebnisse der Analyse in Termin et al. (2022) zeigen, dass der im Barriere-basierten CVSS-Ansatz vorgeschlagene DiD-Zusatz in der CVSS-Bewertung für einige Szenarien bessere Ergebnisse liefert. Die Emulation hat jedoch keine eindeutigen Ergebnisse hervorgebracht. Nachfolgend werden Verwerfungen innerhalb des Barriere-basierten CVSS-Ansatzes diskutiert, und es werden Verbesserungen vorgeschlagen.

[49] Die emulierte Variante wird in Termin et al. (2022) entwickelt, um den in Braband (2019) postulierten Einfluss des DiD-Effekts quantitativ nachzubilden. Diese Überlegungen führen auf die Frage zurück, ob in der physischen Sicherheit gezeigt werden kann, dass bessere Vulnerabilitätsergebnisse erzeugt werden, wenn Ressourcen für Sicherheitsmaßnahmen auf mehrere, hintereinandergeschaltete Barrieren verteilt werden, anstatt alle Ressourcen auf eine einzige Barriere zu setzen. In dem klassischen Harnser-Schema und dem CVSS wird nicht zwischen einzelnen Barrieren bzw. Barrieren in Reihe unterschieden. Deswegen kann weder mit der Harnser-Metrik noch mit dem CVSS ein DiD-Effekt abgebildet werden. Mit der quantitativen Interventionsfähigkeitsmetrik ist dies möglich.

3.2.3 Reduktion von Verwerfungen im Barriere-basierten CVSS-Ansatz

In der physischen Sicherheit liegt bei jedem Bewertungsparameter der Harnser-Metrik dieselbe Stufentiefe (Score „1“ bis Score „5“) vor. Anders als in der physischen Security gibt es bei dem Barriere-basierten CVSS-Bewertungsschema unterschiedlich tiefe Ausprägungsstufen. Die Bedeutung unterschiedlicher Ausprägungen zeigt sich bei dem Vergleich des Barriere-basierten Ansatzes nach CVSS mit dem Ansatz nach Harnser. AV hat beispielsweise vier Slots, „Physical“, „Local“, „Adjacent“ und „Network“, während UI im klassischen CVSS nur zwei besitzt, „None“ und „Required“. Je nach Barriere-Tiefe und Barriere-Typ würde sich demnach die Likelihood-of-Exploitability-Skala (LoE) ändern. Angenommen, es wird zunächst die „AV-Barriere“ geschaltet. AV deckt einen log-Score-Bereich von „0“ bis „3“ ab. Danach wird die Barriere UI gesetzt. UI reicht von log-Score „0“ bis „1“. Nach dem DiD-Prinzip würde das zwei Barrieren in Reihe hintereinandergeschaltet bedeuten. Ist auf erster Position AV und in zweiter Position UI, dann würde sich die Skaleneinteilung in Tabelle 33 ergeben.

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

Tabelle 33: LoE bei Hintereinanderschaltung von AV und UI.
Quelle: Eigene Tabelle in Anlehnung an Braband (2019).

Werden die Barrieren getauscht, d. h. UI ist zuerst geschaltet und danach AV, dann kann die Kategorisierung der LoE-Skala anders aussehen (siehe Tabelle 34).

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

Tabelle 34: LoE bei Hintereinanderschaltung von UI und AV
Quelle: Eigene Tabelle in Anlehnung an Braband (2019).

Insofern in der permutierten Variante (in Tabelle 34) AV durch AC substituiert wird, ergibt sich in der zweiten Spalte eine LoE-Score-Range von „2“ bis „3“. Wenn hier erneut die Barrieren getauscht werden, sodass zuerst AC gesetzt und dann UI geschaltet wird, dann würde sich die Score-Rage der Werte, die hinter den Kategorien stehen, wieder ändern. Das wiederum bedeutet, dass die Reihenfolge der Barrieren einen Einfluss auf die Bewertung der Exploitability nach dem Barriere-basierten CVSS-Ansatz haben kann. Darüber hinaus können die Barrieren PR und UI jeweils den Wert „None“ annehmen. Ein „None“ bedeutet aber, dass es keine PR- bzw. UI-Barriere gibt. PR und UI sind folglich eine Art binärer Schalter. Wenn bei der Hintereinanderschaltung von PR und UI nun ein Experte die Barrieren jeweils auf „None“ setzt, muss sich in der LoE-Kategorisierung auch ein „DiD = 0“ (maximale Exploitability) wiederfinden. In dem Ansatz, wie in Braband (2019) dargestellt, wird dies zwar vorgeschlagen, jedoch haben die anderen Parameter, AC und AV, im Gegensatz zu UI und PR stets eine Minimalausprägung. Es gibt bei AV oder AC keine Ausprägung „None“. Würde jedoch nur die AV-Barriere vorliegen, und rein theoretisch angenommen, es gäbe eine Ausprägung „AV = None“, dann bedeutet dies:

1. Es ist keine Barriere da, d. h. DiD = 0. Der Barriere-basierten CVSS-Metrik zufolge bedeutet dies maximale Exploitability.
2. Es gibt keinen Kontext für ein Bedrohungsszenario. Wenn es das nicht gibt, dann liegt auch keine Exploitability vor.

Diese beiden Punkte widersprechen sich. Die Bewertungsebene von AV bis UI ist unterschiedlich. Es gibt schlussfolgernd Verwerfungen im CVSS-Bewertungsschema. Dieses CVSS-Bewertungsschema erfordert, dass AV als Bewertungsparameter immer mitberücksichtigt werden muss und nicht „None" sein darf. Das ist anders als in dem emulierten, Barriere-basierten Ansatz in der physischen Security-Bewertung nach Termin et al. (2022). Gibt es beispielsweise keine Protektions-lastige, Observations-lastige oder Interventions-lastige Barriere im betrachteten System, kann die fehlende Barriere aus der Bewertung herausgenommen werden, ohne dass dies zu Verwerfungen führt. In der emulierten Sicherheitsbewertung gibt es den Randfall DiD = 0 nicht, wenn angenommen wird, dass es mindestens eine physische Barriere gibt. Das liegt daran, dass bei jeder physischen Barriere im emulierten Ansatz eine gewisse Performanz-Lastigkeit vorausgesetzt wird. Maximale Vulnerabilität – und damit DiD = 0 – wäre hier nur abbildbar, wenn es gar keine Barrieren gibt, also weder eine Protektions-lastige Barriere, noch eine Observations-lastige Barriere oder eine Interventions-lastige Barriere.

Übertragen auf das Barriere-basierte CVSS-Bewertungsschema bedeuten die vorangegangenen Überlegungen, dass im Sinne einer guten Metrik (siehe Kapitel 2.4) dasselbe Abstraktionsniveau bezogen auf die Parameter und deren Ausprägungen gewählt werden sollte. Schlussfolgernd wird vorgeschlagen, dass die vorliegenden „None"-Ausprägungen bei CVSS durch einen Deskriptor ausgetauscht werden, welcher eine konkrete Aktivierungsstufe ungleich null beschreibt. Andersherum, wenn DiD = 0 bei allen möglichen Permutationen von IT-Barrieren, also auch im Falle der Hintereinanderschaltung von AV und AC, abgebildet werden soll, müsste es jeweils bei AV und AC die Ausprägungen „None" geben. Weil das aber aus logischen Gesichtspunkten auszuschließen ist (ohne die AV-Barriere gibt es keinen Kontext für ein Bedrohungsszenario), ist die erstgenannte Variante vorzuziehen. Darüber hinaus werden beim emulierten Ansatz in der physischen Security bei allen drei Parametern, Protektion, Observation und Intervention, vergleichbare Ausprägungsstufen gewählt. Es gibt für jeden Parameter die Scores von „1" bis „5".

Das erlaubt mit Blick auf das in Braband (2019) eingeführte Bewertungsschema eine konsistente Skaleneinteilung hinsichtlich der Verteilung von Scores auf die Skalenkategorien. In dem Barriere-basierten CVSS-Ansatz sind die Einordnung von Scores zu Kategorien aber, bedingt durch die unterschiedliche Tiefe der Parameterausprägungen (z. B. bei AV = 4 und bei UI = 2) und die Anordnung der Barrieren, unterschiedlich. Um dieser Herausforderung zu begegnen, kann überlegt werden, die Parameter hinsichtlich ihrer Ausprägungstiefe gleich aufzubauen, sodass AV bis UI vergleichbare Stufentiefen haben (siehe beispielhaft Tabelle 35). Die vorgeschlagenen Ergänzungen sind kursiv hervorgehoben.

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

Tabelle 35: Modifikation des Barriere-basierten CVSS-Scorings zur Anpassung der LoE-Skala. Quelle: Eigene Tabelle in Anlehnung an Braband (2019).

Übertragen auf die Definition der Ausprägungen einer PR Barriere bedeutet das z. B. die Änderung von „None", „Low", „High" zu „Low", „Medium", „High" und „Very High". Es wird angenommen, dass es in irgendeiner Form erforderliche Rechte geben muss. Hinter den einzelnen Stufen können Rollen und damit verbundene Rechte stehen, beispielsweise einfacher Benutzer, Benutzer mit administrativen Rechten (z. B. Teamleiter), Manager und Entwickler. Für die UI-Barriere ist eine Erweiterung von „None" und „Required" zu aktivierten Stufen etwas schwieriger. Hier kann z. B. überlegt werden, den Grad der Benutzerinteraktion in vier Stufen einzuteilen. Das bedeutet, es ist zu fragen, wie viele Benutzeraktionen ein Benutzer durchführen muss, um eine Ausbeutung zu erleichtern, und welche Art Benutzer eine Benutzeraktionen ausführen muss (siehe Tabelle 35).[50] Eine Ausbeutung ist vermutlich bei Aktionen durch einen einfachen Benutzer leichter als bei Aktionen durch Systemadministratoren.

Eine Änderung an einer Metrik an sich erfordert grundsätzlich eine Begründung, dass die Änderung reale Risiken besser abbildet. Es kann zunächst gezeigt werden, dass die drei vorgeschlagenen Modifikationen Verwerfungen innerhalb der CVSS-Metrik reduzieren:

1. Die log-Transformation reduziert Metrik-inhärente Verwerfungen, wenn die Risikobeschreibung multiplikative Zusammenhänge besitzt.
2. Aktivierung der Parameterausprägungen, sodass die Ausprägungen ungleich null sind: Durch diese Modifikation wird die Problematik bei der Festlegung eines DiD = 0 im Barriere-basierten CVSS-Ansatz gegenüber der physischen Sicherheitsbewertung aufgelöst. DiD = 0 kann es nur geben, wenn entweder UI oder PR „None" annehmen. Bei AV und AC gibt es jedoch kein „None". Wenn AV und AC nun als Barrieren ohne UI und PR stehen würden, dann würde die Bewertungs-Skala eine andere sein, als wenn UI oder PR oder beide Bewertungsgrößen mitberücksichtigt werden würden.
3. Jeder Parameter hat gleich viele Ausprägungsstufen: Durch diese Modifikation kann die Skaleneinteilung im Barriere-basierten CVSS-Ansatz normalisiert werden, indem definiert wird: Mit jeder hinzukommenden Barriere wird eine weitere Kategorie hinzugefügt, die dieselbe Score-Range an Breite hat wie die bisherigen Kategorien.

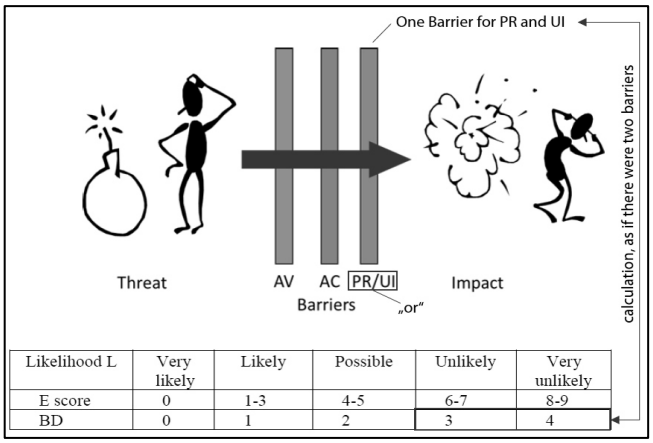
Die Bewertungsparameter von AV bis UI haben nach Tabelle 35 jeweils vier Ausprägungsstufen. Bei der Harnser-Metrik haben Protektion, Observation und Intervention jeweils fünf Ausprägungsstufen. Nun kann überlegt werden, sowohl in der IT-Vulnerabilitätsbewertung als auch in der physischen Vulnerabilitätsbewertung gleich viele Stufen pro Vulnerabilitätsbeitrag zu definieren, z. B. fünf Stufen für jeden Vulnerabilitätsbeitrag. Für das CVSS würde dies bedeuten, dass für den AV ein fünfter Bedrohungskontext identifiziert und definiert werden muss. Ebenso ist für die Beiträge von AC bis UI eine fünfte Stufe festzulegen. Die Erweiterung der Skalen der Exploitability-Beiträge sollte mit Experten konsolidiert werden. Grundsätzlich stellt diese Aufgabe einen Anwender der CVSS-Bewertungsmetrik vor schwer zu lösende Herausforderungen, weil es diese fünfte Stufe möglicherweise auch gar nicht gibt. Dieser Ansatz ist daher impraktikabel. Anstelle einer Anpassung der Skalenstufen aus dem CVSS an die Harnser-Metrik kann eine Anpassung der Skalenstufen von Protektion, Observation und Intervention an die Skalen des CVSS erfolgen:

Denkbar ist hier, für Protektion, Observation und Intervention nur vier Stufen – anstatt fünf Stufen – festzulegen. Die fünfte Stufe der Scorings für die Beiträge physischer Vulnerabilität darf aber nicht einfach weggestrichen werden. Das Wegstreichen würde bedeuten, ein Level an Sicherheitsfähigkeit in der Sicherheitsbewertung unberücksichtigt zu lassen. Wenn die Ausprägungen von Protektion, Observation und Intervention komprimiert werden, dann ist eine Neudefinition der Bedeutung dieser Ausprägungsstufen notwendig. Die Neudefinition

[50] Eine Diskussion der Sinnhaftigkeit dieser Definition erfolgt im nachfolgenden Kapitel.

der Bedeutung umfasst zwei Dimensionen: Die erste Dimension bezieht sich auf die Deskriptoren der neuen Ausprägungsstufen. Zu beantworten ist, welche Sicherheitsfähigkeiten die neuen Stufen im Einzelnen umfassen. Durch die neuen Stufen soll ein vergleichbarer Umfang von Sicherheitsfähigkeiten wie bei den vorherigen Stufen gegeben. Umfasst die neue Protektionsstufe „1" z. B. eine sehr niedrige Schutzwirkung oder eine sehr niedrige bis niedrige oder sogar moderate Schutzwirkung? Für die Neudefinition der Skalen sind Experten zurate zu ziehen. Die zweite Dimension bezieht sich auf die Überführung der neuen Scores in quantitative Werte, die als Input für die quantitative ICM verwendet werden können (siehe dazu Kapitel 3.1). Damit die Harnser-Skala quantitativ konform zu objektiven Vulnerabilitätsniveaus gemacht werden kann, bedarf es zunächst der Festlegung von Mittelwerten und Standardabweichungen für die Scores von „1" bis „4". Auch hierfür ist Expertenwissen erforderlich.

Allgemein zeigen die vorherigen Ausführungen, dass die Anpassung von Skalenstufen wohl durchdacht werden muss. Eine beliebige Komprimierung oder Erweiterung von unterschiedlich groß dimensionierten Skalen ist u. U. nicht durchführbar oder zweckdienlich. Scores sind per se unsicherheitsbehaftet. Die Reduktion von Skalenstufen beispielsweise würde dazu beitragen, dass der Informationsgehalt, der hinter einem Score steht, größer wird. Alternativ kann allerdings die Harmonisierung der Vulnerabilitätsskalen beider Security-Domänen verfolgt werden. Zum Beispiel können für beide Vulnerabilitätsskalen mit derselben Anzahl an Kategorien definiert werden (siehe dazu weitere Ausführungen in Kapitel 3.3.3 und Kapitel 3.3.4). Darüber hinaus werden beim klassischen CVSS zur Bestimmung der Exploitability vier Parameter verwendet, AV, AC, PR und UI. In dem Barriere-basierten Ansatz, wie in Braband (2019) dargelegt, wird die organisationale Barriere als „Privileges Required (PR) or User Interaction (UI)" definiert (siehe Abbildung 39).



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

Abbildung 39: Verwerfung im Barriere-basierten CVSS-Ansatz.
Quelle: Eigene Abbildung in Anlehnung an Braband (2019).

PR und UI werden als eine Barriere im Modell beschrieben, jedoch wird mit PR und UI gerechnet, als wenn es zwei separate Barrieren sind. Insofern es sich aber um eine einzige Barriere handeln sollte, wäre es erforderlich, auch die Bewertungsgrößen PR und UI zu einer Bewertungsgröße zusammenzuführen; ansonsten läge eine logische Inkonsistenz zwischen dem Modell und der Bewertungsmetrik vor. Es ist zuallererst zu hinterfragen, inwieweit die Zusammenführung von UI und PR in einer Bewertungsgröße möglich ist. Zu prüfen ist, ob UI und PR gem. CVSS dasselbe meinen oder doch unterschiedliche Dinge beschreiben, welche so nicht vereinbar sind. Hierfür wird die Bedeutung der CVSS-Bewertungsparameter auf die physische Sicherheit übertragen: PR kann aus physischer Sicherheitsperspektive bedeuten, dass ein Angreifer z. B. die Rechte eines Geschäftsführers braucht oder die eines Mitarbeiters, um in ein bestimmtes Gebäude oder ein bestimmtes Zimmer zu gelangen. UI würde beschreiben, inwiefern ein Angreifer Unterstützung (von Mitarbeitern) bei der Durchführung seines Angriffs

benötigt. Das kann beispielsweise in der physischen Sicherheit ein Pförtner sein, der einem Angreifer den Computer-Raum aufschließt. Mit UI wird bewertet, welche Privilegien anderer ein Angreifer nutzen muss, um an sein Ziel zu kommen.

PR und UI beschreiben dieselbe Sache aus zwei Blickwinkeln: PR umfasst allgemein, welche Rechte ein Angreifer braucht, während mit UI bewertet wird, welche Hilfe er seitens anderer (in irgendeiner Form) berechtigter Personen benötigt, sodass ein Angriff durchgeführt werden kann. In Dürrwang et al. (2021) beispielsweise wird nicht näher spezifiziert, auf welche Art und Weise Privilegien erworben werden, sondern lediglich, welche Ausprägungsstufe an Privilegien erforderlich ist, um einen Angriff auszuführen. Dieser Ansatz kann auf die Zusammenführung von PR und UI zu einer Bewertungsgröße bzw. einer Barriere angewandt werden, indem definiert wird: Die neue Bewertungsgröße PR* besteht in Anlehnung an Dürrwang et al. (2021) z. B. aus den vier Ausprägungen „Execute", „Read", „Write" und „Full Control". Jede der Stufen ist eine Parameterausprägung ungleich „None". Wenn die Ausbeutbarkeit nach dem soeben vorgeschlagenen Ansatz bewertet wird, dann ergibt sich z. B. das folgende Bewertungsschema (siehe Tabelle 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

Tabelle 36: Modifikation II des CVSS-Scorings zur Anpassung der LoE-Kategorien.
Quelle: Eigene Tabelle in Anlehnung an Braband (2019).[51]

Generell ist zu hinterfragen, ob es sinnvoll ist, Barrieren in ihrer Grundfunktionalität in Form von AV bis UI aufzuspalten und hintereinander zu stellen, zumal ein objektiver Wirkmechanismus fehlt, um eine quantitative Analyse in der IT-Security zu ermöglichen. Der Grund dafür ist, dass AV bis UI Variablen sind, die auf einer anderen Ebene funktionieren als die Protektion, Observation und Intervention. AV bis UI sind als Konzepte viel abstrakter als die Mechanismen, die in der physischen Domäne betrachtet werden. AV bis UI umfassen im Allgemeinen mehr Parameter und Werte, die einen Beitrag leisten, als z. B. die Protektion, bei der es sich um einen einzigen, über die Zeit gemessenen Parameter handelt. Die Protektionswahrscheinlichkeit ist eine elementare Größe in der physischen Sicherheit, welche durch eine Verteilung über die Zeit dargestellt wird (Lichte et al., 2016). Ein AV ist zunächst eine Abbildung des gesamten Szenarios (bzw. Kontexts), welcher in allgemeinen Begriffen beschrieben wird. Dies ist ein größeres Konstrukt, hinter dem viel mehr und potenziell unsichere Informationen stehen, als für die Mechanismen der Protektion, der Observation und der Intervention typisch sind.

Trotz der Tatsache, dass die CVSS-Parameter viel mehr Informationen enthalten als die Bewertungsparameter aus der physischen Sicherheit, werden in der CVSS-Metrik lediglich diskrete Exploitability-Beiträge definiert. Diese werden zudem auf der Ebene der Risikobeschreibung multiplikativ verknüpft. Das setzt voraus, dass die CVSS-Parameter völlig unabhängig voneinander sind, also keinen Einfluss aufeinander haben. Mit dem Parameter AC beispielsweise werden die Bedingungen umfasst, die außerhalb der Kontrolle des Angreifers liegen müssen,

[51] Der Parameter UI in dieser Metrik fasst die beiden Bewertungsgrößen UI und PR von CVSS zusammen. Kursiv hervorgehoben sind metrische bzw. deskriptive Modifikationen markiert.

damit eine Schwachstelle ausgenutzt werden kann. Hierzu zählt die Sammlung von Informationen über das Angriffsziel (First.org, 2022). Zur Sammlung von Informationen gehört aber auch, in Erfahrung zu bringen, welchen Grad der Berechtigungen ein Angreifer vor einem Angriff besitzen muss, um eine Schwachstelle erfolgreich ausnutzen zu können (PR). Anderseits beinhaltet AC auch eine Sammlung von Informationen über das Erfordernis, ob ein anderer menschlicher Benutzer als der Angreifer an der erfolgreichen Kompromittierung der verwundbaren Komponente beteiligt sein muss (UI). Diesbezüglich wird in der CVSS-Spezifikation darauf hingewiesen: „Importantly, the assessment of this [attack complexity] metric excludes any requirements for user interaction in order to exploit the vulnerability" (First.org, 2022). Ein Teil von der AC kann auch sein, dass sich ein Angreifer darüber informieren muss, in welchen Kontexten es Schwachstellen gibt, die potenziell ausgebeutet werden könnten. Die Aufwandsabschätzung bzgl. der möglichen Ausbeutbarkeit einer Schwachstelle wird aber durch den Parameter AV beschrieben.

Insgesamt ist die Risikobeschreibung im CVSS zu hinterfragen. In der physischen Sicherheit wird die Gesamtvulnerabilität eines Systems V_{ges} über das Produkt der Vulnerabilität einer jeden Barriere a bis z bestimmt, d. h. $V_{ges} = V_a \cdot \ldots \cdot V_z$. Der Vulnerabilitätsbeitrag jeder Barriere setzt sich aus einem Zusammenspiel von Protektion, Observation und Intervention zusammen. In dem Barriere-basierten CVSS-Ansatz wird nicht die Gesamt-Exploitability E_{ges} über das Produkt der Exploitability an den einzelnen Barrieren i bis k bestimmt ($E_{ges} = E_i \cdot \ldots \cdot E_k$), sondern über das Produkt der Exploitability-Beiträge von AV bis UI. Weder AV noch AC, PR oder UI setzen sich aus einem Zusammenspiel von weiteren „Sub-Exploitability-Beiträgen" zusammen, wie das in der physischen Vulnerabilitätsbewertung der Fall ist. Ein Exploitability-Beitrag wird als Barriere interpretiert. Aus physischer Security-Modell-Sicht würde das bedeuten, z. B. Protektion als Barriere zu interpretieren.[52]

Wenn aber nun der Barriere-basierte CVSS-Ansatz derart aufgefasst wird, dass beispielsweise mit dem Scoring von AV die Exploitability an der Barriere AV bestimmt wird, dann wäre dies aus physischer Security-Perspektive so, also könnte ein Experte sofort die Vulnerabilität an dieser Barriere einstufen – ohne vorherige Zuhilfenahme einer Vulnerabilitätsmetrik für die Bewertung des Zusammenspiels von Protektion, Observation und Intervention. Aus physischer Security-Sicht ist eine direkte Bewertung der Vulnerabilität ohne eine Metrik schwerlich darstellbar. Deswegen kann die Behauptung aufgestellt werden, dass auch IT-Security-Experten nicht die Exploitability unmittelbar, d. h. ohne eine darunterliegende Exploitability-Metrik, bewerten können. Eine Interpretation der CVSS-Bewertungsparameter als Barrieren in Parallelschaltung ist nicht schlüssig, da die Bewertungsparameter nicht „parallel wirken". Jeder CVSS-Parameter betrachtet einen anderen Aspekt einer Schwachstelle. Sie ergänzen sich gegenseitig. Eine Parallelschaltung hat außerdem hat zur Folge, dass kein multiplikativer Zusammenhang mehr zwischen den Exploitability-Beiträgen dargestellt werden kann. Die Sinnhaftigkeit der Anwendung des Logarithmus bei einer Parallelschaltung von AV bis UI ist dann infrage zu stellen. Grundsätzlich kann jedoch auf analytischem Wege gezeigt werden, dass durch die Anwendung des Logarithmus Verwerfungen bei multiplikativen Scoring-Metriken reduziert werden können. Inwieweit der Barriere-basierte CVSS-Ansatz eine Verbesserung im Sinne einer genaueren Abbildung objektiver Exploitability-Niveaus mit sich bringt, kann mangels einer quantitativen (wirksamkeitsbasierten) IT-Security-Metrik, mit welcher die Sicherheitsfähigkeit von Maßnahmen zur Reduktion der Exploitability beurteilt werden könnte, nicht bestätigt werden.

[52] Die Interpretation von Protektion, Observation und Intervention als Barrieren ist der Ausgangspunkt für die Emulation der Überlegungen des Barriere-basierten CVSS in der physischen Sicherheitsbewertung (Termin et al., 2022).

3.3 Domänenübergreifende Bewertung

Im ersten Teil dieses Kapitels wird zunächst dargelegt, inwiefern Sicherheitslevels für die physische Sicherheit und die IT-Sicherheit definiert werden können. Es wird erläutert, wie cyberphysische Wechselwirkungen bewertet werden können, und wie die Schwere einer Wechselwirkung herangezogen werden kann, um die Sicherheitslevels in beiden Domänen aufeinander abzustimmen. Im zweiten Teil dieses Kapitels werden Maßnahmen und Annahmen zur Ermöglichung einer Angleichung von Metriken aus den Domänen Physical Security und IT-Security erarbeitet. Ausgangspunkt bilden die Risikofunktionen „Risiko = Vulnerabilität x Impact" für die physische Security bzw. „Risiko = Exploitability x Impact" für die IT-Security. Die Vulnerabilitätsbeiträge in der physischen Risikobewertung sollen über die Harnser-Metrik abgebildet werden, die Exploitability-Beiträge in der IT-Security durch das CVSS.

Für die Angleichung der Metriken aus beiden Domänen wird eine Normierung der Risikobeiträge vorgeschlagen, um die Skalenkategorien der Risikobeiträge anzugleichen. Die Dimensionierung der Risikobeiträge aus beiden Security-Domänen wird mittels Anwendung einer log-Transformation zueinander angepasst. Daraufhin wird beleuchtet, wie und unter welchen Voraussetzungen zueinander passende Sicherheitslevel aus der physischen Sicherheit und IT-Sicherheit definiert werden können. Für die physische Security wird die Harnser-Metrik herangezogen. Für die IT-Security wird die Barriere-basierte CVSS-Metrik gewählt. Möglichkeiten sowie Grenzen in der Angleichung von Metriken aus den Domänen Physical Security und IT Security sowie in der domänenübergreifenden Bewertung werden dargestellt.

3.3.1 Angleichung der Vulnerabilitätsbeschreibungen

Damit eine Angleichung und Zusammenführung der Domänen Physical Security und IT Security gelingen kann, ist eine vergleichbare Beschreibung der Vulnerabilität erforderlich. Zur Unterscheidung der Vulnerabilitätsbeschreibung in beiden Domänen wird für die IT-Vulnerabilität Exploitability („E") geschrieben und für die physische Vulnerabilität „V". Wird angenommen, dass es in der IT-Security i-Barrieren geben kann, dann kann die Exploitability an der i-ten Barriere mit Gl. (17) bestimmt werden:

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

Bei Vorliegen disjunkter Barrieren in Reihe (siehe Abbildung 40) und unter Annahme strenger Unabhängigkeit ist die Gesamt-Exploitability die Schnittmenge der Einzel-Exploitabilities. Die Gesamt-Exploitability kann somit als Produkt der Einzel-Exploitabilities ($E_A \ldots E_Z$) geschrieben werden (siehe Gl. (18)):

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

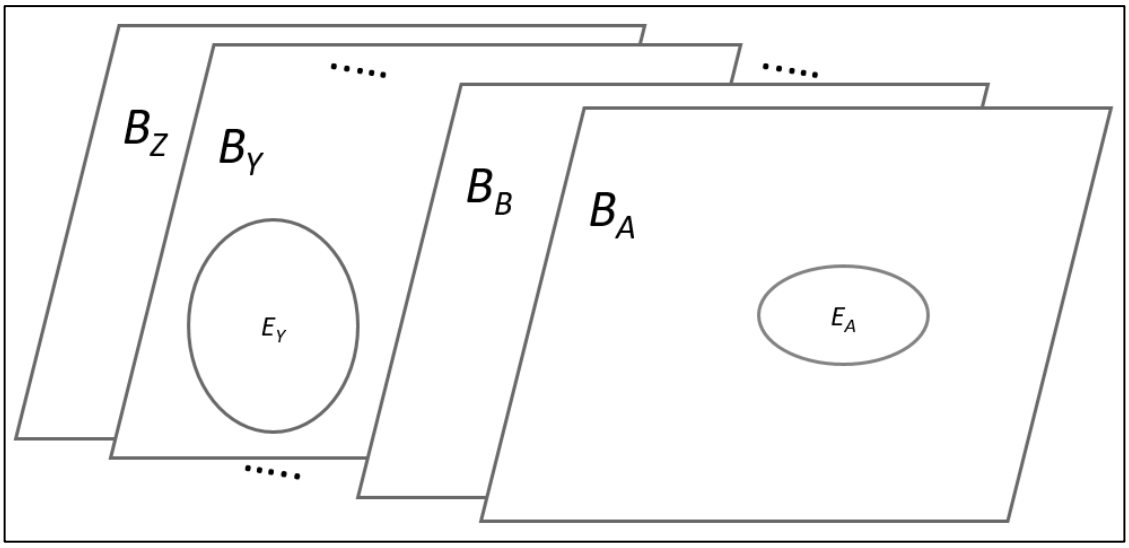


Abbildung 40: Reihenschaltung von disjunkten Barrieren in der IT-Security.
Quelle: Eigene Abbildung.

In den Barrieren $B_A \; bis \; B_Z$ aus Abbildung 40 kann es mehrere Schwachstellen geben (siehe beispielhaft Abbildung 41). Die einzelnen Schwachstellen einer Barriere leisten einen Exploitability-Beitrag zur Gesamt-Exploitability an dieser Barriere. Wenn $E_A = E_{a_k}$ disjunkte Ereignisse sind, dann können die Exploitabilities E_{a_k} an der Barriere B_A addiert werden. Mit vier angenommenen Schwachstellen in Abbildung 41 kann E_A durch Gl. (19) ausgedrückt werden:

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

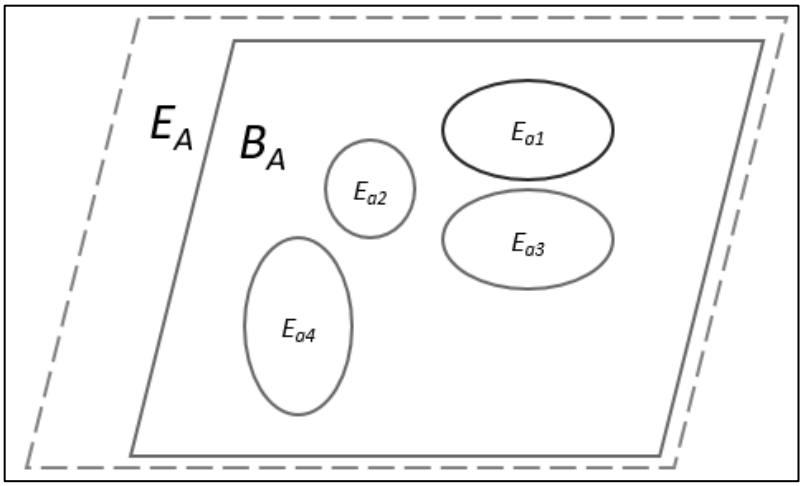


Abbildung 41: Eine IT-Barriere mit mehreren Schwachstellen.
Quelle: Eigene Abbildung.

Die Wahrscheinlichkeit für E_A ergibt sich mit Gl. (20):

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

Die Exploitability einer Schwachstelle kann nach CVSS durch vier unterschiedliche Aspekte beschrieben werden, den Attack Vector (AV), die Attack Complexity (AC), die Privileges Required

(PR) und die User Interaction (UI). Werden diese Aspekte als disjunkte Barrieren in Reihe aufgefasst, und wird für diesen Idealfall strenge Unabhängigkeit angenommen, dann kann beispielsweise für E_{a1} die Exploitability durch das Produkt aus AV bis UI geschrieben werden (siehe Gl. (21) und Abbildung 42). B_J bezeichnet hierbei die Barrieren AV bis UI.

$$E_{a1} = P(E(B_J)) = P(E(B_{AV})) \cap P(E(B_{AC})) \ldots \cap P(E(B_{UI})) = E_{AV} \cdot \ldots \cdot E_{UI} \quad (21)$$

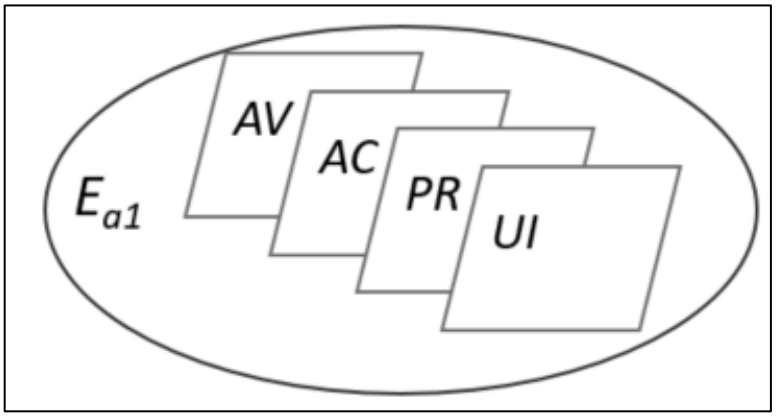


Abbildung 42: Eine Schwachstelle mit mehreren Barrieren.
Quelle: Eigene Abbildung.

Die Einzelbetrachtungen zusammengesetzt ergeben die Zusammenhänge in Abbildung 43.

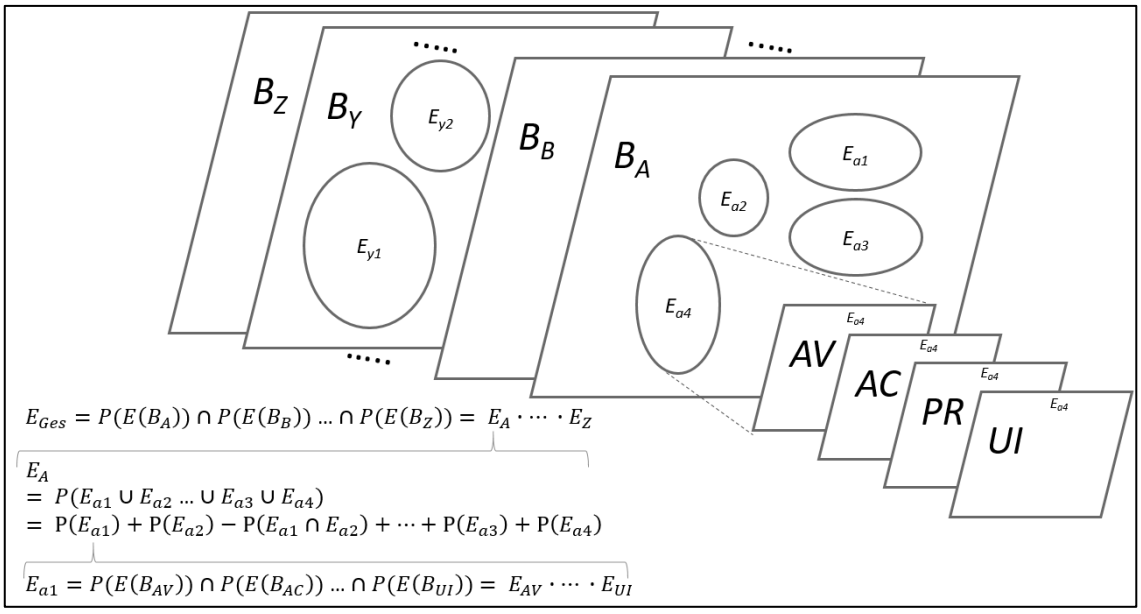


Abbildung 43: Reihenschaltung von mehreren (disjunkten) Barrieren mit mehreren Schwachstellen.
Quelle: Eigene Abbildung.

Die Berechnung der Exploitability für mehrere Schwachstellen einer IT-Barriere über das Aufsummieren der disjunkten Wahrscheinlichkeiten (siehe Gl. (20)) ist jedoch nicht richtig, wenn sich ein Angreifer für einen bestimmten Angriffspfad entscheidet. Die Ereignisse sind dann nicht unabhängig voneinander. Nun könnte angenommen werden, dass es mehrere Angreifer geben kann, welche gleichzeitig angreifen. In der physischen Security wird z. B. in Lichte et al. (2016) bei einem Szenario davon ausgegangen, dass sich ein Angreifer für einen Angriffspfad, also eine Kombination von Barrieren bis zum Asset, entscheidet. In der IT-Security jedoch kann

die Definition des Angriffspfades aus der physischen Sicherheitsperspektive durch die Dimension „Kombination von Schwachstellen“ erweitert werden. Ein IT-Angreifer wählt demzufolge nicht nur eine Kombination von Barrieren bis zu einem Asset aus, sondern entscheidet auch, welche konkreten Schwachstellen bei den gewählten Barrieren ausgebeutet werden sollen (siehe Abbildung 44). Das Prinzip des schwächsten Pfades, wie in Lichte et al. (2016) für die Vulnerabilitätsbewertung in der physischen Sicherheit beschrieben, kann in die IT-Security übertragen werden: Der schwächste IT-Angriffspfad ist die Barrieren-Schwachstellen-Kombination mit der höchsten Exploitability.

Besitzt eine Barriere B_A in einem fiktiven Beispiel zwei Schwachstellen mit E_{a1} und E_{a2}, so kann auch die Wahrscheinlichkeit für die Exploitability an dieser Barriere (E_A) für den Fall berechnet werden, dass die erste Schwachstelle oder die zweite Schwachstelle ausgebeutet wird (siehe Gl. (22)) (Lyu et al., 2020).

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

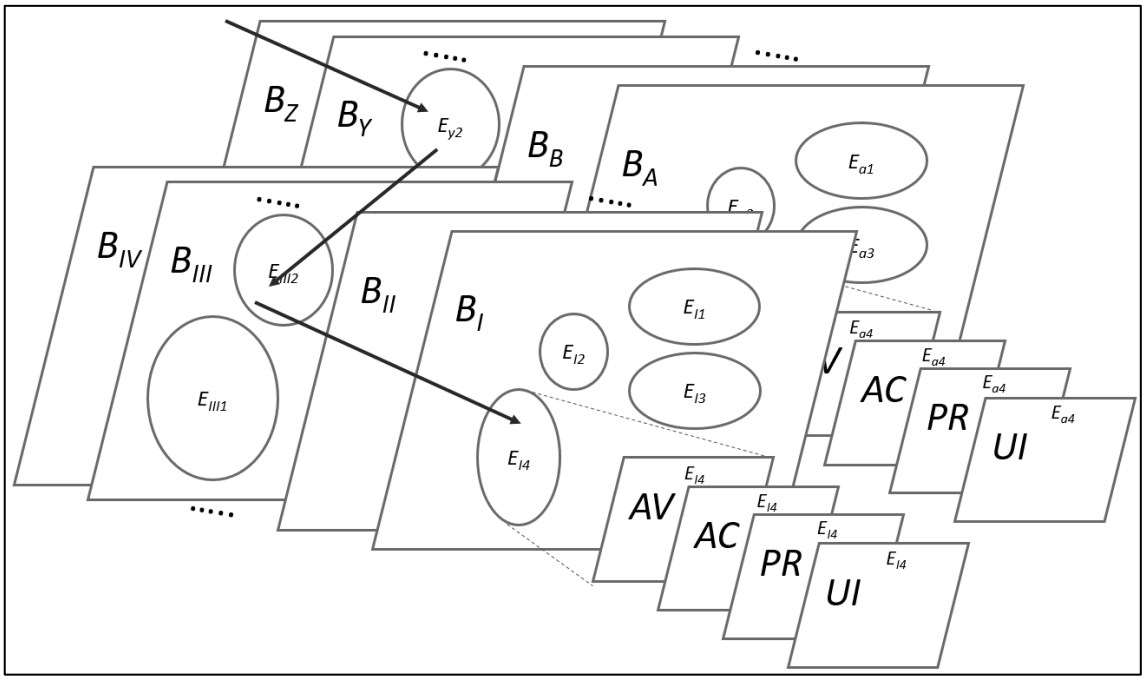


Abbildung 44: Angriffspfad in der IT-Security mit mehreren Barrieren und Schwachstellen.
Quelle: Eigene Abbildung.

In der physischen Sicherheitsbewertung, z. B. nach Lichte et al. (2016), wird angenommen, dass es in m disjunkte Barrieren geben kann. Die Vulnerabilität an der m-ten Barriere kann mit Gl. (23) bestimmt werden:

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

Bei Vorliegen disjunkter Barrieren in Reihe (siehe Abbildung 45) und unter Annahme strenger Unabhängigkeit ist die Gesamt-Vulnerabilität die Schnittmenge der Einzel-Vulnerabilitäten. Die Gesamt-Vulnerabilität kann somit als Produkt der Einzel-Vulnerabilitäten ($V_A \ldots V_Z$) geschrieben werden (siehe Gl. (24)):

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

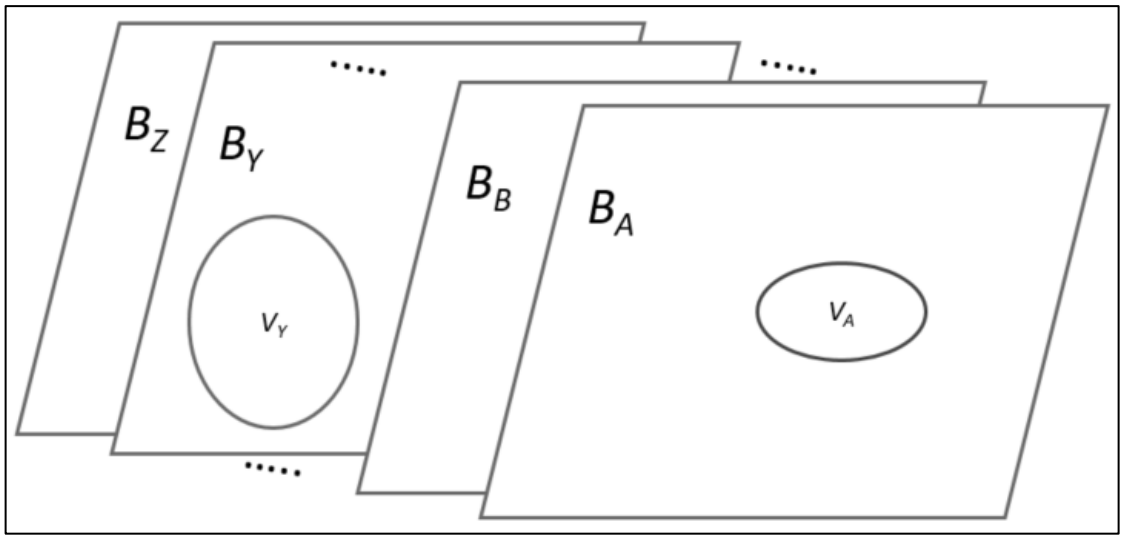


Abbildung 45: Reihenschaltung von disjunkten Barrieren in der physischen Security.
Quelle: Eigene Abbildung.[53]

Die physische Vulnerabilität an einer Barriere wird durch das Zusammenspiel von Protektion, Observation und Intervention bestimmt. Eine Möglichkeit, Vulnerabilität zu berechnen, ist beispielsweise die Anwendung der Vulnerabilitätsmetrik nach Lichte et al. (2016) (schematische Darstellung siehe Abbildung 46).

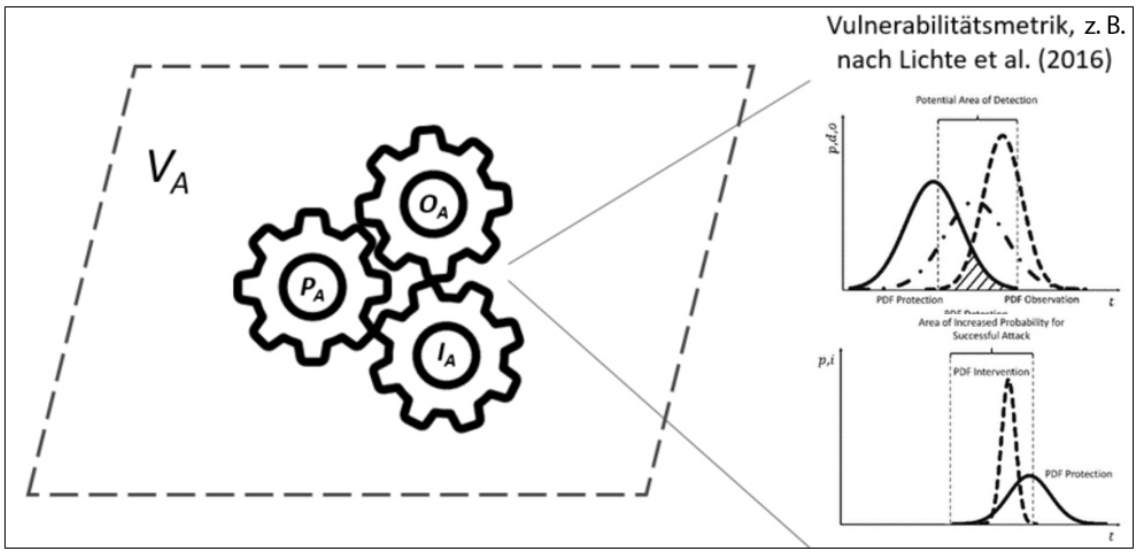


Abbildung 46: Physische Vulnerabilität an einer Barriere.
Quelle: Eigene Abbildung in Anlehnung an Lichte et al. (2017).

Das Pfadmodell in der physischen Sicherheitsbewertung ergibt sich damit zu Abbildung 47.

[53] Auf der rechten Seite wird die Vulnerabilitätsbewertung mittels der quantitativen Vulnerabilitätsmetrik (ICM) nach Lichte et al. (2016) angedeutet.

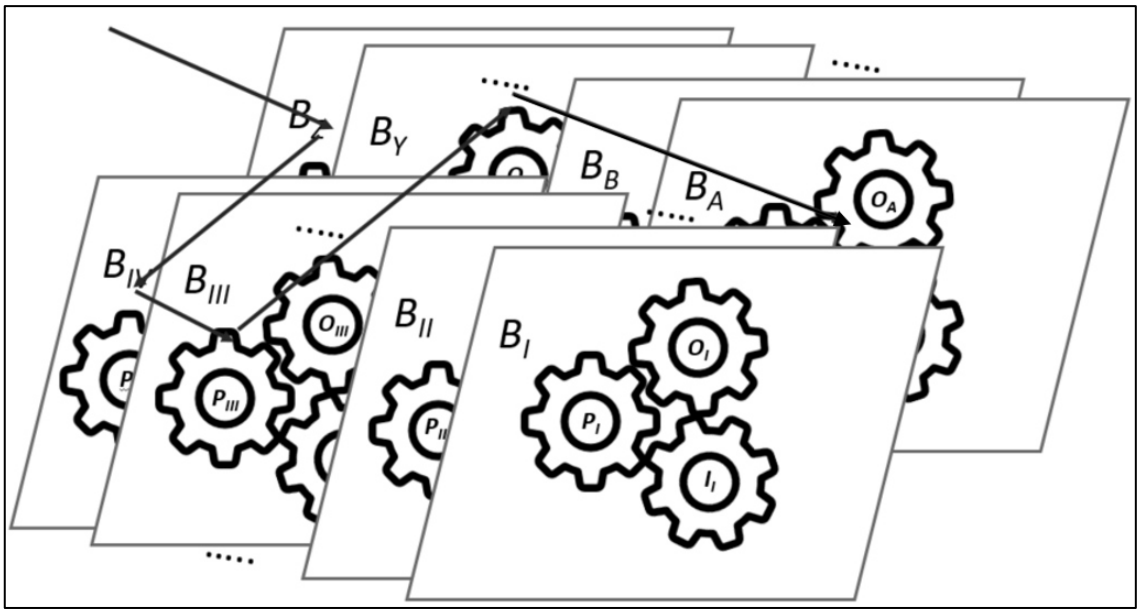


Abbildung 47: Pfadmodell in der physischen Sicherheit.
Quelle: Eigene Abbildung.

Obwohl es in der Art der Angriffspfade in der physischen Sicherheit und in der IT-Sicherheit Unterschiede gibt, teilen beide Domänen Gemeinsamkeiten in der Beschreibung von Angriffspfaden.

3.3.2 Angleichung der Bewertung von Auswirkungen

Um die Sicherheitsbewertungen aus der physischen Sicherheit und aus der IT-Sicherheit in einem weiteren Schritt anzupassen, muss zwar auf eine quantitative IT-Metrik mit objektivem Wirkmechanismus zur Beschreibung des Schutzeffekts von IT-Maßnahmen im Sinne einer Exploitability-Reduktion verzichtet werden. Es gibt jedoch Möglichkeiten, eine Angleichung vorzunehmen: Bei geeigneter Wahl der Stufen der Risikobeiträge (kompatible Skalen), so die aus Kapitel 3.2.1 resultierende Annahme, kann sich eine Metrik mit anderen Metriken zusammenführen lassen, welche ebenfalls reale Risiken abbilden. Die Wahl und Anpassung geeigneter Stufen der Risikobeiträge in der physischen Sicherheitsbewertung sowie in der IT-Sicherheitsbewertung werden nachfolgend erklärt. Ziel ist es, eine multiplikative Scoring-basierte Metrik für die physische Sicherheit und für die IT-Sicherheit aufzusetzen, welche

a) im Ergebnis quantitative Werte für das physische Risiko bzw. IT-Risiko liefert.
b) vergleichbare Skalen für die Risikobeiträge verwendet.

Risiko wird in der physischen Security als ein zusammengesetztes Ereignis betrachtet. Die Einzelbeiträge des physischen Risikos werden klassischerweise multiplikativ verknüpft, sodass sich ein physisches Risiko aus der Bedrohung B, der Vulnerabilität V und dem Impact I zusammensetzt. Durch die Annahmen aus Gl. (1) (siehe Kapitel 2.3) gilt in diesem Zusammenhang für das Risiko (siehe Gl. (25)):

$$R = \text{Vulnerability} \times \text{Impact} \tag{25}$$

Beeinflussen sich die Ereignisse V und I nicht gegenseitig, kann das physische Risiko als Multiplikation aus V und I geschrieben werden (siehe Gl. (26)):

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

In der physischen Security können Risiken auch durch Scoring-basierte Metriken beschrieben werden. Den Stufen der Einzelbeiträge werden Zahlen auf einer Bewertungsskala eingeordnet. Wenn V und I linear skaliert wären, ließen sich physische Risikobewerte berechnen, welche proportional zum wahren physischen Risiko sind (siehe Gl. (27)):

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

Wenn die Zusammenhänge zwischen den Zahlenwerten und Risikobeiträgen nichtlinear sind, kann es zu Verwerfungen kommen (siehe Kapitel 3.2.1): Eine auf Zahlenwerten beruhende physische Risikobewertung entspricht unterschiedlichen realen physischen Risikowerten.

Um die Risikobeschreibung aus der physischen Sicherheit ($R = V \cdot I$) und die Risikobeschreibung aus der IT-Sicherheit ($R = E \cdot I$) zusammenzubringen, werden zuallererst die Auswirkungsskalen aus beiden Security-Domänen harmonisiert (siehe auch die Ausführungen in Kapitel 3.3.4). Experten können in diesem Zusammenhang herangezogen werden, um Auswirkungsstufen mit monetären Verlustwerten zu definieren, in welchen sich sowohl physische Szenarien als auch IT-Szenarien wiederfinden lassen. Für beide Security-Domänen wird eine Skala z. B. mit vier Stufen (bzw. mit den Scores „1“ bis „4“) definiert. Sie können durch deskriptive Attribute ergänzt werden, welche die Auswirkungsstufe beschreiben (siehe hierzu Kapitel 3.3.4). Durch die Experten wird hinter jeden einzelnen Score ein monetärer Verlustwert geschrieben (siehe als Beispiel Tabelle 37). Jedes Stufen-Auswirkungs-Paar kann als Punkt interpretiert werden, z. B. $P1(1|10)$, $P2(2|100)$, usw. Diese Punkte sind durch eine mathematische Funktion darstellbar. Für die Auswirkungsstufen in Tabelle 37 kann für den Impact I der Zusammenhang $I = 10^i$ [Euro] für beide Security-Bewertungen angenommen werden.

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

Tabelle 37: Impact-Stufen und monetäre Verlustwerte für die physische Sicherheitsbewertung und IT-Sicherheitsbewertung.
Quelle: Eigene Tabelle.

Die Risikofunktion ergibt sich damit zu Gl. (28):

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

Wird in den ganz rechten Teil der Gleichung z. B. Score 1 eingesetzt, so resultiert das Ergebnis ($ln\ 10 \cdot 1 =$) 2.3. Eine Rücktransformation liefert für den Impact ($e^{2.3} =$) 10 (Euro). Eine Zusammenführung der Impact-Skalen ist gelungen. Scoring-basiert können wahre Impact-Einstufungen abgebildet werden. Nun stellt sich die Frage nach einer geeigneten Scoring-basierten Abbildung der Vulnerabilitätsbeiträge bzw. der Exploitability-Beiträge in einer multiplikativen Metrik der Form „R = V · I“ bzw. „R = E · I“. Eine Metrik ist gesucht, mittels welcher die Impacts ebenso die Vulnerabilität und Exploitability bzw. deren Beiträge gescort werden können.

3.3.3 Angleichung der Bewertung von Vulnerabilität

Nach der Harmonisierung der Auswirkungsskalen für beide Security-Domänen ist der Frage nachzugehen, wie Vulnerabilitätsstufen für V in der physischen Risikobeschreibung ($R = V \cdot I$) definiert werden können. Vulnerabilität wird in der physischen Sicherheit über das Zusammenspiel von Protektion, Observation und Intervention ermittelt. Eine Metrik, welche zur Bewertung von physischer Vulnerabilität verwendet werden kann, ist die Scoring-basierte

Harnser-Metrik. Scores sind per se nicht quantitativ, weswegen nicht mit ihnen gerechnet werden kann. Nichtsdestotrotz ermöglicht die Idee der Hinterlegung eines objektiven Wirkmechanismus in die zu scorenden Bewertungsparameter aus der physischen Sicherheit, dass vermutete Wahrscheinlichkeitsintervalle, welche hinter den Kategorien der Vulnerabilitätsskala vermutet werden, an objektive Vulnerabilitätsstufen angepasst werden können. Die Analyseergebnisse in Kapitel 3.1 legen am Beispiel der physischen Sicherheit objektiv dar, dass quantitative Ergebnisse trotz unterschiedlicher Skalenkategorien mittels eines Scorings gespiegelt werden können. Zu berücksichtigen ist, dass sich quantitativ errechnete Ergebnisse einer oder mehrerer ICM-Varianten innerhalb von vermuteten Wahrscheinlichkeitsintervallen wiederfinden lassen, welche hinter einer jeden Skalenkategorie stehen. Im Rahmen der Untersuchungen in dieser Arbeit werden insgesamt folgende Maßnahmen vorgeschlagen und validiert, welche Inkompatibilitäten zwischen der Harnser-Metrik und der ICM reduzieren:

1. Erweiterung der Skalenkategorien um vermutete Wahrscheinlichkeitsintervalle.
2. Anpassung der vermuteten Wahrscheinlichkeitsintervalle (und ggf. Skalenkategorien) an den Verlauf der ICM-Vulnerabilitätskurve.

Mithilfe der in dieser Arbeit vorgeschlagenen Harnser-Metrik können schlussfolgernd Bewertungen durchgeführt werden, deren Ergebnisse objektiven Vulnerabilitätseinstufungen zwischen 0 % (keine Vulnerabilität) und 100 % (maximal vulnerabel) entsprechen. Betrachtet wird dabei ein Referenzmodell mit einer Barriere und einem Asset. Die Vulnerabilitätsergebnisse der ICM 1werden in Abhängigkeit von der Größe der Harnser-Vulnerabilitätsergebnisse sortiert sowie anschließend innerhalb der Harnser-Plateaus der Größe nach angeordnet. Anschließend werden die Harnser-Plateaus der in diesem Falle vorliegenden dreizehngliedrigen Skala an die ICM 1-Vulnerabilitätswerte angepasst. An dieser Stelle ist zu fragen, wie einer Harnser-Skala aussehen kann, die wie die Impact-Skala aus Kapitel 3.3.2 aus vier Kategorien besteht und quantitativ konform zur ICM 1 ist. Zudem ist zu fragen, wie das Harnser-Scoring so aufgebaut werden kann, dass auf verfahrenstechnischer Ebene wie beim Barriere-basierten CVSS-Ansatz mit log-Scores operiert wird. In der Harnser-Metrik werden bereits willkürliche Werte addiert. Ob diese Werte aus einer Logarithmierung entstanden sind oder nicht, hat keine entscheidende Rolle bezüglich der Konformität der Harnser-Vulnerabilitätswerte zu den objektiven Vulnerabilitätswerten einer ICM-Variante. Die log-Transformation kann in einer ersten Überlegung direkt auf die Harnser-Scores von „1“ bis „5“ angewandt werden (siehe Gl. (29)):

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

Dies würde jedoch dazu führen, dass dem niedrigsten Harnser-Score der höchste log-Wert und dem höchsten Score der niedrigste log-Wert zugeordnet wird (siehe Tabelle 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

Tabelle 38: log-Transformierte Harnser-Scores.
Quelle: Eigene Tabelle.[54]

[54] Reihenfolge der log-Scores ist invers zu den Harnser-Scores. Auch hier gilt die Rundungsregel: Ist die erste Dezimalstelle der Ziffer eine 0, 1, 2, 3 oder 4, dann wird abgerundet. Ist die erste Dezimalstelle der Ziffer eine 5, 6, 7, 8 oder 9, dann wird aufgerundet.

Bei dem CVSS-Ansatz, wie in Braband (2019) vorgeschlagen, bedeutet ein niedriger log-Wert, dass es sich um eine Ausprägung handelt, die einen großen negativen Einfluss auf die Exploitability hat, z. B. „Network; numerical Value = 0.85; log Score = „0"". Der Logik folgend würde das übertragen auf die physische Sicherheit bedeuten, dass der Harnser-Score „5" die schlechteste Konfiguration darstellt. Gemäß vorheriger Definition (Score „1" := niedrig; Score „5" := hoch) ist das aber nicht der Fall. Score „5" bedeutet eine starke Ausprägung. Je ausgeprägter ein Beitrag zur Vulnerabilität, desto allgemein positiver der Effekt auf die Vulnerabilitätsreduktion. Darüber hinaus gibt es ein weiteres Problem: Werden die log-Scores gerundet, sodass ganzzahlige log-Scores entstehen, dann sind die Harnser-Scores "2", "3", "4" und „5" nicht mehr klar voneinander unterscheidbar, weil sie demselben logarithmischen Wert (= „1") zugeordnet werden würden. Die Scores sollen jedoch klar unterscheidbar sein, sodass eine Erhöhung eines Scores eine Erhöhung der Sicherheitsfunktionalität bedeutet.

Aus der Sicht eines Anwenders des Scorings kann die Definition der log-Werte wie in Tabelle 38 zu Verwirrungen führen. Intuitiv würde erwartet werden, dass ein niedriger Harnser-Score einem niedrigen log-Wert und ein hoher Harnser-Score einem hohen log-Wert zugeordnet wird. Um dieser Herausforderung gerecht zu werden, werden für jeden Harnser-Score – ähnlich wie beim CVSS – (willkürliche) numerische Werte zwischen „0" und „1" definiert: Der kleinste Harnser-Score erhält den größten numerischen Wert zugewiesen. Der größte Harnser-Score erhält den kleinsten numerischen Wert zugeordnet. Die numerischen Werte werden „äquidistant" festgelegt. Wie aus Tabelle 39 ersichtlich ist, haben niedrige Harnser-Scores niedrige numerische Werte und hohe Harnser-Scores hohe numerische Werte. Das ist notwendig, um nach der Logarithmierung Scores zu erhalten, die wie die Harnser-Scores in aufsteigender Reihenfolge angeordnet sind. Die Anwendung des Logarithmus auf die Zahlenwerte der Harnser-Scores zur Basis 0.6, wie in Braband (2019) durchgeführt, ergibt die Zuordnung in Tabelle 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

Tabelle 39: Harnser-Score-Levels mit dazugehörigen numerischen Werten.
Quelle: Eigene Tabelle in Anlehnung an Harnser (2010). [55]

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

Tabelle 40: Bildung von log-Scores aus Harnser-Scores.
Quelle: Eigene Tabelle.

[55] P := Protektion, O := Observation und I := Intervention. Die Umwandlung von deskriptiven Stufen in numerische Werte ähnelt dem Prinzip des Common Vulnerability Scoring Systems (CVSS) (First.org, 2022): Bewertungen, die schlechter sind, werden hohen Zahlenwerten zugeordnet, während Bewertungen, die besser sind, niedrigen Zahlenwerten zugeordnet werden. Obwohl die Bewertungsparameter in der physischen Sicherheit auf einer viel konkreteren Ebene liegen als die Bedrohungsszenario-beschreibenden Parameter im CVSS, könnten sie hier auf die gleiche Weise substituiert werden.

Zusammenfassend werden in dieser Harnser-Scoring-Variante die Scores von Protektion (P), Observation (O) und Intervention (I) logarithmiert, jeweils zwischen „0“ und „5“ gescort sowie addiert. So ergibt sich – analog zur Likelihood of Exploitablity (LoE) im Barriere-basierten CVSS-Ansatz – ein Likelihood of Vulnerability (LoV) Score. Der LoV kann mit Gl. (30) bestimmt werden. Im Ergebnis ist ein Ergebnisraum von „0“ bis „15“ möglich.

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

Eine viergliedrige Harnser-Skala kann mittels des in Kapitel 3.1 eingeführten Ansatzes derart aufgebaut werden, dass alle Vulnerabilitätswerte einer ICM-Variante innerhalb der Vulnerabilitätsplateaus des Scorings liegen. In Tabelle 41 ist eine beispielhafte Einteilung einer solchen viergliedrigen Harnser-Skala zu sehen. Abbildung 48 zeigt, dass alle ICM 1-Vulnerabilitätswerte innerhalb der Plateaus liegen.

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

Tabelle 41: Viergliedrige Harnser log-Skala angepasst an ICM 1.
Quelle: Eigene Tabelle.

Die Wahrscheinlichkeitsintervalle, welche hinter den vier Skalenkategorien stehen, umfassen eine größere Range an ICM 1-Werten, als dies bei der dreizehngliedrigen Skala der Fall ist. Vulnerabilitätswerte der ICM 1 können auf den Intervallgrenzen eines Plateaus oder dazwischenliegen. Bei Vorliegen der Skalenkategorie „Low“ wird beispielsweise eine hohe Range an vermuteten Werten für die Vulnerabilität vermutet. Die Differenz zwischen dem obersten und untersten Wahrscheinlichkeitswert dieser Kategorie liegt bei über 60 %. Insofern unter Annahme eines Worst Cases beim Harnser-Scoring die Kategorie „Low“ resultiert und die „obere Grenze“ des dazugehörigen Wahrscheinlichkeitsintervalls für die Vulnerabilität gewählt wird, könnte der wahre Vulnerabilitätswert (von ICM 1) bei 20 % liegen. Folglich ist der Sicherheitsaufschlag in diesem hierbei groß. Mit Blick auf die Wirtschaftlichkeit ist der Einsatz einer Bewertungsskala für die physische Vulnerabilität mit dreizehn Kategorien sinnvoller als mit einer Bewertungsskala mit vier Kategorien.

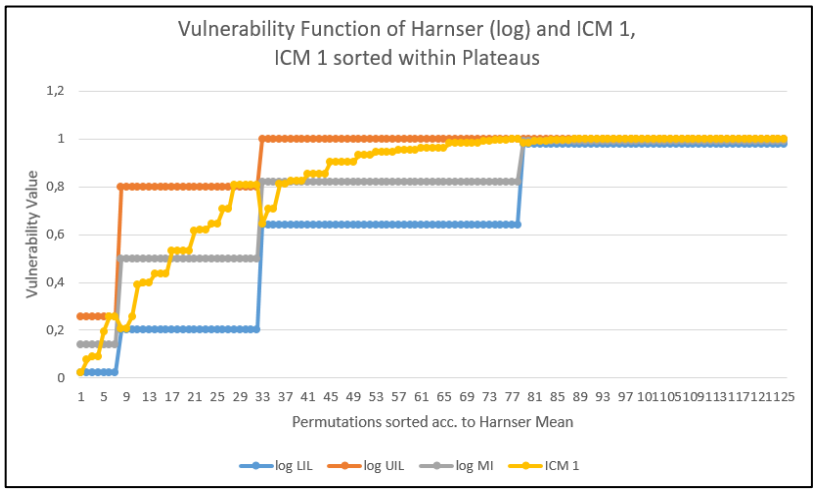


Abbildung 48: Plot der Vulnerabilitätswerte (Harnser log) und ICM 1.
Quelle: Eigene Abbildung.

Jede Kategorie der viergliedrigen Harnser-Skala kann einem Vulnerabilitäts-Score für die multiplikative Scoring-Metrik zugeordnet werden. Hinter jeder dieser Stufen stehen quantitative Wahrscheinlichkeitswerte für die Vulnerabilität (siehe Tabelle 42 dritte und vierte Spalte).

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

Tabelle 42: ICM 1-Vulnerabilitätswerte auf einer vierstufigen Skala.
Quelle: Eigene Tabelle.[56]

Auf Basis der dritten und vierten Spalte in Tabelle 42 ergeben sich folgende Zusammenhänge (siehe Abbildung 49):

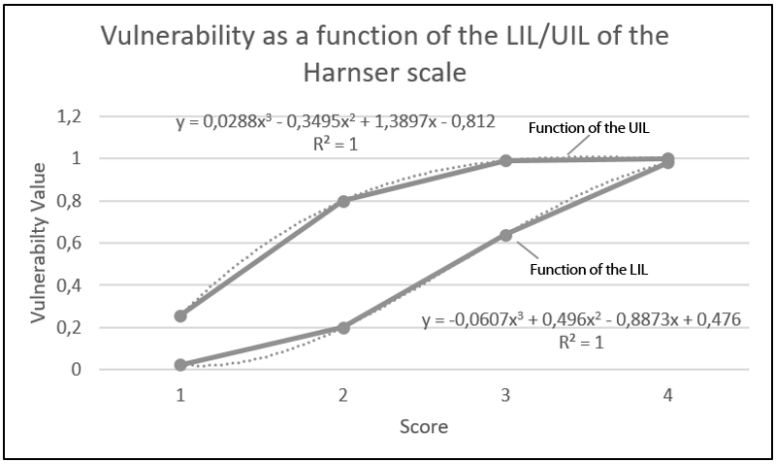


Abbildung 49: Vulnerabilitätsfunktionen nach den Intervallgrenzen der vierteiligen Harnser-Skalenkategorien inkl. Regressionsfunktion.
Quelle: Eigene Abbildung.

Die Vulnerabilitätskurven (LIL und UIL) können jeweils durch eine Polynomfunktion dritten Grades bestimmt werden (siehe Gl. (31)):

$$V_{LIL} = -0.0607v_{LIL}^3 + 0.4965v_{LIL}^2 - 0.8873\, v_{UIL} + 0.476$$
$$V_{UIL} = 0.0338v_{UIL}^3 - 0.3845v_{UIL}^2 + 1.4597\, v_{UIL} - 0.852 \quad (31)$$

Für den Bewertungsparameter Impact ($I = 10^i$) der Risikofunktion (R = V · I) wird hier die Basis 10 gewählt, und für die Vulnerabilitätsfunktionen aus Gl. (31) jeweils die Basis 0.6. Das physische Risiko ergibt sich zu Gl. (32):

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

Physische Vulnerabilität wird dem skizzierten Ansatz zufolge mittels folgender Schritte ermittelt:

1. Experten scoren Protektion, Observation und Intervention.
2. De Score-Summe wird auf einer viergliedrigen Harnser-Skala, die quantitativ konform zu einer ICM-Variante ist, in eine Kategorie einsortiert.

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

3. Jeder Skalenkategorie ist ein Vulnerabilitäts-Score (für die multiplikative Scoring-Metrik) zugeordnet. Liegt die Vulnerabilität z. B. bei „High“, so wird der Vulnerabilitäts-Score „4“ gewählt.
4. Der Vulnerabilitäts-Score wird als Input für den Vulnerabilitätsbeitrag in Gl. (32) eingespeist.
5. Experten scoren das Schadensausmaß (Score „1“ bis „4“).
6. Der Impact-Score wird als Input für den Impact-Beitrag in Gl. (32) eingespeist.
7. Das Risiko wird einmal für die Fälle LIL und UIL mit Gl. (32) berechnet.

Für die Bewertung der IT-Vulnerabilität kann Gl. (8) herangezogen werden. Das Referenzmodell besteht aus einer Barriere, einer Schwachstelle und einem Asset. Für die Bewertung der physischen Vulnerabilität wird Gl. (32) für die Risikobewertung am Referenzmodell einer Barriere und einem Asset herangezogen. Hieraus ergeben sich folgende Risikobeschreibungen (siehe Gl. (33)):[57]

IT-Risiko:

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

Physisches Risiko:

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

Angenommen, für den Barriere-basierten CVSS-Ansatz aus Kapitel 3.2.2 ist eine viergliedrige Exploitability-Skala definierbar, deren Kategorien durch Rücktransformation der log-Score-Summen aus AV bis UI objektiven Exploitability-Niveaus zugeordnet werden können (siehe beispielhaft Tabelle 43).

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

Tabelle 43: LoE-Skala mit vermuteten Wahrscheinlichkeitsintervallen.
Quelle: Eigene Tabelle.[58]

Wenn die Zuordnungen in Tabelle 43 angenommen werden, können für die Exploitability in die IT-Risikobeschreibung ($R = E \cdot I$) ebenfalls vier Stufen definiert werden (siehe Tabelle 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

Tabelle 44: „Quantitative“ Exploitability-Werte auf einer vierstufigen Skala.
Quelle: Eigene Tabelle.[59]

[57] Für die IT-Security wird angenommen: eine Barriere mit einer Schwachstelle und ein Asset. Für die physische Sicherheit wird angenommen: eine Barriere und ein Asset.
[58] Die Intervallgrenzen werden wie folgt bestimmt:
$e_{LIL} = e^{\ln(0.6) \cdot LoE\ Score\ min}$ bzw. $e_{UIL} = e^{\ln(0.6) \cdot LoE\ Score\ max}$.
[59] UIL := Upper Interval Limit. LIL := Lower Interval Limit.

Für die Exploitability ergeben auf Basis der dritten und vierten Spalte in Tabelle 44 folgende Zusammenhänge (siehe Abbildung 50):

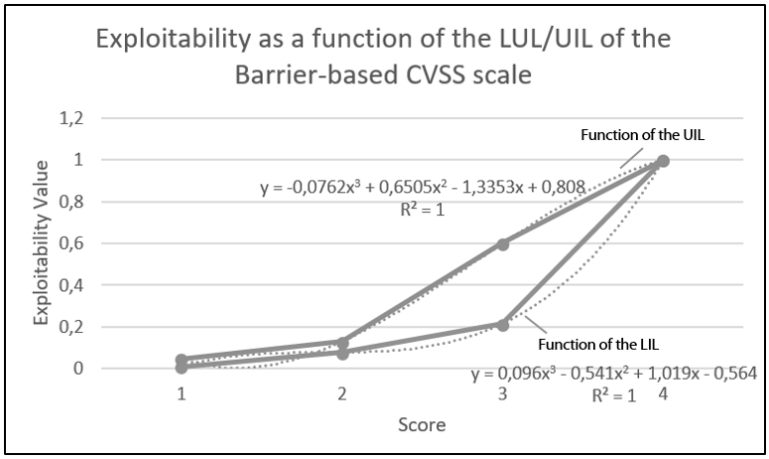


Abbildung 50: Exploitability-Funktionen nach den Intervallgrenzen der vierteiligen CVSS-Skalenkategorien inkl. Regressionsfunktion.
Quelle: Eigene Abbildung.

Die Exploitability-Kurven können jeweils durch eine Polynomfunktion dritten Grades bestimmt werden (siehe Gl. (34)):

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

Für den Bewertungsparameter Impact ($I = 10^i$) der Risikofunktion (R = E · I) wird hier die Basis 10 gewählt, und für die Exploitability-Funktionen die Basis 0.6. Für das IT-Risiko ergeben sich die Formeln für das Risiko in Gl. (35):

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

Exploitability wird dem skizzierten Ansatz zufolge mittels folgender Schritte ermittelt:

1. Experten scoren die CVSS-Bewertungsparameter AV, AC, PR und UI.
2. De Score-Summe wird auf einer viergliedrigen Skala, wie sie in Tabelle 43 angenommen wird, in eine Kategorie einsortiert.
3. Jeder Skalenkategorie ist ein Exploitability-Score (für die multiplikative Scoring-Metrik) zugeordnet. Liegt die Exploitability z. B. bei „Very Low", so wird der Exploitability-Score „1" gewählt.
4. Der Exploitability-Score wird als Input für den Exploitability-Beitrag in Gl. (35) eingespeist.
5. Experten scoren das Schadensausmaß (Score „1" bis „4").
6. Der Impact-Score wird als Input für den Impact-Beitrag in Gl. (35) eingespeist.
7. Das Risiko wird einmal für die Fälle LIL und UIL mit Gl. (35) berechnet.

Zu beachten ist die strenge Annahme, dass in die mathematischen Funktionen der Risikoeiträge nur die in den Skalen definierten Scores (hier: Score „1", „2", „3" und „4") eingesetzt werden. Sowohl die physische Risikobeschreibung als auch die IT-Risikobeschreibung können durch die vorgestellten Möglichkeiten zueinander angepasst werden (siehe Gl. (33) und Gl. (35)). Bei der Angleichung beider Security-Metriken kann grundsätzlich überlegt werden, die Risikobeiträge zur gleichen Basis zu logarithmieren, z. B. zur Basis zehn. In Kapitel 3.2.2 wird in Gl. (11) und Gl. (12) gezeigt, dass die Basis, zu der logarithmiert wird, keinen Einfluss auf die Berechnung wahrer Risikowerte hat. Zu berücksichtigen ist jedoch grundsätzlich, dass die

Wahl der Basis einen Einfluss auf die Skalierung der Daten hat: Sehr große Werte werden durch die log-Transformation verkleinert, und sehr kleine Werte werden vergrößert. Folglich kann die Wahl einer bestimmten Basis die Interpretation der transformierten Daten beeinflussen. Zur Basis zehn transformierte Daten können aufgrund der zugrunde gelegten Zehnerpotenz leichter interpretiert werden als z. B. zur Basis 0.6 transformierte Daten.

Die Anwendung des log-Transformationsansatzes kann nachweislich dazu beitragen, Metrik-inhärente Verwerfungen bei Scoring-basierten Bewertungssystemen zu reduzieren. Gleichzeitig können die Metriken aus der physischen Sicherheitsbewertung und aus der IT-Sicherheitsbewertung über eine Kompatibilität der Skalen der Risikobeiträge zusammengeführt werden. Folgende Voraussetzungen sind für eine Zusammenführung zu erfüllen:

- Mit den Metriken aus beiden Security-Domänen wird dasselbe bewertet, z. B. Risiko über eine Verknüpfung von Bedrohung (Annahme = 100 %), Vulnerabilität und Auswirkungen.
- Wahre Risikobeiträge müssen bekannt sein.
- Die Skalen der Risikobeiträge werden hinsichtlich der Stufeneinteilung gleich aufgebaut, insofern möglich, z. B. vier Stufen pro Risikobeitrag.
- Insofern ein multiplikativer Zusammenhang vermutet wird (Disjunktheit zwischen den Risikobeiträgen und strenge Unabhängigkeit angenommen): Die Basis, zu welcher die Risikobeiträge in beiden Domänen logarithmiert werden, werden jeweils gleich gewählt. Das kann z. B. für die Auswirkungen 10 und für die Vulnerabilität 0.6 sein, wie an den Beispielen in dieser Arbeit demonstriert wird. Es ist jedoch auch allgemein möglich, dieselbe Basis für die log-Transformation alle Risikobeiträge vorzusehen.
- Der epistemische Bedrohungsanteil wird durch die Annahme eines Angriffsfalls (Bedrohung = 100 %) aus der Risikobetrachtung ausgeklammert.

3.3.4 Bestimmung von Sicherheitslevels

In der Funktionalen Sicherheit werden qualitative Risikoanalysen zur Bestimmung des erforderlichen Automotive Safety Integrity Levels (ASIL) verwendet (Krisper, 2021) (siehe z. B. ISO 26262-3:2018, S. 19-26). Im Rahmen der IT-Security kommen ebenso qualitative Risikoanalysen zur Bestimmung der Cybersecurity Assurance Level (CAL) zum Einsatz (siehe z. B. ISO/SAE 21434, S. 59). In der IT-Security werden einerseits Bedrohungsszenarien (beschrieben durch den Attack Vector) und andererseits Impact-Anteile miteinander auf einer Tabelle kombiniert, um den CAL zu bestimmen (siehe Tabelle 45). Mit dem CAL von „1“ bis „4“ verbunden sind Anforderungen an die Entwicklung (siehe Tabelle 46). „---“ bedeutet, dass es nicht erforderlich ist, weitere Maßnahmen zur Risikominderung zu ergreifen, die über das akzeptierte Qualitätssystem innerhalb des Unternehmens hinausgehen.[60] In der ISO/SAE 21434 wird im Falle „---“ vorgeschlagen, das IT-System oder die Komponente nach dem V-Modell zu entwickeln (ISO/SAE, 2021b, S. 15).

[60] Nach der Risikobewertung können Risk Treatment Decisions (accept, remove, sharing, reduction) durchgeführt werden. Die Option „Reduction“ verfolgt das Ziel, den CAL zu reduzieren.

		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.

Tabelle 45: Bestimmung des CAL nach ISO/SAE 21434.
Quelle: ISO/SAE (2021b, S. 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

Tabelle 46: Cybersecurity-Maßnahmen korrespondierend zu den CAL nach ISO/SAE 21434.
Quelle: ISO/SAE (2021b, S. 60).

Der CAL aus der ISO/SAE 21434 ist vergleichbar mit dem theoretischen Sicherheitsprofil nach Schwerdtfeger, das Anforderungen in Form von zu beantwortenden Leitfragen an den Prüfer stellt (2018, S. 53-54), oder mit den Evaluation Assurance Levels (EAL) „1" bis „7" nach den Common Criteria (CC, 2021). Ein hoher EAL bedeutet, dass die behauptete Sicherheitsgarantie des betrachteten Systems umfassender überprüft wird als bei einem niedrigeren EAL. Dasselbe Prinzip liegt dem CAL zugrunde, das sich aus einem Impact-/Attack-Vector-Paar ergibt. Der Attack Vector ist Teil des Attack-Feasibility-Ratings nach ISO/SAE 21434 (ISO/SAE, 2021b, S. 76-77) und besteht aus den Ausprägungen „Physical", „Local", „Adjacent" und „Network" gem. CVSS (ISO/SAE, 2021b, S. 59). Die CAL-Kategorisierung kann in einer ersten Idee auf die physische Security übertragen werden.[61] Eine Übertragung würde aber zu Einschränkungen in der PAL-Kategorisierung führen, weil „Local", „Adjacent" und „Network" IT-Bedrohungsvektoren sind, die in der physischen Domäne nicht betrachtet werden. Alle Kombinationen, die diese drei Attack-Vector-Attribute enthalten, sind in der physischen Sicherheit nicht definiert. Es ist hier nur die Spalte „Physical" besetzt (siehe kursiv hervorgehobene Markierung in Tabelle 47). Wenn dem Schema zur Verknüpfung von Attack Vector und Impact aus ISO/SAE 21434 gefolgt wird, dann sind nur PAL „1" und PAL „2" definiert. PAL „3" und PAL „4" bleiben undefiniert.

[61] In der ISO/SAE 21434 ist der PAL nicht definiert.

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	**---**	---	---	---

Tabelle 47: Einschränkungen beim Mapping von CAL zu PAL.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 59).[62]

Das Mapping von CAL zu PAL könnte wie folgt modifiziert werden, um PAL „1" bis PAL „4" zu erhalten: Dem Attack-Vector-/Impact-Paar „Physical-Severe" wird der höchste PAL zugewiesen. Das Attack-Vector-/Impact-Paar „Physical-Negligible" wird dagegen der geringste PAL zugeordnet (siehe Tabelle 48). In diesem Falle zeigt sich, dass CAL „1" zwei unterschiedlichen PAL („2" und „3") zugeordnet wird (siehe rote Markierung in der Tabelle 48). Die Sicherheitsstufen sollten jedoch paarweise eindeutig unterscheidbar sein. Das bedeutet, dass ein CAL (z. B.: „1") auch nur einem PAL, z. B. also nur „1" und nicht „1" und „2", entspricht.

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

Tabelle 48: Modifikation des Mappings von CAL zu PAL.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 59).[63]

In diesem Zusammenhang ist es zudem erforderlich, zu definieren, was konkret hinter den Impact-Kategorien steht. Aus physischer Sicht werden Worst-Case-Szenarien bewertet. Das kann im Kontext MAS der erfolgreiche Diebstahl eines Fahrzeugs sein. Gemäß dieser Annahme würde jeder physische Angriff als „Severe" bzw. PAL „4" klassifiziert werden. Aus Sicht eines Systembetreibers, der mehrere Flotten besitzt und über einen Mobile-Access-Service betreibt, wäre aber der rein finanzielle Verlust eines Fahrzeugs im Gegensatz zum Verlust einer ganzen Flotte geringer (Reputationsschäden ausgeschlossen). IT-Angriffe können demnach anders skalieren als physische Angriffe.[64] Wenn nun ein Betreiber definiert, dass die Impact-Kategorien so zu verstehen sind, dass „Severe = alle Flottenkunden bzw. Fahrzeuge betroffen, Major = alle Flotten bzw. Fahrzeuge eines Kunden betroffen, Moderate = Flottenfahrzeuge einer Flotte eines Kunden betroffen, Negligible = ein Fahrzeug betroffen", dann wäre jeder erfolgreiche physische Angriff gem. obiger Tabelle als PAL „1" festgelegt.

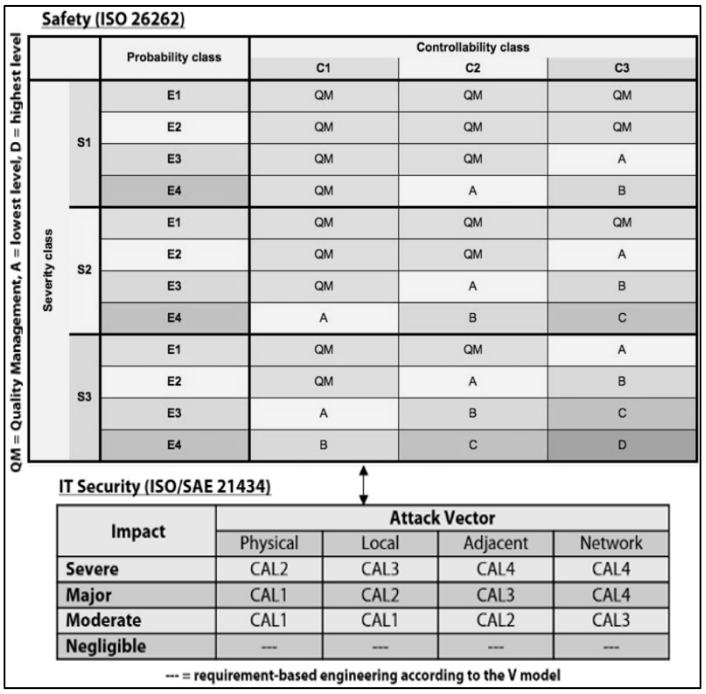
Dabei wird davon ausgegangen, dass physische Angriffe nur lokale Auswirkungen haben, d. h. es kann nur ein einziges Fahrzeug gestohlen werden. Ein physischer Diebstahl wird durch einen vorangegangenen Diebstahl nicht begünstigt. Für die Produktentwicklung könnte dies

[62] Die hellgraue Markierung zeigt an, dass diese Spalten für die Herleitung der physischen Security-Level nicht herangezogen werden können. Die grüne Markierung zeigt die zulässigen Zuordnungen für die Physical Security an.

[63] In grauer Farbe ist kursiv hervorgehoben, dass ein CAL („1)" zu zwei unterschiedlichen PAL („2" und „3") zugeordnet wird.

[64] Lokale, physische Angriffe können ebenfalls ähnliche Auswirkungen haben. Wenn beispielsweise Versorgungsknoten in Energieversorgungssystemen betroffen sind, dann bleibt die Wirkung nicht lokal (Lichte et al., 2020b). Ein weiteres Beispiel können Drohnenangriffe sein. Sie können aus beliebiger Entfernung durchgeführt werden, aber ein Angreifer muss trotzdem physisch zu der Anlage gelangen (Schneider et al., 2021).

allgemein in minimale Anforderungen an die Entwicklung korrespondieren. Das wiederum würde zur Minimalauslegung des physischen Vertreters des Mobile Access Produkts und damit potenziell zu einer Steigerung der Attraktivität für einen Angreifer führen. Das wäre nicht schlimm, wenn der Impact tatsächlich gering ist. Wenn aber beispielsweise ein Hauptschlüssel gestohlen werden kann und der erwartete Impact größer ist, dann könnte es in einem möglichen Szenario zu Wechselwirkungen zwischen IT-Sicherheit und physischer Sicherheit kommen. Die Anforderungen an die Gestaltung der physischen Barrieren müssen dann sorgfältig überdacht werden. Die vorherigen Erklärungen legen Wichtigkeit nahe, eine Auswirkungsskala für beide Domänen einheitlich aufzubauen. Bei der Bestimmung eines ASIL nach ISO 26262 werden – nicht so wie in der ISO/SAE 21434 – die Größen „Severity", „Probability Class" („Frequency") und „Controllability" miteinander in einer Matrix verknüpft (siehe Abbildung 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

Abbildung 51: Vergleich von ASIL und CAL.
Quelle: Embitel.com (2018) (oben); eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 59) (unten).

In der Security könnte die Bewertungsgröße „Frequency" durch den Bedrohungsanteil beschrieben werden. Dieser ist jedoch selbst mithilfe von Experten schwerlich abzuschätzen, weil er epistemisch ist. In diesem Zusammenhang wird z. B. in Witte et al. (2020) an Modellen zur Beschreibung der Szenarienwahrscheinlichkeiten gearbeitet. Der Grundgedanke der Überlegungen in Witte et al. (2020) ist, dass eine absolute Häufigkeitsangabe mangels Evidenz nicht abbildbar ist. Eine vernetzte Darstellung jedoch würde es erlauben, Bedrohungsszenarien auf logische Konsistenz zu prüfen: Über eine Kombination von Angreifer-Eigenschaften (z. B. Skills, Werkzeuge, öffentlich verfügbare Informationslage) kann von Experten eine Aussage getroffen werden, ob bestimmte Szenarien plausibler sind als andere.

Wenn nun die Frequency-Spalte der ASIL-Matrix durch die Attack Feasibility (Vulnerabilität) und die Severity-Spalte durch den Impact substituiert werden, können CAL nach demselben Schema wie ASIL ermittelt werden: Die Auswirkungen werden mit der Vulnerabilität und der Controllability tabellarisch miteinander verknüpft (siehe Tabelle 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

Tabelle 49: Überlegung zur Rekategorisierung von CAL nach ISO 26262.
Quelle: Eigene Tabelle in Anlehnung an Embitel.com (2018)[65]

Die Größe „Controllability" beschreibt in der IT-Security beispielsweise, wie groß die Fähigkeit eines Betreibers ist, bei einer Kompromittierung des betroffenen Systems einen Schaden durch eine geeignete Reaktion nach Erreichung eines Assets zu reduzieren. Das könnte z. B. die Möglichkeit einer Deaktivierung des Mobile Access Service aus der Ferne oder die Aktivierung eines Fallback-Plans umfassen. Im Gegensatz zur IT-Sicherheitsbewertung wird in der physischen Sicherheitsbewertung (z. B. nach Lichte et al. (2016)) nur den Zeitraum vom Beginn eines Angriffes bis zur Asset-Erreichung betrachtet, nicht darüber hinaus. Reaktive Maßnahmen sind nach der Asset-Erreichung aus rein physischer Sicht schwierig umzusetzen, da erwartet wird, dass das Fahrzeug gestohlen wird. Nun könnte argumentiert werden, dass reaktive Maßnahmen für alle noch im Feld befindlichen Produkte initiiert werden könnten, so z. B. Rückrufaktionen oder die physische Nachrüstung von Mobile Access Produkten vor Ort. Eine Controllability-Skala kann für die physische Sicherheit und für die IT-Sicherheit wie folgt aussehen (siehe Tabelle 50):

Controllability	Description
Difficult	Weiterer Impact kann durch postventive Maßnahmen nur unzureichend verhindert werden.
Normal	Es liegen Möglichkeiten vor, weiteren Impact durch postventive Maßnahmen einzuschränken.
Simple	Weiterer Schaden kann durch postventive Maßnahmen weitestgehend begrenzt werden.

Tabelle 50: Controllability Category Description.
Quelle: Eigene Tabelle.[66]

Anders als beim CAL bezieht sich der ASIL aber auf Anforderungen an eine ganz konkrete Sicherheitsunktion einer Komponente: Die Komponente ist – je nach ASIL – derart mit geeigne-

[65] Die Sicherheitseinstufungen „Quality Managed" (QM, ISO 26262) und „---" (ISO/SAE 21434) sind vergleichbar. QM bedeutet, dass der Entwicklungsprozess einer standardisierten und wiederholbaren Methodik für die Entwicklung des Produkts folgen soll (ISO 26262). Ein Beispiel dafür kann z. B. Automotive SPICE sein. Gemäß Automotive SPICE ist das Produkt nach dem V-Modell zu entwickeln. In der ISO/SAE 21434 wird für die Sicherheitseinstufung „---" vorgeschlagen, das Produkt nach dem V-Modell zu entwickeln (SAE, 2022, S. 15). Demzufolge können „QM" und „---" synonym verwendet werden.

[66] Postventiv bezeichnet die Zeit nach einem erfolgreichen Angriff.

ten Maßnahmen auszurüsten, dass eine bestimmte Ausfallrate dieser Komponente nicht überschritten wird. In der physischen Security beispielsweise findet die Sicherheitsbetrachtung auf Systemebene statt. Das liegt daran, dass die Vulnerabilität von dem Zusammenspiel der Vulnerabilitätsbestandteile Protektion, Observation und Intervention abhängig ist. Ein System ist demzufolge vulnerabel, wenn das Zusammenspiel von Protektion, Observation und Intervention entlang eines betrachteten Pfades nicht ausreichend ist. Insofern eine Komponente ausfallen sollte, z. B. die Protektion an Barriere eins (von insgesamt drei Barrieren), dann ist das noch keine hinreichende Bedingung, dass das Gesamtsystem zu 100 % vulnerabel ist. Beim ASIL wird nach einer konkreten Ausfallrate entwickelt. Bei der vorgeschlagenen CAL-Matrix ist die Attack Feasibility (Vulnerabilität), nach welcher bei einem bestimmten CAL entwickelt werden müsste, jedoch Bestandteil der CAL-Matrix.

In der physischen Sicherheit wiederum müsste bei einem bestimmten PAL nach einem Vulnerabilitätsniveau entwickelt werden. Folglich darf ein CAL nicht von der Attack Feasibility und ein PAL darf nicht von der Vulnerabilität abhängen. Ein Lösungsansatz kann sein, die Vulnerabilität aus der CAL- bzw. PAL-Matrix in einem ersten Schritt herauszunehmen und zu definieren, dass sich ein Security-Level aus der Kombination von Impact und Controllability ergibt. Hinter jedes Impact-/Controllability-Paar kann in einem zweiten Schritt ein Vulnerabilitätsniveau geschrieben werden, nach welchem das betrachtete System zu entwickeln ist. Bei der Anwendung einer viergliedrigen Skala für die Vulnerabilität („Very Low" – „Low" – „Medium" – „High") kann die Verknüpfung von Impact und Controllability wie folgt aussehen (siehe Tabelle 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

Tabelle 51: Ansatz zur Herleitung von CAL und PAL.
Quelle: Eigene Tabelle.

Die Zusammenhänge in Tabelle 51 sind in einem dritten Schritt auf Plausibilität zu prüfen. Die Eintragung „---" bedeutet, dass keine weiteren Maßnahmen zur Risikominderung erforderlich sind und dass empfohlen wird, nach dem V-Modell zu entwickeln. Insofern die Auswirkungsskala als „Severe = alle Flottenkunden bzw. Fahrzeuge betroffen, Major = alle Flotten bzw. Fahrzeuge eines Kunden betroffen, Moderate = Flottenfahrzeuge einer Flotte eines Kunden betroffen, Negligible = ein Fahrzeug betroffen" aufgestellt wird, gibt es aus physischer Security-Perspektive ein Problem: Wenn angenommen wird, dass physische Angriffe geringer skalieren als IT-Angriffe und folglich mit einem Fahrzeugeinbruch nur ein einziges Fahrzeug gestohlen werden kann, dann können gem. Tabelle 51 nur die Impact-Controllability-Zuordnungen „Negligible-Simple" („---"), „Negligible-Normal" („---") und „Negligible-Difficult" (PAL „1") zutreffen. Nach dieser Einstufung würden in der physischen Sicherheit in allen drei Fällen minimale Anforderungen an die Vulnerabilität gestellt werden.

Der maximale physische Impact ist ein gestohlenes Fahrzeug. Es wurde zuvor als niedrigstes Auswirkungslevel festgelegt. Aus IT-Security-Perspektive jedoch ist der physische Impact „ein Fahrzeugdiebstahl" in Relation zum Impact „ganze Fahrzeugflotten können gestohlen werden" gering. Um das Problem aufzulösen, kann die Auswirkungsskala überdacht und neu de-

finiert werden. In der ISO/SAE 21434 werden vier Impact-Typen unterschieden: Financial, Privacy, Operational und Safety (ISO/SAE, 2021b, S. 63-64). Jedes Impact-Rating besitzt vier Ausprägungsstufen: „Severe", „Major", „Moderate" und „Negligible" (siehe beispielhaft Tabelle 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.

Tabelle 52: Operational Impact-Rating nach ISO/SAE 21434.
Quelle: ISO/SAE (2021b, S. 64).

Die Kriterien, wie sie in der ISO/SAE 21434 vorliegen, sind denen von Harnser (2010, B3 S. 42) aus der physischen Sicherheit ähnlich. Im Gegensatz zu den Impact-Typen Financial, Privacy, Operational und Safety in der ISO/SAE 21434 verwendet Harnser die Einordnungen „Loss of Life/Health", „Loss of Production" und „Loss of Containment". „Loss of Life/Health" entspricht in etwa dem Impact-Typ „Safety". "Loss of Production" (Auswirkungsskala nach Harnser (2010)) entspricht dem Impact-Typ „Operational". „Loss of Containment" besteht dagegen aus Anteilen von „Safety", „Operational" und der „Controllability". Hierbei geht es um sekundäre Folgen nach einem erfolgreichen Angriff, z. B. bedingt durch freigesetzte toxische Gase, etc. Anstelle eines Ratings mithilfe von deskriptiven Stufen verwendet Harnser numerische Werte zwischen „10" (keine signifikanten Konsequenzen) und „100" (großer monetärer bzw. gesundheitlicher Schaden). Die Dimensionierung bei Harnser ist offensichtlich eine andere als beim Impact-Rating nach ISO/SAE 21434. Harnser betrachtet ganze kritische Infrastrukturen (KRITIS). In der ISO/SAE 21434 geht es um ein Fahrzeug. Bei MAS ist aber nicht nur der Impact auf ein Fahrzeug zu berücksichtigen, sondern auch auf ganze Fahrzeug-Flotten. Den Kriterien aus Tabelle 52 folgend, kann unter Berücksichtigung der Flottenperspektive ein neues Impact-Rating wie folgt aussehen (siehe Tabelle 53):

Impact Rating	Criteria
Severe	Der funktionale Schaden führt zum Verlust mehrerer Fahrzeuge oder zu einem Blackout des MAS-Service. Beispiel: Kompromittierte Cloud, Diebstahl mehrerer Fahrzeuge.
Major	Der funktionale Schaden führt zum Verlust des Fahrzeugs oder des MAS-Service für ein Fahrzeug. Beispiel: Diebstahl des Fahrzeugs, Benutzer bekommt das Fahrzeug nicht verriegelt oder entriegelt.
Moderate	Der funktionale Schaden führt zu partiellen Beeinträchtigungen des MAS-Service. Beispiel: Benutzerzufriedenheit ist beeinträchtigt.
Negligible	Der funktionale Schaden führt zu keinen oder nicht wahrnehmbaren Beeinträchtigungen des MAS-Service.

Tabelle 53: Operationales Impact-Rating und Kriterien für MAS.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 63-64).[67]

Das Ziel eines möglichen Angreifers wird als die Erzielung eines funktionalen Schadens durch einen physischen Angriff oder durch einen IT-Angriff definiert. Den Impact-Kriterien zufolge umfassen alle Impact-Kategorien Grade der Kompromittierung auf physischem oder IT-Wege. Darüber hinaus können die Kategorien auch seitens Experten mit monetären Verlustwerten belegt werden (siehe Kapitel 3.3.1). Die Kategorien „Major" und „Severe" beinhalten den Verlust physischer Assets. Das Vorgehen, die Auswirkungsbeiträge auf eine vergleichbare Skala zu bringen, sodass die Auswirkungsskalen in der physischen Sicherheit und in der IT-Sicherheit

[67] Eine Skala, die für zwei Domänen in gleicher Weise aufgebaut ist, kann die Interpretation sowie die Vergleichbarkeit von Levels erleichtern (Newsome, 2013, S. 102, 104).

einen gemeinsamen Bereich abbilden, wird auch als „Min-Max-Normalisierung" bezeichnet (Al Shalabi & Shaaban, 2006). Mit dieser Festlegung kann die Herleitung von CAL und PAL nach der Matrix aus Tabelle 51 erfolgen. Des Weiteren sollen im Zuge der Risikobewertung von CPS auch Szenarien mit domänenübergreifender Wechselwirkung mit einem Sicherheitslevel für beide Domänen versehen werden können. Experten müssen einschätzen, inwiefern z. B. ein IT-Szenario einen domänenübergreifenden Impact auf ein physisches Szenario haben kann. Zunächst ist zu klären, wie Experten den IT Impact on Physical Vulnerability (ITIPV) bewerten können. Es wird angenommen, dass mit einer Wechselwirkung eine Änderung der Funktionalität von Sicherheitsmaßnahmen einhergeht. Das bedeutet, dass mit einem IT-Szenario die Ausprägung der drei Größen Protektion, Observation und Intervention reduziert werden kann. Die Reduktion von Protektion, Observation und Intervention resultiert in einer Verschlechterung der Schutzwirkung. Die Verschlechterung der Schutzwirkung aufgrund einer Wechselwirkung bedeutet eine Erhöhung der Vulnerabilität. Experten können die Beeinträchtigung der Sicherheitsfunktionen abschätzen.

Eine Möglichkeit kann sein, insgesamt zwei Scorings durchzuführen. In einem ersten Schritt werden Protektion, Observation und Intervention unter Annahme einer Barriere und einer quantitativ konformen, viergliedrigen Harnser-Skala (z. B. zu ICM 1) für den Fall gescort, dass sich nur ein physisches Szenario materialisiert. Anschließend wird die Score-Summe auf der viergliedrigen Vulnerabilitäts-Skala einsortiert. Im Ergebnis liegt eine Vulnerabilitäts-Kategorie vor, die einem vermuteten Wahrscheinlichkeitsintervall für die Vulnerabilität entspricht. In einem zweiten Schritt wird die Vulnerabilität wie im ersten Durchlauf ermittelt, jedoch wird davon ausgegangen, dass vor dem physischen Szenario eine IT-seitige Kompromittierung erfolgreich war. Es wird also die physische Vulnerabilität unter Berücksichtigung einer Wechselwirkung bestimmt. Im Ergebnis liegt entweder eine Vulnerabilitäts-Einstufung vor, die auf demselben Level wie im ersten Durchlauf oder auf einem höheren, d. h. schlechteren, Level liegt. Die relative Änderung der Vulnerabilitätsstufe aufgrund einer Wechselwirkung kann als Maß für die Schwere einer Kompromittierung, den ITIPV, heranziehen. Bei einer Bewertungsskala mit vier Kategorien ergeben sich folgende Möglichkeiten zur Einstufung des ITIPV (siehe Tabelle 54).

Wenn mindestens eine der drei Bewertungsgrößen an einer Barriere vollständig ausgehebelt wird, dann kann definiert werden, dass der ITIPV als „High" festgelegt wird. Diese Festlegung liegt darin begründet, dass die Vulnerabilität maximal wird, wenn mindestens eine der drei Bewertungsgrößen an einer Barriere ausfällt. Bei Vorliegen einer Wechselwirkung ist zu fragen, welche Anforderungen an die Entwicklung zu stellen sind. Es ist nicht zielführend, das physische Sicherheitslevel im Falle eines ITIPV zu erhöhen. Das Hinzufügen weiterer Barrieren beispielsweise reduziert den IT-Impact auf die betroffenen physischen Bewertungsgrößen nicht. Aussichtsreicher ist es dagegen, das System gegen die Realisierung des IT-Szenarios zu härten, welches einen Einfluss auf physische Sicherungsmechanismen hat. Angenommen, für ein fiktives physisches Szenario (ohne Berücksichtigung einer Wechselwirkung) wird mit PAL „2" ermittelt. Schätzen Experten ein, dass eine Wechselwirkung vorliegt, so kann das IT-Scenario, welches einen ITIPV aufweist, ebenso mit einem IT-Sicherheitslevel attribuiert werden, welches mindestens als gleichwertig zu PAL 2 aufgefasst wird. In diesem Beispiel ist das ein CAL „2" oder höher.

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

Tabelle 54: Ermittlung des ITIPV.
Quelle: Eigene Tabelle.[68]

Aus Betreibersicht besteht grundsätzlich ein Problem darin, nur knappe Ressourcen zur Verfügung zu haben (Sowa, 2011, S. 8). Die Einstufung eines CAL sollte dem unternehmerischen Management begründet werden können. Alle CAL auf die vierte Stufe bei einem Szenario mit domänenübergreifendem Impact zu setzen, ist unwirtschaftlich. Die Einführung einer Regel kann dabei unterstützen, das IT-Szenario mit einem Impact auf die physische Vulnerabilität mit einem angemessenen CAL zu attribuieren. Nachfolgend ein Beispiel: Bei PAL 4 soll gegen die niedrigste Vulnerabilitätskategorie, „Very Low", entwickelt werden. Liegt die Vulnerabilität in dieser Kategorie, kann gem. Tabelle 54 ein ITIPV potenziell die Kompromittierungsgrade „Very Low", „Low", „Medium" und „High" annehmen. Insofern mindestens einer der drei Bewertungsgrößen vollständig ausgehebelt wird, wird laut der zuvor gemachten Festlegung die ITIPV-Kategorie „High" gesetzt. Weil PAL „4" als das höchste Sicherheitslevel definiert ist, wird für alle ITIPV-Kategorien, die eintreten können, beispielsweise auch der CAL „4" für alle potenziellen Kompromittierungsgrade gewählt.

Bei PAL „2" soll nach dem Vulnerabilitätsniveau „Medium" entwickelt werden. Gemäß Tabelle 54 kann es die potenziellen Kompromittierungsgrade „Very Low" und „Low" geben. Ein Kompromittierungsgrad von „Medium" ist undefiniert. Ferner wird angenommen, dass bei der vollständigen Aushebelung mindestens eines Wirkmechanismus der ITIPV auf „High" gilt. Folglich ist zu fragen, welcher CAL unter Berücksichtigung der ITIPV-Einstufung gesetzt werden sollte. Der minimale CAL für das IT-Szenario ist CAL „2", da PAL „2" für das physische Szenario angenommen wird. Es kann dann beispielsweise allgemein die Vereinbarung getroffen werden, dass bei einem ITIPV von „Very Low" nach CAL „2" entwickelt wird, bei einem ITIPV von „Low" nach CAL „3" und bei einem ITIPV von „High" nach CAL „4". Nach demselben Prinzip kann eine Zuweisung von CAL für PAL „1" und PAL „3" durchgeführt werden (siehe Tabelle 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

Tabelle 55: Vorschlag zur Festlegung von CAL im Falle einer Wechselwirkung.
Quelle: Eigene Tabelle.[69]

[68] Das Harnser-Scoring in diesem Fall ist quantitativ konform zur Variante ICM 1.
[69] „x" steht für undefiniert.

Mithilfe von Tabelle 55 können schlussfolgernd Sicherheitsniveaus in der physischen Sicherheit und in der IT-Sicherheit in Abhängigkeit von dem Grad der Wechselwirkung aufeinander abgestimmt werden. Das gilt allgemein unabhängig von der Wirkrichtung, d. h. anstelle PAL „1“ bis „4“ in der ersten Spalte von Tabelle 55 könnte auch CAL „1“ bis „4“ stehen. In diesem Fall würde dann der PAL in Abhängigkeit von der Schwere einer Wechselwirkung festgelegt werden. Da in der IT-Security jedoch keine Möglichkeit zum quantitativen Nachweis von Vulnerabilität mittels einer Metrik mit objektivem Wirkmechanismus besteht, mit welchem die Effektivität von Maßnahmen zur Vulnerabilitätsreduktion bewertet werden könnte, ist auf eine Betrachtung des Physical Impacts on IT Vulnerability (PIITV) zu verzichten.

4 Aufbau der Risikoanalyse

In diesem Kapitel wird ein Vorgehen zur domänenübergreifenden Bedrohungsanalyse und Risikobewertung von MAS entwickelt. Als Beispiel wird für die physische Sicherheitsbewertung ein Referenzmodell, bestehend aus einer Barriere und einem Asset, herangezogen. Für die IT-Security wird ein Referenzmodell mit einer Barriere mit einer Schwachstelle und einem Asset betrachtet. Die domänenübergreifende Bedrohungsanalyse und Risikobewertung wird unter der Annahme entwickelt, dass eine Anpassung der IT-Exploitability-Niveaus, welche Scoring-basiert über das CVSS ermittelt werden, an objektive Exploitability-Niveaus nicht möglich ist. Diese Annahme liegt im Fehlen einer wirksamkeitsbasierten, quantitativen Metrik für die IT-Exploitability begründet. Die Annahmen aus Gl. (1) (siehe Kapitel 2.3) werden in diesem Kapitel vorausgesetzt.

4.1 Bewertung (Profiling) von Assets

Ein erster wesentlicher Schritt zur Risikobewertung des betrachteten Systems ist die Untersuchung physischer und IT-Security-relevanter Strukturen. Dafür wird in Harnser (2010, B1, S. 4-13) das Profiling des betrachteten Systems vorgeschlagen. Profiling beschreibt das transparente und strukturierte Aufarbeiten immanenter Eigenschaften und Funktionen eines Systems und seiner technologischen Artefakte. Die Ergebnisse der Analyse liefern einen Überblick über zu schützende Elemente und Funktionen, sog. Assets. Darüber hinaus geben sie einen Hinweis darauf,

1. wie die einzelnen physischen Komponenten und IT-Komponenten miteinander in Beziehung stehen.
2. auf welche mannigfaltige Weise das Ziel, z. B. im Falle MAS das unerwünschte Auslösen eines Trigger-Events, erreicht werden kann.
3. welche Auswirkungen mit einem Angriff einhergehen können.

Für die Definition und Einordnung von Assets wird in Lyu et al. (2020) die Auflistung aller Assets in Form einer Tabelle demonstriert. Die Asset-Tabelle wird in Lyu et al. (2020) nach den folgenden Kriterien strukturiert: Asset-Typ, Bezeichnung, Verortung des Assets (z. B. physisch und IT). Eine ähnliche Vorgehensweise wird in Harnser (2010, B1, S. 4-13) durch die sog. What-If-Technik verfolgt. Diese Technik kann dabei unterstützen, Assets zu finden (Termin et al., 2020). Hierbei werden Szenarien aufgestellt, um systemrelevante Elemente zu identifizieren: „Was passiert, wenn Einheit x ihre Funktion nicht mehr erfüllt oder entfernt wird?“. In Lyu et al. (2020) und in Harnser (2010) werden nahezu gleiche Schritte zur Identifikation von Assets vorgeschlagen:

- **Schritt 1:** Sammlung und Analyse von Design-Dokumenten und Durchführung von Experteninterviews.
- **Schritt 2:** Klassifizierung der Assets des betrachteten Systems, z. B. gem. Lyu et al. (2020) nach materiell/immateriell, Daten, Software, Hardware, etc. oder nach Harnser (2010, B1, S. 6) nach Name, Rolle, Schlüsselabhängigkeit zu anderen Einheiten, Niveau der Leistungserbringung der Einheit im Gesamtkontext, usw.
- **Schritt 3:** Zusammenfassung und Erstellung einer Liste der Assets, wobei diese hinsichtlich ihres Wertes bewertet werden können, z. B. nach Harnser (2010, A4, S. 42; B1, S. 4) über ein Kritikalitäts-Scoring.

Zur Unterstützung der Identifikation von Assets wird in Termin et al. (2020) die Einordnung des zu untersuchenden Systems in einen Morphologischen Kasten (für MAS) vorgeschlagen. Die Asset-Analyse wird in Harnser (2010, B1, S. 4) funktionsbasiert durchgeführt. Diese Analyse

umfasst auch Prozesse, Sub-Prozesse und die Bewertung der Kritikalität von Sub-Komponenten. In Harnser (2010, B1, S. 4) werden Assets hinsichtlich ihrer Kritikalität zwischen „1" (niedrig) und „5" (hoch) gescort. Assets mit Scores kleiner gleich „2" werden in der weiteren Analyse nicht weiter betrachtet. Danach werden die mit einem Asset verbundenen (Sub-)Prozesse betrachtet, die Ergebnisse wieder nach den kritischsten Prozessen[70] gefiltert, usw. Ziel ist es, so Harnser (2010, B1, S. 4), dass sich Risikoanalysten auf die wichtigsten Assets konzentrieren und die weniger wichtigen ausschließen. Das liegt daran, dass nur knappe Ressourcen (Zeit und Geld) zur Verfügung stehen (Sowa, 2011, S. 8). Zudem wird bei Harnser (2010) eine kritische Infrastruktur betrachtet, die aus mehreren Sub-Systemen besteht. Der Umfang an möglichen Assets ist bei der Betrachtung von ganzen Infrastrukturen i.d.R. größer als z. B. bei der Betrachtung eines Fahrzeugs oder eines Systems, das im Fahrzeug verbaut wird.

Das Asset-Profiling ist grundsätzlich Use-Case-spezifisch (Harnser, 2010, B1, S. 4), d. h. ein Asset-Register – die Übersicht aller berücksichtigten und priorisierten Assets – eines Produkts im Use Case A kann andere Assets und Kritikalitätsbewertungen haben als ein Asset-Register im Use Case B. Eine Antwort auf eine Frage, welche im Zuge der Anwendung der What-If-Technik gestellt wird, entspricht laut der ISO/SAE 21434 einem oder mehrerer Schadensszenarien (Damage Scenarios). Mit einem Schadensszenario ist eine potenzielle Schutzzielverletzung von Vertraulichkeit (Confidentiality, C), Verfügbarkeit (Availability, A) und Integrität (Integrity, I) verbunden (ISO/SAE, 2021b, S. 73-74) (siehe als Beispiel Tabelle 56). Der Ansatz zur Bewertung von Assets, wie in ISO/SAE 21434 vorgeschlagen, kann sowohl für die physische als auch die IT-Sicherheit angewandt werden. Dieser wird für die Entwicklung eines Ansatzes zur domänenübergreifenden Bedrohungsanalyse und Risikobewertung verwendet.

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	—	...

Tabelle 56: Beispielhafte Asset-Analyse nach ISO/SAE 21434.
Quelle: Quelle: ISO/SAE (2021b, S. 74).

[70] Hiermit sind die operational wichtigsten Aktivitäten gemeint.

4.2 Bewertung (Profiling) von Bedrohungen

Gemäß der PRISM nach Harnser (2010) und der TARA nach ISO/SAE 21434 folgt auf das Asset-Profiling das Profiling der Bedrohungen (Harnser, 2010, B2, S. 15; ISO/SAE, 2021b, S. 74). Den Assets bzw. den Schadensszenarien werden in diesem Schritt Bedrohungsszenarien (Threat Scenarios) zugeordnet (siehe als Beispiel Tabelle 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

Tabelle 57: Beispielhaftes Damage Scenario – Threat Scenario Mapping nach ISO/SAE 21434. Quelle: ISO/SAE (2021b, S. 74).

In Termin et al. (2020) wird vorgeschlagen, Use Case Diagramme zu entwickeln und die Identifikation sowie Lokalisation von Angriffsvektoren durch Misuse Case Diagramme vorzunehmen. Außerdem müssen mögliche Angriffspfade untersucht werden, wie ein Asset erfolgreich kompromittiert werden kann. In Termin et al. (2020) wird die Durchführung einer Attack-Tree-Analysis (ATA) bzw. Attack-Graph-Analyse (AGA) am Beispiel MAS vorgeschlagen. Die Ergebnisse aus der ATA oder AGA liefern mögliche physische Angriffspfade und IT-Angriffspfade. In der ISO/SAE 21434 wird die Durchführung einer solchen Attack-Path-Analyse (APA) ebenfalls vorgeschlagen (ISO/SAE, 2021b, S. 75-76). Angriffspfade werden gem. ISO/SAE 21434 in tabellarischer Form einem Bedrohungsszenario zugewiesen (siehe beispielhaft Tabelle 58). Die APA kann sowohl in der IT-Domäne als auch in der physischen Domäne angewandt werden.

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).

Tabelle 58: Beispielhafte Attack Path-Analyse nach ISO/SAE 21434. Quelle: ISO/SAE (2021b, S. 75).

4.3 Bewertung (Profiling) von Attack Paths

Nachdem Bedrohungsszenarien zu Damage Scenarios zugeordnet sind und eine APA durchgeführt ist, ist es erforderlich, die Angriffspfade zu bewerten. Bewertungsgröße ist die Vulnerabilität. Zur Unterscheidung wird für die physische Sicherheitsbewertung Vulnerabilität geschrieben und für die IT-Sicherheitsbewertung Exploitability bzw. Attack Feasibility. Die Schwere einer Wechselwirkung wird durch den IT Impact on Physical Vulnerability (ITIPV) beschrieben. Die Vulnerabilitätsbewertung erfolgt auf Basis von Experteneinschätzungen. Den Überlegungen aus Kapiteln 3.3.1 folgend, kann die Attack Feasibility über die Bewertungsgrößen Attack Vector (AV), Attack Complexity (AC) und Privileges Required (PR*) bewertet werden. Die Ausprägungsstufen eines jeden Bewertungsparameters haben nach CVSS (First.org, 2022) jeweils einen zugeordneten numerischen Wert zwischen null und eins. Jeder dieser numerischen Werte wird nach Kapitel 3.3.4 zur Basis 0.6 logarithmiert. Jede Ausprägung eines Bewertungsparameters wird durch einen logarithmischen Score-Wert beschrieben (siehe beispielhaft Tabelle 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

Tabelle 59: Bewertungsparameter der IT-Vulnerabilitätsmetrik.
Quelle: Eigene Tabelle.

Um die Attack Feasibility respektive LoE zu bestimmen, werden für jeden Angriffspfad eines vorliegenden IT-Bedrohungsszenarios die Ausprägungsstufen von AV bis PR* von Experten festgelegt. Anschließend werden die log-Scores addiert. Danach wird das Ergebnis auf einer viergliedrigen Skala einsortiert. Im Ergebnis ergibt sich eine LoE- bzw. Attack-Feasibility-Kategorie zugehörig zu einem Angriffspfad (siehe Tabelle 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

Tabelle 60: LoE-Skala zur Bewertung der IT-Vulnerabilität.
Quelle: Eigene Tabelle.[71]

Die Attack-Feasibility-Skala hat insgesamt vier Einordnungen: „Very Low“, „Low“, „Medium“, und „High“. Diese können nach ISO/SAE 21434 (ISO/SAE, 2021b, S. 47) wie folgt interpretiert werden können (siehe Tabelle 61):

[71] Die vermuteten Wahrscheinlichkeitsintervalle sind hier beispielhaft gesetzt und zu gleichen Teilen auf die Kategorien der Skala verteilt. Aufgrund des Fehlens eines objektiven Wirkmechanismus kann die CVSS-Skala bisher nicht quantitativ konform gemacht werden.

Likelihood of Exploitability (Attack Feasibility)	Description
High	Der Angriffspfad kann mit sehr geringem Aufwand durchgeführt werden.
Medium	Der Angriffspfad kann mit geringem Aufwand durchgeführt werden.
Low	Der Angriffspfad kann mit moderatem Aufwand durchgeführt werden.
Very Low	Der Angriffspfad kann mit hohem Aufwand durchgeführt werden.

Tabelle 61: Beschreibung der Attack-Feasibility-Kategorien.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 47).

Die Vulnerabilität wird ebenfalls über einen Scoring-basierten Ansatz bewertet. Hierfür wird beispielhaft das Harnser-Scoring vorgeschlagen, welches quantitativ konform zur Variante ICM 1 ist. Das bedeutet, es werden moderate Streuungen bei den Bewertungsgrößen angenommen. Je nach vorliegendem Use Case müssen Experten die Annahme über die zugrungegelegten Mittelwerte und Streuungen abschätzen, welche den Harnser-Score-Stufen „1" bis „5" zugeordnet werden. Sind diese festgelegt, kann eine Harnser-Skala entwickelt werden, die quantitativ konform zu den angenommenen Mittelwerten und Streuungen ist. Die Festlegung von konkreten Zeiten für einen MAS-Use-Case ist grundsätzlich eine Herausforderung. Das liegt an den dynamischen Randbedingungen im Use Case. Die Bewertungsgrößen Protektion, Observation und Intervention können mit größeren Unsicherheiten behaftet sein als kritische Infrastrukturen, wo statische Randbedingungen vorherrschen (Möller et al. 2019, S. 307). Die konkrete Benennung, was insbesondere Observation und Intervention im MAS-Use-Case darstellt, muss mit Experten konsolidiert werden.

Die Festlegung von Kriterien kann dabei unterstützen, Sicherheitsfunktionalitäten hinsichtlich ihrer Ausprägung durch Experten einzusortieren (Harnser, 2010, B4, S. 51) (siehe als Beispiel Tabelle 62):

P-Score	**log-Score, base = 0.6**	**Kriterien zur Einordnung**	**ICM 1 Values (sec)**
1	0	Geringfügig ausgeprägte Fähigkeiten zur Überwindungshemmung.	$\mu = 15$ $\sigma = 30$
2	1	Begrenzte Fähigkeiten zur Überwindungshemmung.	$\mu = 45$ $\sigma = 30$
3	2	Moderat ausgeprägte Fähigkeiten zur Überwindungshemmung.	$\mu = 75$ $\sigma = 30$
4	3	Hoch ausgeprägte Fähigkeiten zur Überwindungshemmung.	$\mu = 105$ $\sigma = 30$
5	5	Sehr hoch ausgeprägte Fähigkeiten zur Überwindungshemmung.	$\mu = 135$ $\sigma = 30$
O-Score	**log-Score, base = 0.6**	**Kriterien zur Einordnung**	**ICM 1 Values (sec)**
1	0	Keine technischen Möglichkeiten zur Kontrolle der Zugangsmöglichkeiten, geringfügige Beobachtung der Zugangsmöglichkeiten durch den Menschen.	$\mu = 135$ $\sigma = 30$
2	1	Eingeschränkte technische Möglichkeiten zur Kontrolle der Zugangsmöglichkeiten, zeitweise Beobachtung der Zugangsmöglichkeiten durch den Menschen.	$\mu = 105$ $\sigma = 30$
3	2	Moderate technische Möglichkeiten zur Kontrolle der Zugangsmöglichkeiten, moderate Beobachtung der Zugangsmöglichkeiten durch den Menschen.	$\mu = 75$ $\sigma = 30$
4	3	Hohe technische Möglichkeiten zur Kontrolle der Zugangsmöglichkeiten, häufige Beobachtung der Zugangsmöglichkeiten durch den Menschen.	$\mu = 45$ $\sigma = 30$
5	5	Sehr hoher Grad an Möglichkeiten, den Zugang zu jeder Zeit und an jedem Ort durch technische Maßnahmen und/oder den Menschen zu kontrollieren.	$\mu = 15$ $\sigma = 30$
I-Score	**log-Score, base = 0.6**	**Kriterien zur Einordnung**	**ICM 1 Values (sec)**
1	0	Geringfügig ausgeprägte Fähigkeiten zur technischen und/oder menschlichen Intervention.	$\mu = 135$ $\sigma = 30$
2	1	Begrenzte Fähigkeiten zur technischen und/oder menschlichen Intervention.	$\mu = 105$ $\sigma = 30$

3	2	Moderat ausgeprägte Fähigkeiten zur technischen und/oder menschlichen Intervention.	$\mu = 75$ $\sigma = 30$
4	3	Hoch ausgeprägte Fähigkeiten zur technischen und/oder menschlichen Intervention.	$\mu = 45$ $\sigma = 30$
5	5	Sehr hoch ausgeprägte Fähigkeiten zur technischen und/oder menschlichen Intervention.	$\mu = 15$ $\sigma = 30$

Tabelle 62: Kriterien zur Festlegung von Harnser-Scores für eine Mobile-Access-Anwendung.
Quelle: Eigene Tabelle i Anlehnung an Harnser (2010, B4, S. 51).[72]

In gleicher Weise wie bei der Ermittlung der Attack Feasibility werden die numerischen Werte, welche jeweils zu den Scores von Protektion, Observation und Intervention gehören, zur Basis 0.6 logarithmiert. Die log-Werte werden für einen physischen Angriffspfad gesetzt und es wird die Summe der log-Scores gebildet, um den Likelihood of Vulnerability (LoV) Score zu erhalten. Wenn angenommen wird, dass ein MAS nur aus einer Produktbarriere besteht und die Annahmen für die ICM-Variante eins gelten, dann kann das Scoring mit den vermuteten Wahrscheinlichkeitsintervallen aus Tabelle 41 verwendet werden. Der LoV-Score wird entsprechend auf der vierstufigen Harnser-Skala einsortiert (siehe Tabelle 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

Tabelle 63: LoV-Skala zur Einordnung der physischen Vulnerabilität.
Quelle: Eigene Tabelle.

Analog zu Tabelle 61 ist eine Beschreibung der Stufen durch Deskriptoren möglich (siehe Tabelle 64).

Likelihood of Vulnerability (Attack Feasibility)	Description
High	Das Asset wird mit hoher Wahrscheinlichkeit erreicht. Die Schutzwirkung ist gering ausgeprägt.
Medium	Das Asset wird mit moderater Wahrscheinlichkeit erreicht. Die Schutzwirkung ist mittelmäßig ausgeprägt.
Low	Das Asset wird mit geringer Wahrscheinlichkeit erreicht. Die Schutzwirkung ist gut ausgeprägt.
Very Low	Das Asset wird mit sehr geringer Wahrscheinlichkeit erreicht. Die Schutzwirkung ist stark ausgeprägt.

Tabelle 64: LoV Category Description.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 47).

Die Wahl der Scores von Protektion, Observation und Intervention hängt vom vorliegenden Angriffspfad und dem Angreifer ab. In der IT werden die Größen AV, AC und UI entlang eines ganzen Pfades, unabhängig von der Pfadlänge, bewertet (ISO/SAE, 2021b, S. 76). In der physischen Sicherheit bedeutet aber „Angriffspfad", dass ein Angreifer eine bestimmte Barriere-Kombination bis zum Asset überwinden muss (Lichte et al., 2016). In dem Ansatz, wie er in

[72] Hinter jedes Kriterium wird jedoch eine quantitative Stufe geschrieben, hier angenommen auf Basis der ICM 1.

dieser Arbeit vorgeschlagen wird, scoren Experten Protektion, Observation und Intervention jeweils für eine Barriere. Das liegt daran, dass die Harnser-Skala quantitativ konform zu einer ICM-Variante gemacht wird, mit der die Vulnerabilität einer einzigen Barriere bewertet wird. Hat ein Produkt z. B. mehrere vergleichbare Barrieren, kann die Gesamtvulnerabilität wie folgt bestimmt werden:

1. Die Bewertungsgrößen der einzelnen Barrieren werden jeweils von Experten gescort.
2. Der Vulnerabilitäts-Score wird für jede Barriere ermittelt.
3. Die Vulnerabilitäts-Scores für Barriere eins und zwei werden auf der zu ICM 1 quantitativ konformen, viergliedrigen Harnser-Skala in eine Kategorie einsortiert.
4. Da hinter jeder Kategorie auf der Vulnerabilitätsskala ein vermutetes Wahrscheinlichkeitsintervall steht, kann für jede Barriere ein Vulnerabilitätsniveau ermittelt werden.
5. Um die Gesamtvulnerabilität zu erhalten, kann eine Möglichkeit sein, die folgenden Schritte durchzuführen:
    1. Für jede Barriere wird unter Annahme eines Worst Cases jeweils die obere Intervallgrenze des vermuteten Wahrscheinlichkeitsintervalls gewählt, z. B. Barriere eins, „Medium“ = 0.98, Barriere zwei, „Very Low“ = 0.2.
    2. Die beiden Wahrscheinlichkeiten werden miteinander multipliziert.
    3. Das Ergebnis wird in die Kategorien der zu ICM 1 quantitativ konformen, viergliedrigen Harnser-Skala einsortiert, d. h. hier Gesamtvulnerabilität = 0.196 (≙ „Very Low“). Liegt die Gesamtvulnerabilität beispielsweise bei 0.8 (obere Intervallgrenze der Kategorie „Low“ und untere Intervallgrenze der Kategorie „Medium“), dann wird die Kategorie mit der höheren Vulnerabilität gewählt.

Für das Beispiel zweier Barrieren, die vergleichbar hinsichtlich ihrer Sicherheitseigenschaften aufgebaut sind, sind in Tabelle 65 die Werte und Einstufungen der Gesamtvulnerabilität für alle möglichen Permutationen dargestellt.

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

Tabelle 65: Scoring-basierte Ermittlung der physischen Gesamtvulnerabilität bei Vorliegen zweier Barrieren.
Quelle: Eigene Tabelle.

Nach der Bewertung von physischen Angriffspfaden und IT-Angriffspfaden wird der IT Impact on Physical Vulnerability (ITIPV) von Experten für Szenarien mit domänenübergreifender Wechselwirkung bewertet (siehe Kapitel 3.3.4). Die Skala des ITIPV hat ebenso wie die Skala der physischen Vulnerabilitätsbewertung und IT-Exploitability-Bewertung vier Kategorien. Die Beschreibung der Kategorien kann wie folgt aussehen (siehe Tabelle 66).

IT Impact on Physical Vulnerability	Description
High	Die Schutzwirkung wird massiv reduziert. Die LoV wird um drei Kategorien erhöht.
Medium	Die Schutzwirkung wird stark reduziert. Die LoV wird um zwei Kategorien erhöht.
Low	Die Schutzwirkung wird mäßig reduziert. Die LoV wird um eine Kategorie erhöht.
Very Low	Die Schutzwirkung wird geringfügig reduziert. Die LoV-Kategorie bleibt gleich.

Tabelle 66: IT Impact on Physical Vulnerability Category Description.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 47).

4.4 Bewertung (Profiling) von Auswirkungen

Wenn Assets, Bedrohungen und die Exploitability bzw. Vulnerabilität bewertet werden, dann ist auch die Bewertung der Auswirkungen notwendig, um eine ganzheitliche Risikobetrachtung zu ermöglichen. In der Risikobewertung müssen sich also Auswirkungen von erfolgreichen Angriffen wiederfinden lassen. Die Auswirkungen können je nach Art des Angriffs unterschiedlich skalieren (Termin et al., 2020). CPS liegt das Prinzip „from physical to digital to physical“ zugrunde (Hoffmeister, 2017, S. 136, 193; Sinha et al., 2015). Deswegen gibt es drei Perspektiven, Auswirkungen zu bewerten: die physische Sicht (Auswirkungen durch physische Angriffe), die IT-Sicht (Auswirkungen von IT-Angriffen) und die cyberphysische Sicht (Auswirkungen von IT-Angriffen auf physische Szenarien und vice versa). Auswirkungen können in erster Linie am Asset bzw. einer Komponente des Assets, welches von einem Angreifer erreicht wird, festgemacht werden (Harnser 2010, B6, S. 64). Da Assets im Rahmen dieser Forschungsarbeit funktionalitätsbasiert bewertet werden, gibt es im Falle eines erfolgreichen Angriffs einen Funktionalitäts-Impact auf eine Komponente, eine Einheit oder ganze Systeme. Physische Szenarien mit einem Impact auf IT-Szenarien werden nachfolgend nicht betrachtet, da die Beeinträchtigung von IT-Sicherheitsfunktionen durch physische Angriffe schwer zu quantifizieren ist.

Grundsätzlich kann es innerhalb eines Systems verschiedene Komponenten geben, die auf beliebig komplexe Weise hierarchisch angeordnet sind. Die Frage ist, wie diese Beziehungen verwendet werden können, um Auswirkungen über Skalenkategorien klassifizieren zu können. In der IT gibt es ein Standardkonzept namens Server-Client-Modell (SCM) (DIN SPEC 27070). Das SCM beschreibt die Beziehung von Systemeinheiten zueinander und die Verteilung von Aufgaben unter diesen Einheiten. Ein Server stellt beispielsweise Dienste für einen Client bereit. Aufgrund dieser klaren hierarchischen Struktur kann davon ausgegangen werden, dass wenn der Server gehackt wird, auch die untergeordneten Komponenten gehackt werden können. Angenommen, dass eine Komponente C1 über zwei Angriffsmodi angegriffen werden kann. Darüber hinaus hat C1 die übergeordnete Komponente C2. C1 kann erfolgreich kompromittiert werden, wenn C2 erfolgreich gehackt wird oder einer der Bedrohungsszenarien erfolgreich ist oder wenn alle Möglichkeiten eintreten. Mit der erfolgreichen Kompromittierung einer Einheit oder einer Komponente geht eine Auswirkung einher, die sich in der physischen Welt manifestiert. Für MAS wird die Auswirkungsskala, wie in Kapitel 3.3.4 vorgeschlagen, verwendet.

4.5 Bewertung (Profiling) von Risiken

Risiko wird nach ISO/SAE 21434 mithilfe einer Risikomatrix ermittelt. Nach Hubbard et al. (2016) ist die Anwendung einer Risikomatrix eine bewährte Vorgehensweise aus der Industrie. „These scales represent both likelihood and impact, not in probabilistic or monetary terms, but in ordinal scales", so Hubbard et al. (2016, S. 84). Nach ISO/SAE 21434 wird der Impact in tabellarischer Form mit der Attack Feasibility, z. B. nach CVSS, verknüpft (ISO/SAE, 2021b, S. 76-77). Jedes Impact-/Attack-Feasibility-Paar erhält einen Score-Wert von „1" (= niedrig) bis „5" (= hoch). Je höher der Impact und je höher die Attack-Feasibility-Kategorie, desto größer ist der Risiko-Score. Mit der Attack Feasibility wird bewertet, dass ein durchgeführter Angriff zum Erfolg führt. Hierfür braucht es auf der einen Seite eine Bedrohung und auf der anderen Seite eine Vulnerabilität (Exploitability). Die Bedrohungswahrscheinlichkeit wird aber bei der Bewertung der Attack Feasibility ausgeklammert. Ein Grund dafür kann die (möglicherweise) zugrunde gelegte Annahme sein, dass eine Schwachstelle theoretisch auch von einem Angreifer ausgenutzt wird, wenn diese vorhanden ist. In Nayak et al. (2014) wird zwar festgestellt: „[…] some vulnerabilities are never exploited in the wild, partly due to security technologies that make exploiting them difficult" (Nayak et al., 2014, S. 1). Im Interagency Report 7628 „Guidelines for Smart Grid Cyber Security" des National Institutes of Standards and Technology (NIST) aus dem Jahr 2010 wird aber in diesem Zusammenhang hervorgehoben: „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, S. 3).

Identifizierte Schwachstellen sind somit per Default zu schließen. Grundsätzlich ist nicht bekannt, wann ein Angreifer eine Schwachstelle ausbeuten wird. Mit einer Bedrohungsanalyse und Risikobewertung kann jedoch ermittelt werden, wo es Schwachstellen im System gibt und wie diese ausgebeutet werden könnten. Ferner wird in Foreman (2019) klargestellt: „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, S. XV). Aufbauend auf den Überlegungen aus Kapitel 3.3.4 ergibt sich in Anlehnung an die Risikomatrix aus der ISO/SAE 21434 für das physische Risiko Tabelle 67 und für das IT-Risiko Tabelle 68. Auf Basis dieses Scorings können physische und IT-Risiken der Größe nach sortiert und priorisiert werden.

	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

Tabelle 67: Physische Risiko-Matrix.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 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

Tabelle 68: IT-Risiko-Matrix.
Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 78).

Eine Möglichkeit, sich auf große Risiken zu fokussieren, kann darin bestehen, eine Risikoakzeptanzschwelle zu definieren. Das heißt, durch Experten wird z. B. festgelegt, dass alle Risiken mit einem Score kleiner gleich „2" eingegangen werden. Für alle anderen Risiken ist eine Behandlung in Form einer Maßnahmen-Implementierung notwendig. Da beide Risikomatrizen dieselbe Einteilung haben, können diese auch in einer Matrix zusammengeführt werden (siehe Tabelle 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

Tabelle 69: Matrix zur Bestimmung des physischen, IT und cyberphysischen Risiko-Scores. Quelle: Eigene Tabelle in Anlehnung an ISO/SAE (2021b, S. 78).

4.6 Modellierung in Bayes'schen Netzen

Nachdem in den vorangegangenen Kapiteln Schritte zur Durchführung einer Bedrohungsanalyse und Risikobewertung für CPS dargelegt wurden, stellt sich die Frage nach einer Möglichkeit zur probabilistisch konsistenten Zusammenführung. Die Methode Bayes'scher Netze ist eine Option, wie Eigenschaften aus der physischen Domäne und Eigenschaften aus der IT-Domäne miteinander probabilistisch konsistent verknüpft werden können. Bayes'sche Netze werden bereits auf Probleme der Risikobewertung unter Berücksichtigung zweier Domänen angewendet, so beispielsweise in Lichte et al. (2019), um Auswirkungen von Cybersicherheit auf die Safety am Beispiel eines „x-by-wire-Systems" zu bewerten. In Lyu et al. (2020) wird ein „Cyber-to-Physical"-Risikoanalysemodell zur Bewertung der Funktionalen Sicherheit unter Berücksichtigung von Cyber-Bedrohungen vorgeschlagen und am Beispiel eines angegriffenen Wassertanksystems evaluiert. Die Erkennung und Bestimmung von Anomalien in CPS wird in Chockalingam et al. (2017) durch Bayes'sche Netze modelliert. In Chockalingam et al. (2017) wird ein Ansatz aufgezeigt, wie zwischen der Anomalie durch einen physischen Fehler (Safety-Fall) oder durch einen Cyber-Angriff differenziert werden kann, um je nach Ursache entsprechende Maßnahmen einleiten zu können. In Wang et al. (2017) werden Möglichkeiten aufgezeigt, wie sich Wechselwirkungen von ausgebeuteten Schwachstellen innerhalb eines IT-Netzwerks durch Bayes'sche Netze abbilden lassen.

Die Methode des Bayes'schen Netzes findet darüber hinaus in der IT-Security Anwendung, wie z. B. in Xie et al. (2010) und Wu et al. (2017). Darüber hinaus wird die Methode ebenso in der Physical Security, etwa in Fakhravar et al. (2017) und Argentini et al. (2018), verwendet. Während in Fakhravar et al. (2017) die Vulnerabilität physischer Protektionssysteme (PPS) am Beispiel einer Gaspipeline modelliert und bewertet wird, wird in Argentini et al. (2018) eine Chemieanlage betrachtet. Bayes'sche Netze sind somit eine gängige Methode in der IT-Security-Bewertung und Physical-Security-Bewertung. Die Methode wird auch zur Beantwortung von Fragestellungen bezüglich der Wechselwirkung von Safety und IT-Security herangezogen. Vorteilhaft am Einsatz der Methode Bayes'sches Netz ist, dass das zur Verfügung stehende Wissen und getroffene Annahmen probabilistisch konsistent abgebildet werden können, d. h. der Ansatz ist mit der Wahrscheinlichkeitstheorie vereinbar (Koch, 2013). Die Methode Bayes'scher Netze wird in Prokain (2008, S. 74) mit anderen Methoden[73] anhand der Kriterien

[73] Das sind: Schlüsselwertmethode, modifizierter Basisindikatoransatz/Standardansatz nach Basel II, interner Bemessungsansatz, Score-Card-Ansätze, Capital Asset Pricing Model, Szenario-Analyse, Vollenumeration und Monte-Carlo-Simulation.

Risikosensitivität, Unterteilung der Gesamtverluste in erwartete und unerwartete Verluste, Anforderung an das Datenmaterial, Berücksichtigung qualitativer und quantitativer Faktoren sowie Umsetzungsaufwand verglichen. Ziel des Vergleichs ist es, herauszufinden, welcher Ansatz besonders gut geeignet ist, um Risiken in einer eingesetzten IT-Infrastruktur und damit verbundenen Geschäftsprozessen zu quantifizieren. Die Ergebnisse von Prokains Untersuchungen zeigen in diesem Zusammenhang eine gute Eignung Bayes'scher Netze auf. Für den Einsatz Bayes'scher Netze werden folgende Vor- und Nachteile benannt (Prokain, 2008, S. 78):

- **Vorteile:** Transparente Abbildung von Kausalketten, Berücksichtigung von qualitativen und quantitativen Faktoren, Quantifizierung von Verlusten, Unterteilung in erwartete/unerwartete Verluste bei verschiedenen Konfidenzniveaus möglich.
- **Nachteile:** Hohe Anforderungen an das Datenmaterial, Aufbau des Netzes mit hohem Aufwand verbunden.

Auf Basis genannter Anwendungspotenziale kann folglich die Vermutung aufgestellt werden, dass mit dem Transfer von Expertenwissen in bedingte Wahrscheinlichkeiten auf Basis Bayes'scher Netze auch die Metriken aus der physischen und IT-Security zusammengeführt werden können, sodass eine Gesamtbewertung entsteht, die auch Wechselwirkungen abbilden kann. Bayes'sche Netze sind im Sinne der Einsetzbarkeit für die Risikobewertung versatil, weil Expertenwissen und Kausalitäten durch bedingte Wahrscheinlichkeiten beschrieben und tatsächliche Vorgänge mathematisch dargestellt werden können (Lyu et al., 2020). Expertenwissen wird in der Security mangels Evidenz verwendet, um die Wahrscheinlichkeit bestimmter Angriffsszenarien für einen bestimmten Use Case abzuschätzen (Harnser, 2010, A4, S. 42). Die Überführung von Expertenwissen in subjektiven Wahrscheinlichkeiten (Expert Knowledge Allocation, (Nevo et al., 2012)) muss bei einer domänenübergreifenden Bewertung für die physische Domäne und für die IT-Domäne vorgenommen werden können. Im Ergebnis könnte das Bayes'sche Netz, so die Hypothese, zum einen das Wissen und die Annahmen über die Systemkomponenten in der physischen Security darstellen, zum anderen das Wissen sowie die Annahmen über die Systemkomponenten in der IT-Security abbilden. Im Rahmen dieser Idee kommt weiterhin die Frage auf, wie eine Metrik in ein entsprechendes Netz überführt und mit einer anderen Metrik bzw. einem anderen Netz zusammengebracht werden kann.

In diesem Kapitel wird dargelegt, wie der Transfer der TARA für CPS in ein Bayes'sches Netz gelingen kann. Für die Modellierung wird das Software-Tool GeNIe Academic verwendet (Bayesfusion, 2021). In einem Bayes'schen Netz in GeNIe wird allgemein zwischen „Chance Nodes" (zu dt. Zufallsknoten) und „Deterministic Nodes" (zu dt. deterministische Knoten) unterschieden. Zufallsknoten werden in der GeNIe-Software als Ovale abgebildet und beschreiben unsichere Variablen. Es können n Zustände definiert werden, wobei diesen Zuständen Wahrscheinlichkeiten zugewiesen werden. Werden Knoten miteinander verbunden, sodass zwischen Eltern- und Kindknoten differenziert werden kann, so ergeben sich für den Kindknoten bedingte Wahrscheinlichkeiten. Der Ursache-Wirkungs-Zusammenhang zwischen zwei Knoten wird durch die Pfeilrichtung definiert. Sie zeigt die Einflussrichtung „von (Ursache, Pfeilursprung) – nach (Wirkung, Pfeilende)" an. In GeNIe werden Wahrscheinlichkeiten in Wahrscheinlichkeitstabellen abgebildet. Deterministische Knoten werden als Doppelkreise oder Doppelovale dargestellt. Dabei handelt es sich entweder um konstant definierte Werte oder welche, die sich (algebraisch) aus den jeweiligen Zuständen der Elternknoten ergeben, d. h. ist der Wert eines Elternknotens bekannt, dann ist der Wert des deterministischen Kindknotens auch mit Sicherheit ($p = 1$)[74] bekannt.

Im Gegensatz zu Zufallsknoten bestehen die hinterlegten Wahrscheinlichkeitstabellen der deterministischen Knoten nur aus Nullen und Einsen. Deterministische Knoten bilden somit eine

[74] p steht für „Probability" (zu dt. Wahrscheinlichkeit).

rein binäre Betrachtung ab. Darüber hinaus können Werte-Knoten in GeNIe dargestellt werden. Werte-Knoten werden in Form von Sechsecken abgebildet und zeigen allgemein das erwartete Ergebnis aller Kombinationen von den im Modell dargestellten Entscheidungsalternativen, z. B. in Form eines monetären Verlustwertes, an. Darüber hinaus können in GeNIe Submodelle abgebildet werden. Sie fassen mehrere Knoten zu Einheiten zusammen und fördern die Übersichtlichkeit von Modellen. Geht von einem Submodell zu einem Knoten ein Doppelpfeil ab, dann bedeutet das, dass es in dem Submodell mindestens zwei Knoten gibt, die Elternknoten des Knotens in Wirkrichtung sind. Besitzt der Pfeil dagegen nur eine einfache Spitze, gibt es nur einen Elternknoten.

4.7 Überführung der Risikoanalyse in ein Bayes'sches Netz

Begonnen wird die Risikoanalyse mit dem Profiling der Assets. Für die Assets werden mögliche Schutzzielverletzungen (Vertraulichkeit, Verfügbarkeit und Integrität) festgelegt. Danach werden diesen Assets Damage Scenarios zugeordnet. In einem nächsten Schritt findet einerseits eine Zuordnung von Bedrohungsszenarien zu diesen Damage Scenarios statt, andererseits werden die Auswirkungen (Impacts) eines Damage Scenarios bewertet. Nach der Identifikation von Bedrohungsszenarien werden Angriffspfade (Implementierungsmöglichkeiten mit und ohne Wechselwirkung) analysiert. Aus IT-Perspektive wird die Ausbeutbarkeit dieser Angriffspfade bewertet. In der physischen Sicherheit wird die Vulnerabilität bewertet. Für Szenarien mit cyberphysischer Wechselwirkung wird der IT Impact in Physical Vulnerability herangezogen. Über eine Risikomatrix, welche den Impact mit der Bewertung der Angriffspfade[75] verknüpft, wird der Risiko-Score bestimmt.

Für die Bestimmung des erforderlichen CAL und PAL wird der Impact mit der Controllability tabellarisch verknüpft. Zur Reduktion der Assurance Levels können z. B. Maßnahmen definiert werden. Der Schritt der Risk Treatment Decision wird jedoch hier nicht weiter betrachtet. Bei der Risikoanalyse ist eine klare Struktur erkennbar, wo in den einzelnen Sub-Schritten eine punktuelle Verbindung von Bewertungsgrößen erfolgt. Der Risiko-Score ergibt sich beispielsweise aus einer Kombination des Impacts und der Bewertung der Angriffspfade. Er ist damit bedingt durch diese beiden Größen. Die Überlegung ist nun, diese kausalen Zusammenhänge in einem Bayes'schen Netz darzustellen. Hierfür wird der Ansatz der Rückwärtsplanung aus dem klassischen Projektmanagement verwendet (Friedrich et al., 2009, S. 47-87). Output-Größen am Ende eines Assessments sollen der Risiko-Wert und das Security-Assurance-Level (PAL bzw. CAL) sein. Das Security-Assurance-Level ist bedingt durch den Impact und die Controllability. Für die Übertragung in ein Bayes'sches Netz bedeutet das, dass es folgende Knoten gibt: Der Assurance Level-Knoten ist Kindknoten von Controllability und Impact. Zum Kindknoten des Risiko-Scores gehören die Elternknoten Impact und Bewertung des Angriffspfads (siehe Abbildung 52). Die Knoten sind hier deterministisch, da zu jeder Kombination der Ausprägungen der Elternknoten eine Ausprägung beim Kindknoten zugeordnet wird.

[75] Physische Sicherheit: Likelihood of Vulnerability (LoV), IT-Sicherheit: Likelihood of Exploitability (LoE).

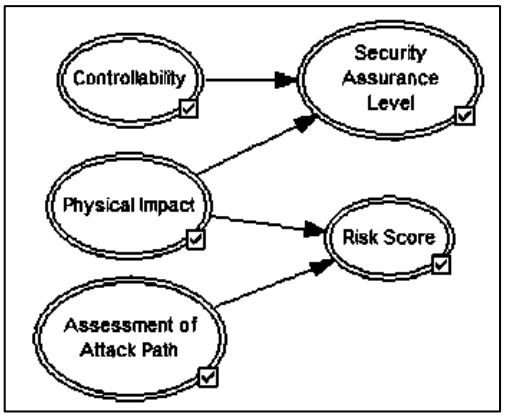


Abbildung 52: Bayes'sches Netz zur Bestimmung des Risiko-Scores und des Assurance Levels.
Quelle: Eigene Abbildung.

Die Bewertung des Angriffspfads erfolgt beispielsweise in der physischen Sicherheit über die Harnser-Skala für die physische Vulnerabilität (LoV). Die LoV-Kategorie wird über die vorliegende Kombination der logarithmierten Harnser-Scores von Protektion (P), Observation (O) und Intervention (I) bestimmt. Der LoV-Knoten ist damit bedingt durch die drei Knoten, die jeweils den log-Scores beschreiben (kurz: P-S, O-S und I-S). Über die beim LoV-Knoten hinterlegte Wahrscheinlichkeitstabelle können gemäß der erarbeiteten Vulnerabilitätsskalen alle Permutationen entsprechend einer LoV-Kategorie zugeordnet werden (siehe Abbildung 53). Alle Knoten werden auch hier als deterministisch definiert.

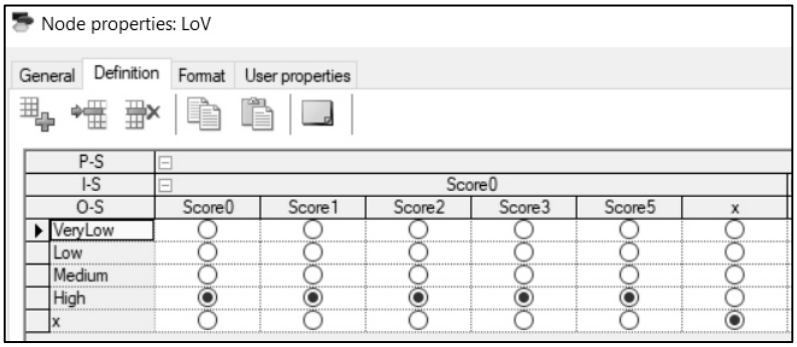


Abbildung 53: Auszug aus der Wahrscheinlichkeitstabelle LoV.
Quelle: Eigene Abbildung.

Ein logarithmierter Harnser-Score hängt vom Harnser-Score von „1" bis „5" (als Deskriptor „Very Low" bis „Very High") ab. Die Knoten der Harnser-Scores, P, O und I, sind folglich Elternknoten von P-S, O-S und I-S. Es erfolgt ein 1:1-Mapping von Harnser-Scores zu logarithmierten Scores. Insgesamt ergibt sich damit folgende Darstellung (siehe Abbildung 54):

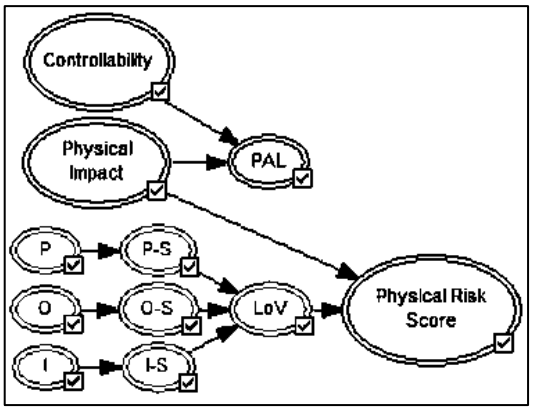


Abbildung 54: Bayes'sches Netz zur physischen Risikobewertung.
Quelle: Eigene Abbildung.

In gleicher Weise kann das Bayes'sche Netz zur IT-Risikobewertung aufgebaut werden (siehe Abbildung 55). Anstelle der Bewertungsgrößen Protektion, Observation und Intervention für die physische Vulnerabilität wird hier die CVSS-Metrik für die Bewertung der Likelihood of Exploitability verwendet. Bewertungsgrößen sind der Attack Vector (AV), die Attack Complexity (AC) und die Privileges Required* (PR*). Bei PR* handelt es sich um eine in dieser Arbeit vorgeschlagene Bewertungsgröße, welche sich aus den Größen Privileges Required (PR) und User Interaction (UI) zusammensetzt.

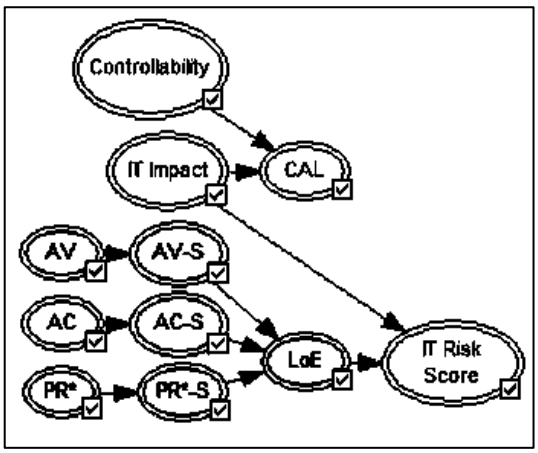


Abbildung 55: Bayes'sches Netz zur IT-Risikobewertung.
Quelle: Eigene Abbildung.

Sowohl die Scores in der physischen Security als auch die Scores in der IT-Security sind vom betrachteten Angriffspfad abhängig. Da in Bayes'schen Netzen für die Gewährleistung probabilistischer Konsistenz stets zwei Ausgänge bei Zufalls- und deterministischen Knoten definiert werden müssen, stellt sich die Frage, welcher Eintrag bei P, O und I erfolgt, wenn der Angriffspfad nicht auf „Ja = gegeben", sondern auf „Nein = nicht gegeben" gesetzt wird. Hierbei kann eine Behelfslösung, die „undefinierte" Ausprägung „x", für P, O und I eingeführt werden. Für „x" wird auch eine Ausprägung „x" bei den log-Score-Knoten festgelegt. Gibt es mindestens einen log-Score-Knoten, der der Ausprägung x annimmt, so ist die LoV, folglich auch das Assurance Level sowie der Risiko-Score „x". Angriffspfade sind gem. der TARA nach ISO/SAE 21434 bedingt durch ein Bedrohungsszenario (Threat Scenario, TS) (ISO/SAE, 2021b, S. 75-77). Dass ein Angriffspfad (AP) möglich ist, kann wie folgt ausgedrückt werden (siehe Gl. (36)):

$$P(AP|TS) = \begin{cases} 1 & if\ TS = 1 \\ 0 & else \end{cases} \tag{36}$$

Für jeden Angriffspfad gibt es jeweils eine Bewertung nach Abbildung 54 bzw. Abbildung 55, je nach Domäne. Die Controllability hängt von dem Bedrohungsszenario ab. Daraus ergibt sich am Beispiel der physischen Risikobewertung das Netz in Abbildung 56. Die Bezeichnungen sind beispielhaft zu sehen. Das IT-Security-Netz kann nach demselben Schema aufgebaut werden.

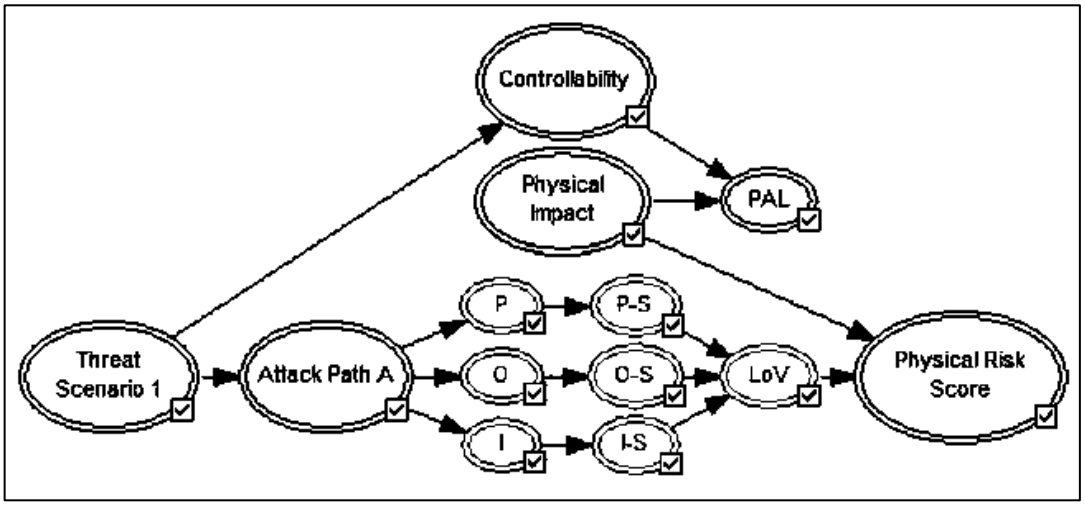


Abbildung 56: Bayes'sches Netz zur physischen Risikobewertung mit Angriffspfad und Bedrohungsszenario.
Quelle: Eigene Abbildung.

Das Netz aus Abbildung 56 kann darüber hinaus auch eine andere Ursache-Wirkungs-Richtung zwischen den Attack-Path- und Threat-Scenario-Knoten aufweisen. Anstelle, dass definiert wird „Der Angriffspfad ist bedingt durch ein einziges Threat Scenario", kann auch definiert werden: „Ein Threat Scenario ist gegeben, unter der Bedingung, dass es einen oder mehrere bestimmte Angriffspfade (AP_i) gibt" (siehe Gl. (37)).

$$P(TS|AP_i) = \begin{cases} 1 & if\ \exists \mathrm{i}\ (AP_i = 1) \\ 0 & else \end{cases} \tag{37}$$

Hier kann argumentiert werden, dass nur über einen Angriffspfad angegriffen werden kann, wenn es dafür eine entsprechende Bedrohung gibt. Nach der ISO/SAE 21434 können ferner mehrere Bedrohungsszenarien zu einem Damage Scenario zugeordnet werden (ISO/SAE, 2021b, S. 74). Der Knoten „Physical Impact" ist in dem Netz aus Abbildung 56 noch unbedingt, weil er von dem jeweiligen Damage Scenario abhängt.

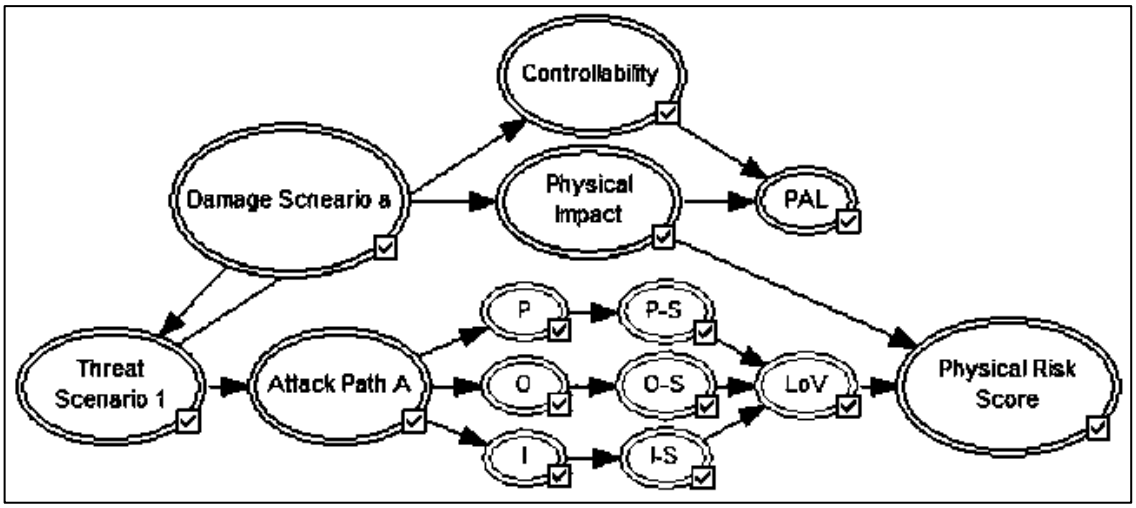


Abbildung 57: Bayes'sches Netz zur physischen Risikobewertung inkl. Damage Scenarios.
Quelle: Eigene Abbildung.

Ein Damage Scenario hängt vom vorliegenden Asset ab. Es tritt folglich ein, bedingt dadurch, dass das Asset vorliegt, andernfalls nicht. Zudem kann mit einem Damage Scenario die Möglichkeit einer Schutzzielverletzung von Vertraulichkeit, Verfügbarkeit und Integrität verbunden sein. Der Damage-Scenario-Knoten ist demnach Elternknoten des Knotens, der die Schutzzielverletzung beschreibt (siehe Abbildung 58).

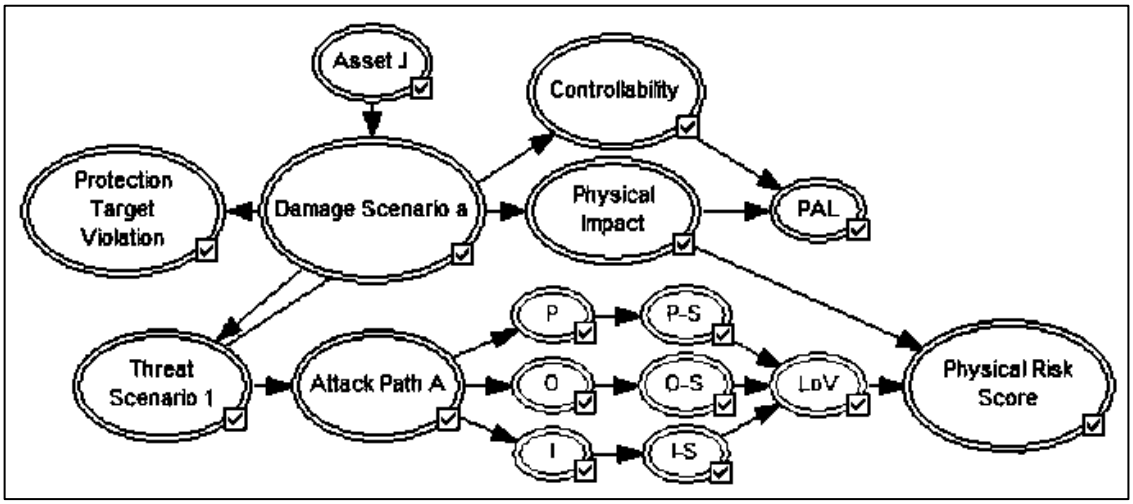


Abbildung 58: Bayes'sches Netz zur physischen Risikobewertung gem. der Risikoanalyse.
Quelle: Eigene Abbildung.

Das Bayes'sche Netz aus Abbildung 58 kann auf die Modellierung der IT-Security übertragen werden (siehe Abbildung 59).

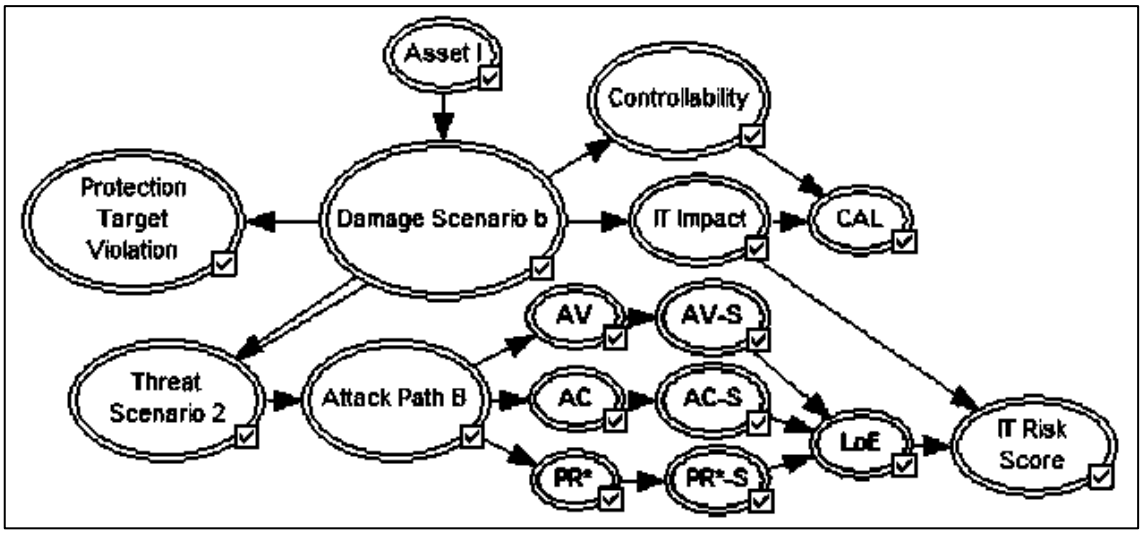


Abbildung 59: Bayes'sches Netz zur IT-Risikobewertung gem. der Risikoanalyse.
Quelle: Eigene Abbildung.

In einem letzten Schritt sind cyberphysische Wechselwirkungen in dem Bayes'schen Netz darzustellen. Angenommen, mit Attack Path B ist eine Wechselwirkung verbunden, welche einen Impact auf die Ausprägung physischer Sicherungsmechanismen hat. Zur Abbildung dieser Wechselwirkung wird der Knoten IT Impact on Physical Vulnerability eingeführt. Mit dem IT Impact on Vulnerability wird die Schwere der Kompromittierung physischer Sicherungsfunktionen durch einen erfolgreichen IT-Angriff bewertet. Diese Größe ist abhängig von der physischen Vulnerabilitätsbewertung ohne Berücksichtigung eines IT-Szenarios und der physischen Vulnerabilitätsbewertung unter Berücksichtigung eines IT-Szenarios. Wenn es einen IT Impact on Physical Vulnerability gibt, dann muss das betroffene Szenario aus der physischen Domäne nochmal bewertet werden (siehe P-, O- und I-Knoten in der Mitte der Abbildung 60).

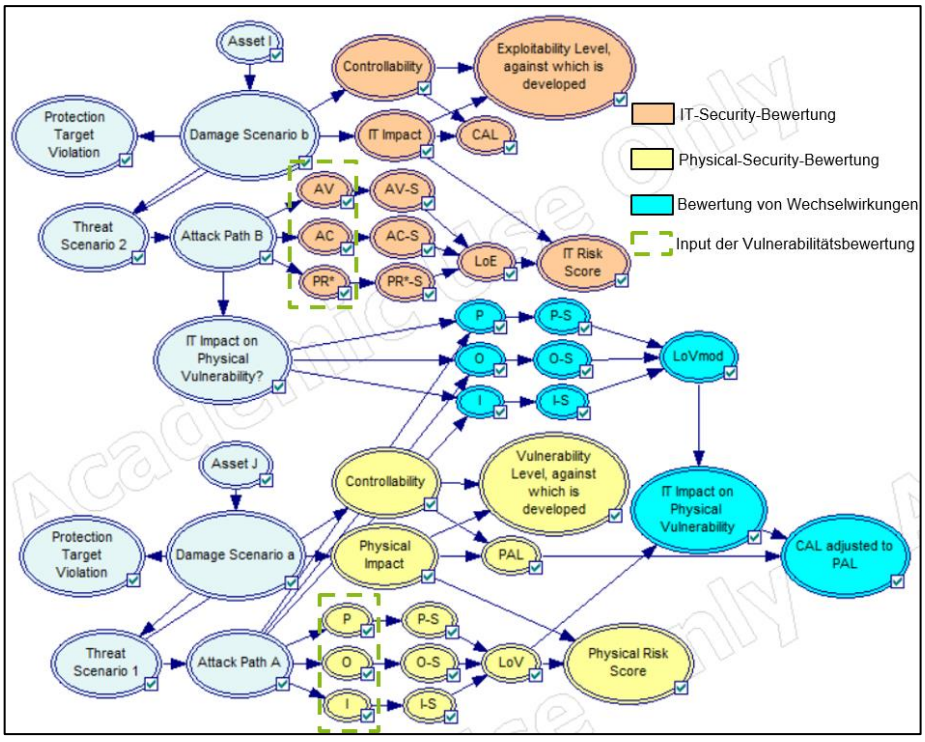


Abbildung 60: Bayes'sches Netz zur cyberphysischen Risikobewertung.
Quelle: Eigene Abbildung.

Der Knoten IT Impact on Physical Vulnerability ist Kindknoten des Angriffspfades B. Bei der nochmaligen Bewertung physischer Vulnerabilität gilt jedoch eine Besonderheit für die Knoten Protektion, Observation und Intervention des Bayes'schen Netzes: Die Berücksichtigung der gänzlichen Aushebelung der Bewertungsgrößen (siehe beispielhaft in Abbildung 61).

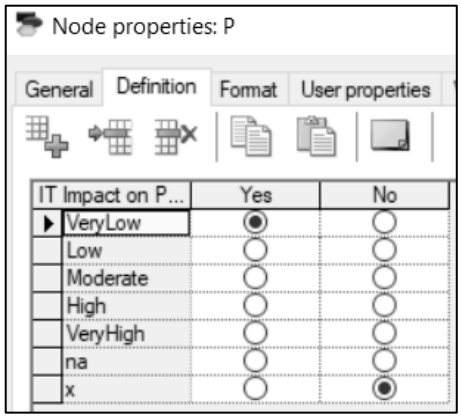


Abbildung 61: Ausprägungen des Protektionsknotens inklusive IT Impact on Vulnerability.
Quelle: Eigene Abbildung.

Aus der Kombination von Controllability und Impact kann auch, wie in dieser Arbeit in Kapitel 3.3.4 gezeigt, das Vulnerabilitäts-Level respektive das Exploitability-Level ermittelt werden, nach dem Produktentwickler entwickeln sollen. Controllability und Impact sind Elternknoten von „Exploitability Level, against which is developed" (IT-Security-Bewertung) bzw. „Vulnerability Level, against which is developed" (Physical-Security-Bewertung). Die Knoten „physisches Sicherheitslevel" und „IT Impact on Vulnerability" sind Elternknoten des Knotens „CAL adjusted to PAL". Der CAL des IT-Szenarios, welches einen Impact auf ein physisches Szenario hat, wird in Abhängigkeit von der Schwere der Kompromittierung physischer Sicherungsfunktionen mittels der Regel aus Kapitel 3.3.4 festgelegt. Zusätzlich zu den bisherigen Ausprägungen wird die Ausprägung „n. a." (not applicable) eingeführt. Tritt dieser Fall ein, ist der IT Impact on Physical Vulnerability grundsätzlich als „High" zu bewerten. Für die Knoten der Observation und Intervention wird die Ausprägung „n. a." ebenso ergänzt und mitgeführt (siehe Abbildung 62). Bei der Überführung der Deskriptoren „High", „Medium", usw. in einen Score wird ebenso „n. a." als Ausprägung hinzugefügt. Die „n. a." werden in der Wahrscheinlichkeitstabelle verknüpft: Nimmt der Elternknoten P die Ausprägung „n. a." an, tritt im Kindknoten P-S „n. a." ein.

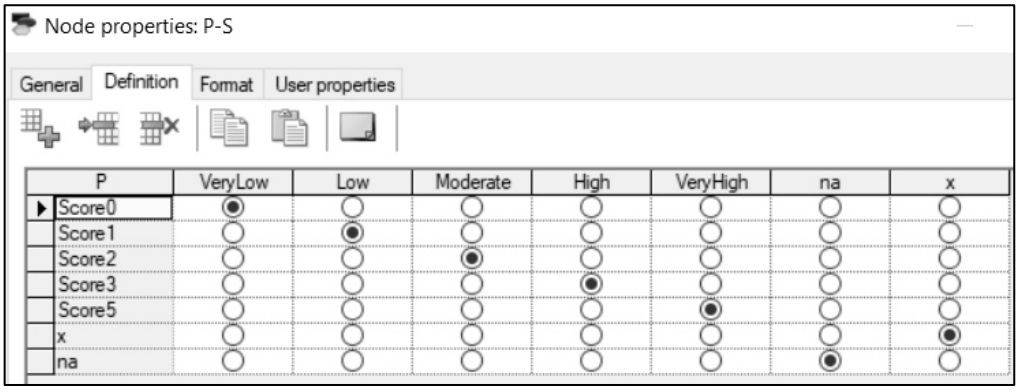


Abbildung 62: Mapping von Ausprägungen des Protektionsknotens zu Protektions-Scores.
Quelle: Eigene Abbildung.

Das Ergebnis der Score-Summe von P, O und I wird hier durch „LoVmod“[76] beschrieben. Auch im LoVmod-Knoten wird die Ausprägung „n. a.“ entsprechend ergänzt. In einem weiteren Schritt wird der IT Impact on Physical Vulnerability bestimmt. Hierfür wird die Beeinträchtigung der Vulnerabilität in vier Kompromittierungsgrade eingeteilt, wie in Kapitel 3.3.4 dargelegt. Abschließend kann der CAL, welcher für das IT-Szenario mit einem IT Impact on Physical Vulnerability zu bestimmen ist, gem. der vorgeschlagenen Regeln in Kapitel 3.3.4 ermittelt werden. Darüber hinaus kann zu jedem PAL und zu jedem CAL eine Vulnerabilitätskategorie geschrieben werden, nach welcher entwickelt werden soll. Die Zuweisung erfolgt, wie in Kapitel dargelegt (siehe Abbildung 63).

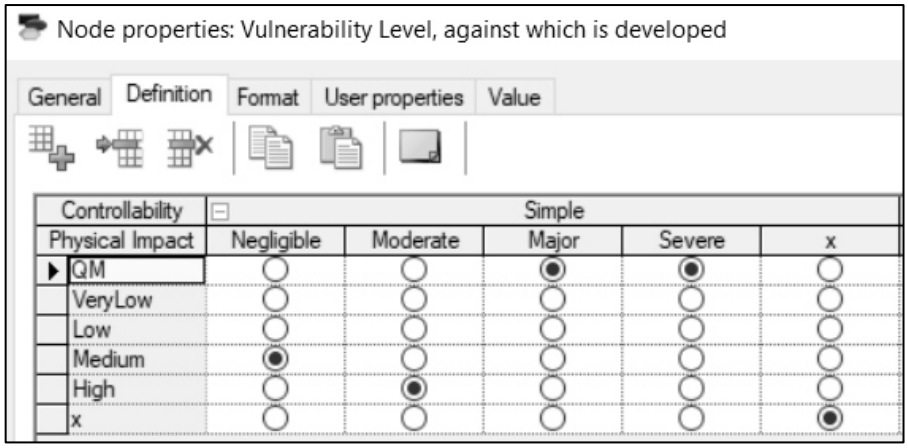


Abbildung 63: Mapping von der Kontrollierbarkeit und den Auswirkungen zu Vulnerabilitätslevels. Quelle: Eigene Abbildung.

Insgesamt zeigt sich, dass über ein Bayes’sches Netz Expertenwissen probabilistisch konsistent zusammengeführt werden kann. Herausfordernd ist in diesem Zusammenhang jedoch die Größe und Komplexität des Bayes’schen Netzes. Im Beispiel aus Abbildung 60 werden lediglich zwei Assets, zwei Damage Scenarios, zwei Threat Scenarios und zwei Attack Paths betrachtet. Wie in der TARA der ISO/SAE 21434 zu sehen, kann ein Risiko-Assessment jedoch viel umfangreicher sein. Das macht die Zugänglichkeit und die Nutzbarkeit für industrielle Anwender schwierig. Zur Durchführung einer Risikoanalyse fördert eine tabellarische Darstellung, wie sie z. B. in der ISO/SAE 21434 vorgeschlagen wird, die Übersichtlichkeit. Zusätzlich zu einem Risikoregister für das physische Risiko, wie in Harnser (2010, B6, S. 66) skizziert, können ein IT-Risikoregister bzw. ein cyberphysisches Risikoregister entsprechend den dargelegten Schritten zur Durchführung einer Risikoanalyse aufgebaut werden (siehe Abbildung 64). Die Genese eines Risikoregisters ist auch in der IT gängige Praxis (Ahmed et al., 2019).

[76] LoVmod = Likelihood of Vulnerability modified

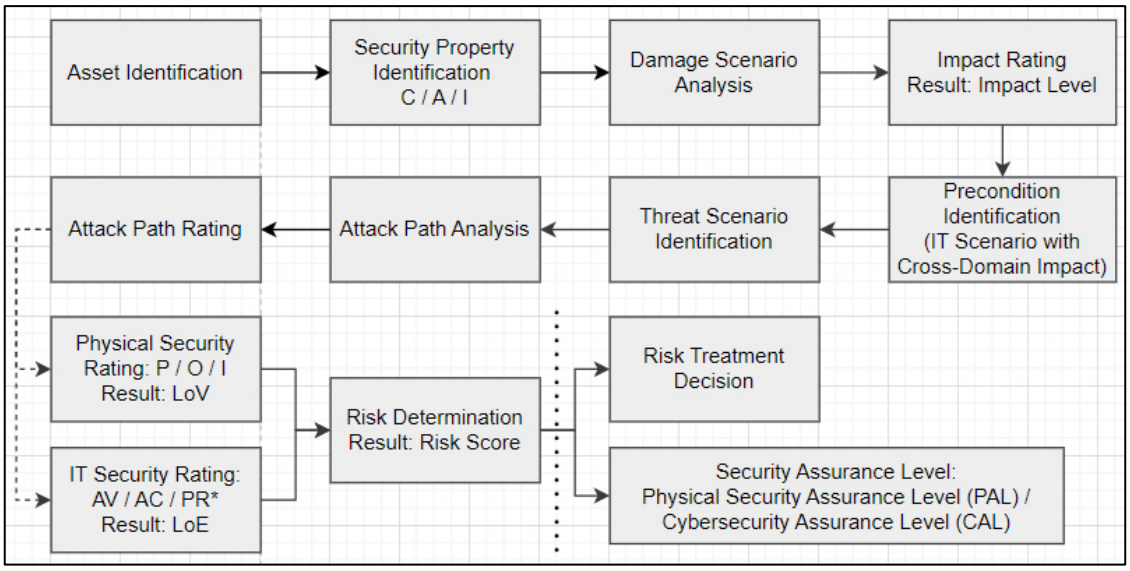


Abbildung 64: Schematische Darstellung der Arbeitsschritte zur Erstellung eines Risiko-Registers. Quelle: Eigene Abbildung in Anlehnung an ISO/SAE (2021b).[77]

4.8 Synthese von Modell-Input-Größen

Bei der Risikoanalyse mittels Bayes'scher Netze stellt sich die Frage nach der Abbildung von Unsicherheiten. Hierfür ist die Definition der Wahrscheinlichkeitsausprägungen der Modellparameter durch Experten notwendig. Expertenwissen kann in Bayes'schen Netzen grundsätzlich verwendet werden, um entweder die Struktur des Modells zu modifizieren, z. B., indem neue Knoten hinzugefügt werden und kausale Zusammenhänge detaillierter dargestellt werden, oder um die Zustände der Knoten mit Wahrscheinlichkeitsverteilungen zu versehen. Anstelle der deterministischen Knoten für die Protektion, Observation und Intervention in der physischen Sicherheit und der deterministischen Knoten für die Bewertungsgrößen Attack Vector, Attack Complexity und User Interaction in der IT-Sicherheit können Zufallsknoten verwendet werden. Das bedeutet, dass die Summe der Wahrscheinlichkeiten aller Zustände eines Knotens 100 % ergeben muss. Expertenwissen kann als subjektiver Grad der Überzeugung interpretiert werden (siehe Kapitel 2.6.1). Eine Wahrscheinlichkeit von 0.5 bedeutet beispielsweise, dass die interessierende Größe dem persönlichen Grad der Überzeugung eines Experten zufolge dort zu verorten ist. Eine Angabe kann von Experte zu Experte unterschiedlich sein (ESFA, 2021, S. 26), weil nicht alle Experten über dasselbe Wissen über einen Sachverhalt verfügen:

> 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, S. 55).

Die Überführung von Expertenwissen in eine Sicherheitsmetrik ist eine fundamentale Voraussetzung für die Nutzbarmachung des Bayes'schen Netzes der TARA. Auf der Webseite Bayesia.com (2021) wird eine Kombination aus der Cooke'schen und der Delphi-Methode vorgeschlagen, um systematisch Expertenwissen für Knoten eines Bayes'schen Netzes zu erheben. Der Ansatz sieht eine zweistufige Befragung von mehreren Experten durch einen Moderator vor. Zur Vorbereitung werden folgende Arbeitsschritte empfohlen (BayesiaLab, 2012):

[77] LoE = Likelihood von Exploitability, LoV = Likelihood of Vulnerability, A = Availability, C = Confidentiality, I = Integrity.

Durchführung von Brainstorming Sessions, um eine klare Definition der Zielsetzung des Bayes'schen Netzes zu erhalten; Identifikation der konzeptuellen Dimensionen, die mit dem Ziel verbunden sind; bei Bedarf: Probabilistisches Training (siehe auch EFSA (2014, S. 8)). Die Expertenbefragung ist in zwei Teile unterteilt. Im ersten Teil wird den teilnehmenden Experten der Kontext präsentiert und es werden die (Vor-)Bedingungen genannt, welche an die Ausprägungen des betrachteten Knotens geknüpft sind. Das können Assets, Damage Scenarios, Threat Scenarios sowie die dazugehörigen Attack-Path-Bewertungen sein.

Danach werden die Teilnehmer aufgefordert, ihre persönliche Einschätzung – Ihre subjektive Wahrscheinlichkeitsverteilung – abzugeben, wobei die Eintrittswahrscheinlichkeit der betrachteten Zustände zwischen null (0 %, niedrig) und eins (100 %, hoch) abgeschätzt werden soll. Darüber hinaus müssen die Experten angeben, wie sicher sie sich mit ihrer Aussage sind, d. h. sie geben ihr persönliches Vertrauen in die gemachte Angabe – ihre Konfidenz – zwischen null (0 %, geringes Vertrauen) und eins (100 %, hohes Vertrauen) an. Dieser Ansatz wird im Rahmen dieser Arbeit für die Risikoanalyse mittels Bayes'scher Netze adaptiert. Die Konfidenz wird als Mittel zur Gewichtung der Expertenaussagen verwendet, d. h., wenn probabilistische Angaben $x_1, \dots, x_i$ $(0 \leq x_1, \dots, x_i \leq 1)$ von Experten mit den Konfidenzen $c_1, \dots, c_i$ $(0 \leq c_1, \dots, c_i \leq 1)$ gemacht werden, dann errechnet sich der gewichtete Mittelwert zu Gl. (38)[78]:

$$m = \frac{\sum_i x_i \times c_i}{\sum_i c_i} = \frac{x_1 \times c_1 + x_2 \times c_2 + \cdots + x_i \times c_i}{c_i + c_2 + \cdots + c_i} \tag{38}$$

Je höher die Konfidenz, desto größer ist auch die Gewichtung der jeweiligen Expertenaussage. Das bedeutet, Expertenaussagen, die unsicher sind, werden aufgrund der Gewichtung weniger in der Gesamtbetrachtung berücksichtigt (siehe als Beispiel Tabelle 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**

Tabelle 70: Ausgefülltes Template zur Erhebung von Expertenwissen am Beispiel des Protektions-Scorings an der Barriere X.
Quelle: Eigene Tabelle in Anlehnung an Bayesia.com (2021).

[78] Der Ansatz, eine Expertenaussage zu gewichten, ist auch z. B. in Lichte et al. (2018) vorhanden: Scores werden gewichtet und in einen quantitativen Ausdruck überführt.

Grundsätzlich werden Ergebnisse nach der ersten Session im Plenum offengelegt und diskutiert. In einer zweiten Session wird die Aufforderung zur Angabe subjektiver Wahrscheinlichkeiten zum selben Sachverhalt wiederholt. Dieser Schritt dient dazu, dass Experten ihre Meinung nach der Sichtung der Ergebnisse bei Bedarf nochmal schärfen können, sodass die Konfidenz in die Expertenaussage erhöht wird. Die Herangehensweise sieht nicht vor, Experten durch Kalibrierungsfragen des Moderators zu qualifizieren, wie das klassischerweise beim klassischen Cooke'schen Ansatz empfohlen wird (BayesiaLab, 2012) (siehe Kapitel 2.6.1).[79] Die Experten bewerten in diesem Ansatz das Vertrauen in ihre Einschätzung selbst. Daraus folgt auf der einen Seite ein reduzierter Aufwand für den Moderator, Experten zu qualifizieren bzw. zu disqualifizieren, gleichzeitig muss der Moderator darauf vertrauen, dass die Experten kompetent und ehrlich genug sind, die Konfidenz in ihre Einschätzung bewerten zu können.

Die Formulierung des Kontextes und die Beschreibung der zu definierenden Zielgrößen durch den Moderator können Experten bei der Angabe eines Konfidenzwerts unterstützen. Je schärfer eine konkrete Zielgröße beschrieben und je konkreter die Rahmenbedingungen, welche auf die Zielgröße einwirken, benannt sind, desto förderlicher ist dies für die Destillierung des gewünschten Expertenwissens. Die Wahl von Experten, welche zu einem bestimmten Sachverhalt eine fundierte Aussage treffen können, liegt beim Moderator. Dies hat zur Folge, dass das Ermessen des Moderators, Experten auszuwählen, indirekt die Aussagekraft des Ergebnisses beeinflusst. Unter der Annahme, dass die Risikobewertung und damit die Erhebung von Expertenwissen von einem qualifizierten Prüfer durchgeführt werden, ist der Gewichtungsansatz eine skalierbare, einfache Möglichkeit, mehrere Experten zu befragen, um Expertenangaben mittels der Gewichtung von subjektiven Wahrscheinlichkeiten mit den dazugehörigen Konfidenzangaben auf quantitativem Wege zu aggregieren. Aus diesem Grund wird dieser Ansatz für die Anwendung des Bayes'schen Netzes der TARA vorgeschlagen. Um die gesuchten Zielgrößen den Experten möglichst zugänglich zu machen, kann eine Möglichkeit sein, Leitfragen in Anlehnung an die What-If-Technik, wie in Kapitel 4.1 vorgestellt, zu formulieren: „Unter der Voraussetzung, dass das System […] – wie wahrscheinlich ist es, dass die Protektion Ausprägung x hat?".

Kausale Zusammenhänge, welche für die Bewertung des Sachverhalts wichtig sind, sind möglichst einfach durch den Moderator zu artikulieren. Die Leitfragen werden von dem Moderator vor der Erhebung vorbereitet. Diese Art der Erhebung von Expertenwissen ist damit ein „Mixed-Methods"-Ansatz, bei dem zunächst eine Frage formuliert (qualitativer Teil) und diese von Experten in quantitativer Form beantwortet wird (Vogl, 2017). Diese wird dann in das Modell als Input transferiert. Für die Bewertung der Auswirkung von erfolgreichen IT-Angriffen auf die physischen Sicherheitsfunktionen kann der Mixed-Method-Ansatz ebenso angewandt werden. Durch die Applikation des vorgeschlagenen Erhebungsansatzes auf die TARA können unterschiedliche Experteneinschätzungen berücksichtigt werden. Mittels des Mixed-Method-Ansatzes ist es möglich, eine Spreizung von Vulnerabilitätsergebnissen aufzudecken. Diese kann zustande kommen, wenn verschiedene Experten z. B. die Protektion, Observation und Intervention oder den Attack Vector, die Attack Complexity oder die Privileges Required* unterschiedlich ranken. Das Heranziehen unterschiedlicher Expertenmeinungen kann dazu beitragen, aufseiten des Betreibers eines MAS das Investment in Sicherheitsmaßnahmen zu überdenken, wenn eine festgelegte Risikoakzeptanzschwelle nicht erreicht wird, beispielsweise: „zu mindestens 95 % muss die Risikostufe „2" vorliegen".

[79] Methoden zur Verbesserung der Kalibrierung werden z. B. in Hubbard et al. (2016, S.137-154) dargelegt.

5 Diskussion

Die vorliegende Arbeit schlägt einen methodischen Ansatz zur Durchführung einer domänenübergreifenden Sicherheitsbewertung von CPS am Beispiel von MAS in Mobilitätsanwendungen vor. Mithilfe des methodischen Ansatzes ist es möglich, die Beeinträchtigung physischer Sicherungsmechanismen durch erfolgreiche IT-Angriffe zu bewerten. Die Analyse bisheriger Ansätze zur domänenübergreifenden Sicherheitsbewertung zeigt, dass Auswirkungen von erfolgreichen IT-Angriffen auf die physische Sicherheit bisher kaum in Bedrohungsanalysen und Risikobewertungen Berücksichtigung finden. Bei bestehenden Sicherheitsstandards für Kraftfahrzeuge, wie z. B. ISO 26262 oder ISO/SAE 21434, sind quantitative Methoden zur domänenübergreifenden Sicherheitsbewertung wenig zu finden, welche Unsicherheiten in der Beschreibung der Sicherheitsfähigkeit einbeziehen können. Anknüpfend an bestehende Ansätze zur Vulnerabilitätsbewertung können die Eigenschaften eines physischen Systems wirksamkeitsbasiert durch die Protektion, Observation und Intervention beschrieben werden. Für die Beschreibung der Eigenschaften eines IT-Systems fehlt ein objektiver Wirkmechanismus für die Darstellung der Schutzmaßnahmen zur Minderung der Vulnerabilität, weswegen die Sicherheitseigenschaften nur auf einer abstrakten Ebene ausgedrückt werden können. Szenario-beschreibende Charakteristiken, wie z. B. die Komplexität, die Erforderlichkeit von Privilegien und die Erforderlichkeit von Benutzerinteraktionen, werden zur Beschreibung der Sicherheitsfähigkeit von IT-Systemen verwendet.

Bei der domänenübergreifenden Bewertung von physischer Security und IT-Security gibt es Herausforderungen, die auf inkompatible Metriken zur Bewertung der Vulnerabilität eines Systems zurückzuführen sind. In der physischen Sicherheit werden semi-quantitative Ansätze zur Vulnerabilitätsbewertung verwendet, wie z. B. in Harnser (2010). Es gibt jedoch auch quantitative Ansätze zur Vulnerabilitätsbewertung, wie beispielsweise nach Lichte et al. (2016). In der IT-Sicherheit sind dagegen vor allem qualitative und semi-quantitative Ansätze präsent. Ein Beispiel für einen semi-quantitativen Ansatz ist insbesondere CVSS (First.org, 2022). Weil in der IT-Security-Bewertung ein objektiver Wirkmechanismus zur Beschreibung der Sicherheitsfähigkeit fehlt (Jacobs et al., 2019), kann eine Zusammenführung von physischer Sicherheit und IT-Sicherheit auf wirksamkeitsbasierter Ebene und damit auf Modellebene nicht erfolgen. Das ist ein Problem, welches noch zu lösen ist.

Die Unterschiedlichkeit der Bewertungssysteme aus den Domänen Physical Security und IT Security führt zur ersten Forschungsfrage: Wie kann eine domänenübergreifende Bewertung funktionieren? Für die Beantwortung dieser Forschungsfrage werden weitere Forschungsfragen formuliert, um das Problem der domänenübergreifenden Bewertung in einzelne Bestandteile zu zerlegen. Aus wissenschaftlicher Sicht stellt sich zunächst die Frage nach der Möglichkeit des Vergleichs von Metriken. Diese Frage wird gestellt, weil am Beispiel der physischen Sicherheitsbewertung gezeigt werden kann, dass zwar sowohl mit der Hanser-Metrik nach Harnser (2010) als auch mit der Vulnerabilitätsmetrik nach Lichte et al. (2016) physische Vulnerabilität bestimmt werden kann, sich jedoch die Ergebnisse in Teilen stark voneinander unterscheiden. Das führt zu der Forschungsfrage: Wie können Inkompatibilitäten zwischen zwei Metriken aus der physischen Sicherheitsbewertung quantifiziert und durch Maßnahmen bzw. Forderungen gemindert werden?

In dieser Arbeit wird zur Beantwortung dieser Frage eine strukturierte Analyse der Harnser-Metrik (2010) und der Vulnerabilitätsbewertung nach Lichte et al. (2016) aus der physischen Sicherheitsbewertung durchgeführt. Für die Vulnerabilitätsbewertung nach Lichte et al. (2016) wird in Anlehnung an Garcia (2005) die Bezeichnung Interventionsfähigkeitsmetrik (In-

tervention Capability Metric, ICM) gewählt. Bei der Harnser-Metrik werden Protektion, Detektion und Intervention zwischen „1" und „5" gescort und addiert. Mittels der ICM wird das Zeitspiel zwischen der Eindringzeit eines Angreifers und der Reaktionszeit eines Verteidigers quantitativ abgebildet. Bewertungsgrößen sind Protektion, Observation und Intervention. Zunächst fällt auf, dass in Lichte et al. (2016) eine andere Bezeichnung für den zweiten Bewertungsparameter gewählt wird als in Harnser (2016). Der Argumentation in Lichte et al. (2016) folgend ist die Detektion ein Ereignis, welches sich aus Protektionsanteilen und Observationsanteilen zusammensetzt; folglich würde gem. dieser Annahme die Protektion zweimal in die Vulnerabilitätsbewertung nach Harnser (2010) einbezogen werden: Einmal über das Scoring der Protektion und einmal über das Scoring der Detektion. Darüber hinaus stellt sich die Frage, inwieweit Experten in der Lage sind, zusammengesetzte Ereignisse zu bewerten. Als Argumentationsgrundlage wird folgende Begründung vorgebracht: Ein Experte muss erst die Input-Paramater einer Vulnerabilitätsmetrik festlegen und in eine Vulnerabilitätsmetrik einspeisen, um eine Aussage über das Vulnerabilitätsniveau treffen zu können. Eine direkte Angabe der Vulnerabilität durch einen Experten ohne vorherige Anwendung einer Vulnerabilitätsmetrik ist deswegen schwierig. Diese Argumentation ist Ausgangspunkt für den Vorschlag, die Bewertungsgröße „Detektion" in der Harnser-Metrik durch die Bewertungsgröße „Observation" zu ersetzen, sodass bei der Harnser-Metrik nun Protektion, Observation und Intervention gescort werden.

Um das Harnser-Scoring mit der quantitativen ICM vergleichen zu können, wird vorgeschlagen, dass die Vulnerabilitäts-Scores nach Harnser auf einer Skala in Kategorien einsortiert und diesen Kategorien vermutete Wahrscheinlichkeitsintervalle zugewiesen werden. Darüber hinaus werden zu den Scores „1" bis „5" korrespondierende Zeitstufen in der ICM definiert. In der ICM werden Protektion, Observation und Intervention mit probabilistischen Dichtefunktionen hinterlegt, damit Unsicherheiten in der Beschreibung von Sicherungsmaßnahmen berücksichtigt werden können. Für die Protektion, Observation und Intervention wird in der ICM eine Normalverteilung zugrunde gelegt, d. h. jede der Stufen „1" bis „5" wird zu einem Mittelwert und einer Standardabweichung für die drei Bewertungsgrößen zugewiesen. Es wird davon ausgegangen, dass nur eine Barriere mit den Eigenschaften der Protektion, Observation und Intervention bewertet wird. Aus Anwendersicht ist zu fragen, wie eine sinnvolle Stufendefinition für die ICM aussehen kann. Je nach Anwendungsfall kann eine Definition von „kleinen Zeitsprüngen" von Stufe zu Stufe impraktikabel sein, ggf. wäre auch die Annahme von anderen Verteilungen anstelle der Normalverteilung anwendungsnäher. In dieser Arbeit wird die Normalverteilung als exemplarisches Beispiel herangezogen und erklärt, dass Experten die Stufen in der ICM beliebig in Abhängigkeit des vorliegenden Anwendungsfalls setzen können.

Unter Berücksichtigung unterschiedlicher metrischer Randbedingungen, wie z. B. verschiedene Arten der Score-Aggregation aufseiten der Harnser-Metrik und der Variation von Streuungen aufseiten der ICM-Metrik, werden Vulnerabilitätsniveaus mit beiden Metriken ermittelt und gegenübergestellt. Die Gegenüberstellung der Vulnerabilitätsergebnisse erfolgt nach den insgesamt (5 x 5 x 5 =) 125 betrachteten Permutationen. Die Vulnerabilitätswerte werden in sortierter Form insbesondere nach den Harnser-Mittelwerten respektive ICM-Werten innerhalb der Harnser-Plateaus, welche sich aufgrund gleicher Score-Summen bei unterschiedlichen Permutationen herausbilden, dargestellt. Im Ergebnis resultieren aus den geplotteten Vulnerabilitätswerten für beide Metriken objektive Vulnerabilitätsfunktionen. Nach der Auswertung der Ergebnisse werden Maßnahmen identifiziert, damit mit beiden Metriken vergleichbare Vulnerabilitätsniveaus erzeugt werden können.

In dieser Arbeit wird die Angleichung der Vulnerabilitätsniveaus als quantitative Konformität bezeichnet. Zu den Maßnahmen gehören die Erhöhung der Streuung aufseiten der quantitativen Metrik und die Anpassung der Harnser-Vulnerabilitätsskala an den Kurvenverlauf der

ICM-Funktion. Es zeigt sich, dass die Bewertungsgrößen zur Beschreibung des Wirkmechanismus in konsistente Scores überführt werden können, sodass die unterschiedlichen Bewertungen nach Harnser (2010) und Lichte et al. (2016) hinsichtlich der Vulnerabilitätseinstufung kompatibel gemacht werden können. Zu beachten ist, dass lediglich eine Anpassung des Harnser-Scorings an bestimmte ICM-Varianten vorgenommen wird, hinter denen klar definierte Zeitstufen (angenommene Mittelwerte und Standardabweichungen für Protektion, Observation bzw. Intervention) stehen.

Zusammenfassend kann für die physische Sicherheit die Güte der Harnser-Metrik durch eine Anpassung an die Vulnerabilitätsergebnisse der ICM geschärft und verifiziert werden. Das ist möglich, weil angenommen wird, dass mit der quantitativen Bewertung auf Basis der ICM nach Lichte et al. (2016) reale Vulnerabilitätsstufen dargestellt werden können. Die quantitative Bewertungsmetrik wird nicht derart angepasst, dass mit ihr die Scoring-basierten Ergebnisse nach Harnser (2010) abgebildet werden können. Gemäß den Überlegungen in Gigerenzer (2014, S. 44-47, 130-131) soll die Realität vielmehr mit einem vereinfachten Algorithmus (einer „guten, vereinfachenden Faustregel") bewertet werden können. Im Kontext der physischen Sicherheitsbewertung bedeutet das beispielsweise: Die Ergebnisse der ICM („Realität") sollen durch ein Scoring („Faustregel") abgebildet werden. Anstatt die Parameter der quantitativen ICM einem mit Mängeln behafteten Scoring anzupassen, ist es notwendig, Forderungen an das Scoring zu definieren, sodass mit den unterschiedlichen Bewertungsmetriken nach Harnser (2010) und Lichte et al. (2016) gleiche Vulnerabilitätsstufen erzeugt werden können. Eine Vorgehensweise zur metrischen Analyse wird folglich so entwickelt, dass quantifiziert werden kann, wie gut eine nicht quantitative Metrik ist und inwieweit bestimmte Maßnahmen zu weniger Inkompatibilitäten zwischen dem Scoring und der quantitativen Metrik führen. Darauf aufbauend kann es ermöglicht werden, Metrik-Versionen, wie beispielsweise in Harnser (2010) und Lichte et al. (2016) vorgeschlagen, zu vergleichen und eine Aussage darüber zu treffen, unter welchen Voraussetzungen eine konkrete Art und Weise der Zusammenführung von Expertenwissen in einem Scoring besser ist als eine andere.

In dieser Arbeit wird die Angleichung des Harnser-Scorings mit unterschiedlichen Skalen an konkrete ICM-Varianten durchgeführt. Es zeigt sich, dass die Intervallbreiten pro Skalenkategorie allgemein größer werden, je weniger Skalenkategorien es gibt. Das bedeutet: Wird z. B. eine viergliedrige Harnser-Skala quantitativ konform zu einer ICM-Variante gemacht, so sind die vermuteten Wahrscheinlichkeitsintervalle hinter diesen vier Kategorien deutlich breiter als im Falle z. B. einer dreizehngliedrigen Harnser-Skala, welche zu derselben ICM-Variante quantitativ konform gemacht wird. Wenn eine Harnser-Skala an mehrere ICM-Varianten angepasst wird, dann werden die vermuteten Wahrscheinlichkeitsintervalle pro Skalenkategorie ebenso größer. Zudem überschneiden sich die Intervallgrenzen pro Skalenkategorie zunehmend. Dies hat zur Folge, dass das Harnser-Scoring eine mitunter große Range an Vulnerabilität vermuten lässt. Hier ist zu fragen, inwiefern es Produktentwicklern, die eine physische Sicherheitsbewertung durchführen, hilft, wenn im Ergebnis eine Vulnerabilität von z. B. 0.2 bis 0.8 vermutet wird. Je größer die vermuteten Wahrscheinlichkeitsintervalle hinter den Skalenkategorien, desto schwieriger wird die Entscheidung bzgl. des Investments von knappen Ressourcen in Sicherheitsmaßnahmen, um physische Vulnerabilität zu reduzieren. Das ist ein Nachteil der Nutzung von Harnser-Skalen, die wenige Skalenkategorien besitzen und an mehrere ICM-Varianten angepasst werden. In diesem Zusammenhang ist es eine Herausforderung, eine Balance zwischen der Praktikabilität (Anzahl an verwendeten Skalenkategorien) und der Verwertbarkeit von Ergebnissen des Scorings (bezogen auf die Intervallbreite des vermuteten Vulnerabilitätsniveaus) zu finden.

In IT-Security-Assessments sind Scoring-basierte Ansätze weit verbreitet. Es wird vereinfacht gesagt, dass die „1" schlecht ist und die „5" gut. Bewertungsgrößen sind Szenario-beschreibende Parameter, wie z. B. Angriffsvektor, Angriffskomplexität, usw. Sie werden im Falle CVSS (First.org, 2022) über eine Metrik ohne einen hinterlegten objektiven Wirkmechanismus zur Beschreibung des Effekts von Maßnahmen auf die Vulnerabilitätsreduktion miteinander verbunden, sodass im Ergebnis eine Vulnerabilitäts-Einstufung resultiert, die nicht quantitativ verifizierbar ist. Das bedeutet, dass in der IT-Security eine solche metrische Schärfung, wie sie am Beispiel der Harnser-Metrik und Interventionsfähigkeitsmetrik demonstriert wird, schwerlich durchführbar ist. Neueste Überlegungen verfolgen den Ansatz, die im CVSS vorhandenen Bewertungsgrößen im CVSS als hintereinandergeschaltete Barrieren zu interpretieren und die dazugehörigen Scores zu logarithmieren. Die Transformation wird vorgeschlagen, weil es sich bei der Verrechnung der CVSS-Parameter um eine multiplikative Verknüpfung handelt. Gleichzeitig löst die Logarithmierung Probleme mit quantitativen Skalen verschiedener Größenordnung auf, denen die Bewertungsparameter auf einer einheitlichen Skala, z. B. „1" bis „4", zugeordnet werden. Zur Auflösung des Problems bei der Verrechnung von Ordinalwerten muss das Scoring-System, wie am Beispiel der Harnser-Metrik und der ICM gezeigt, hinsichtlich der vermuteten Wahrscheinlichkeitsintervalle, welche hinter den Skalenkategorien stehen, an Vulnerabilitätswerte einer quantitativen Metrik mit objektivem Wirkmechanismus angepasst werden. Da eine quantitative Metrik mit objektivem Wirkmechanismus beim CVSS fehlt, wird in der Arbeit die Frage aufgeworfen, wie bewertet werden kann, ob Vorschläge zur Veränderung der CVSS-Bewertungsmetriken Besserungen bringen.

Jetzt gibt es auf der einen Seite die klassischen Scoring-Ansätze, z. B. CVSS, und auf der anderen Seite Barriere-basierte Scoring-Ansätze, z. B. bei Braband (2019), in dem die Transformation der Exploitability-Beiträge (nach CVSS) zu log-Scores vorgeschlagen wird. In dieser Arbeit kann auf analytischem Wege gezeigt werden, dass die Anwendung einer log-Transformation auf eine multiplikative Scoring-Metrik Verwerfungen reduziert. Das setzt jedoch voraus, dass wahre Risikobeiträge und die Skalierung zwischen den Zahlenwerten der wahren Risikobeiträge bekannt sind. Um die Güte metrischer bzw. modelltechnischer Modifikationen prüfen zu können, bedarf es einer quantitativen Metrik, mithilfe derer die in Braband (2019) gemachten Überlegungen übertragen und nachgerechnet werden können. Das CVSS der IT-Security gibt das aber nicht her, weil es an Möglichkeiten fehlt, richtig zu quantifizieren und wirksamkeitsbasiert zu bewerten. Im Rahmen der Analyse in Termin et al. (2022) werden die Überlegungen aus der IT-Security in der physischen Security nachgeahmt, um die Plausibilität der gemachten Überlegungen im IT-Security-Assessment zu untersuchen. Die Resultate waren jedoch nicht eindeutig.

Darüber hinaus wird erklärt, dass z. B. die Barriere des Attack Vectors zur Beschreibung des Kontexts eines Angriffs aus logischen Gründen in jedem Fall eine Ausprägung besitzen muss. Sie darf nicht null sein: Ohne einen Attack Vector gibt es keinen Bedrohungskontext und damit auch keine Möglichkeit zur Ausbeutung einer Schwachstelle eines Systems. Die Barrieren User Interaction und Privileges Required besitzen im Gegensatz zu den anderen Bewertungsgrößen die Ausprägung „None". Nehmen User Interaction und Privileges Required diese Ausprägung an, gibt es im Grunde keine Barrieren. Weiterhin haben die Bewertungsparameter unterschiedlich tiefe Ausprägungsstufen: Der Attack Vector besitzt vier, die Attack Complexity zwei, die Privileges Required drei und die User Interaction zwei. Die Ausprägungsstufen der Bewertungsparameter innerhalb des CVSS sind folglich unterschiedlich. Es werden in dieser Arbeit Bestrebungen unternommen, die Ausprägungsstufen so anzupassen, dass sie erstens stets einen Aktivierungszustand beschreiben und dass zweitens jeder CVSS-Parameter gleich viele Ausprägungsstufen besitzt.

Abschließend wird in Anlehnung an die Überlegungen in Braband (2019) diskutiert, wie die Bewertungsgrößen Privileges Required (PR) und User Interaction (UI) in eine Bewertungsgröße überführt werden können. Das wird getan, weil PR und UI dasselbe aus unterschiedlichen Blickwinkeln beschreiben: Es sind in irgendeiner Form Privilegien erforderlich, um einen bestimmten Angriff auszuführen. Anknüpfend an Dürrwang et al. (2021) wird vorgeschlagen, die Bewertungsgrößen PR und UI zu einer Bewertungsgröße PR* zusammenzuführen, die die vier Ausprägungen „Execute", „Read", „Write" und „Full Control" besitzt. Die Zusammenführung von PR und UI wird gemacht, um einerseits die Inkompatibilität zwischen dem Barriere-basierten CVSS-Modell und der CVSS-Metrik, wie in Braband (2019) eingeführt, aufzulösen. Zugleich bietet die Zusammenführung den Vorteil, dass sowohl in der IT-Security-Bewertung als auch in der physischen Security-Bewertung je drei Bewertungsparameter bewertet werden. Nachteilig ist jedoch, dass die vorgeschlagene Spezifizierung des Bewertungsparameters PR* nicht quantitativ bestätigt werden kann, weil hierfür eine quantitative Metrik zur Justierung der PR*-Exploitability-Beiträge, anders als in der physischen Sicherheitsbewertung, fehlt.

Basierend auf den in dieser Arbeit entwickelten Ansätzen zur Angleichung einer semi-quantitativen Vulnerabilitätsmetrik (Harnser-Metrik) an eine quantitative Vulnerabilitätsmetrik (ICM) und zur Bewertung von Verbesserungsvorschlägen für eine semi-quantitative Metrik ohne hinterlegten, objektiven Wirkmechanismus (Barriere-basierter CVSS-Ansatz) wird die erste Forschungsfrage erneut aufgegriffen: Wie kann eine domänenübergreifende Bewertung funktionieren? In dieser Arbeit werden die Vulnerabilitätsbeschreibungen und Vulnerabilitätsbewertungen in der physischen Sicherheit und in der IT-Sicherheit eingehender analysiert. Im Rahmen der Analyse kann festgestellt werden, dass ein pfadbasiertes Vulnerabilitätsmodell in beiden Security-Domänen abbildbar ist: In der physischen Sicherheit kann ein Angriffspfad (Szenario) durch eine Kombination von (disjunkten) physischen Barrieren in Reihe bis zum Asset beschrieben werden. In der IT-Security stellt ein Angriffspfad auch eine Kombination aus (disjunkten) Barrieren in Reihe dar, welche ein Angreifer bis zu einem Asset zu überwinden hat. Diese Barrieren können jedoch ausbeutbare Schwachstellen besitzen. Ein physischer Angreifer kann aus einer Kombination von Barrieren wählen, um an ein physisches Asset zu gelangen. Ein IT-Angreifer dagegen kann aus einer Barrieren-Schwachstellen-Kombination wählen, um ein IT-Asset zu erreichen.

In beiden Security-Domänen kann Risiko durch das Produkt aus der Bedrohung, der Vulnerabilität und den Auswirkungen beschrieben werden. Diese Dreiteilung kann auf eine Zweiteilung, Vulnerabilität multipliziert mit den Auswirkungen, reduziert werden, wenn zwei Bedingungen vorliegen:

1. Die Beiträge von der Bedrohung, der Vulnerabilität und den Auswirkungen sind völlig disjunkt voneinander. Zusätzlich wird mit dieser Idealisierung strenge Unabhängigkeit zwischen den drei Beiträgen angenommen.
2. Die Bedrohungswahrscheinlichkeit wird zu 100 % (p = 1.00) angenommen. Damit einher geht, dass die Sicherheitsfähigkeit eines Systems im Angriffsfall betrachtet wird.

Das physische Risiko kann damit durch „$R = V \cdot I$" beschrieben werden, das IT-Risiko entsprechend durch „$R = E \cdot I$" (E := Exploitability, IT-Vulnerabilität). Für die Zusammenführung der physischen Auswirkungen und der IT-Auswirkungen wird in dieser Arbeit vorgeschlagen, eine harmonisierte Skala z. B. mit Scores von „1" bis „4" zu definieren. Es wird angenommen, dass jede Score-Stufe derart durch einen Deskriptor beschrieben werden, dass sich sowohl physische Auswirkungen als auch IT-Auswirkungen wiederfinden lassen. Experten geben anschließend monetäre Verlustwerte für jede Score-Stufe von „1" bis „4" an. Jedes Score-/Verlustwert-Paar kann als Punkt in ein Koordinatensystem übertragen werden. Die Scores von „1" bis „4" auf der Abszisse werden den Verlustwerten auf der Ordinate zugeordnet. Die eingetragenen

Punkte können durch eine mathematische Funktion beschrieben werden. Wird ein Auswirkungs-Score in die mathematische Funktion eingespeist, resultiert die dazugehörige monetäre Auswirkung als Funktionswert. Die mathematische Funktion der Auswirkungen wird an späterer Stelle bei der Zusammenführung der Risikobewertungen in der physischen Sicherheit und in der IT-Sicherheit benötigt.

Zusätzlich zu den Auswirkungen ist die Vulnerabilität (physische Security) bzw. Exploitability (IT-Security) zu bewerten. Wenn in der physischen Sicherheit eine Barriere und ein Asset als Referenzmodell angenommen werden, dann kann die physische Vulnerabilität durch das Zusammenspiel von Protektion, Observation und Intervention an dieser Barriere bewertet werden. Wenn in der IT-Sicherheit eine Barriere mit einer Schwachstelle als Referenzmodell angenommen wird, dann kann die IT-Vulnerabilität (Exploitability) z. B. durch die Exploitability-beschreibenden Aspekte des CVSS, Attack Vector, Attack Complexity, Privileges Required und User Interaction, bewertet werden. In Braband (2019) wird vorgeschlagen, die CVSS-Scores zu logarithmieren und auf einer Exploitability-Skala in Kategorien einzusortieren. Um zuallererst eine Angleichung der Scorings aus der physischen Sicherheit am Beispiel Harnser und der IT-Sicherheit am Beispiel CVSS zu ermöglichen, wird die Durchführung der log-Transformation der Scores für die Vulnerabilitäts- bzw. Exploitability-Beiträge vorgeschlagen. Die Dimensionierung in beiden Scorings wird über eine gemeinsame Basis normiert. Für die quantitative Konformität der Harnser-Skala an konkrete ICM-Varianten spielt es keine Rolle, wie die bereits willkürlichen Harnser-Scores zustande kommen. In Anlehnung an ISO/SAE 21434 wird eine viergliedrige Bewertungsskala für die Vulnerabilität entwickelt, welche z. B. mittels der Deskriptoren „Very Low“, „Low“, „Medium“ und „High“ beschrieben werden kann (ISO/SAE, 2021b, S. 78). Das bietet den Vorteil, dass auf verfahrenstechnischer Ebene die Vulnerabilitätsbewertung in der physischen Security und die Bewertung in der IT-Security gleich aufgebaut sind. Sowohl die physische Vulnerabilität als auch die IT-Vulnerabilität werden log-Scoring-basiert ermittelt. Das Ergebnis wird auf einer viergliedrigen Skala einsortiert.

Eine Harnser-Skala zur Bewertung der physischen Vulnerabilität wird entwickelt, welche aus vier Kategorien besteht und quantitativ konform zur ICM 1 ist. Zu jeder Skalenkategorie kann ein Vulnerabilitäts-Score für die semi-quantitative Scoring-Metrik von „1“ bis „4“ geschrieben werden. Die vermuteten Wahrscheinlichkeitsintervalle, welche hinter den Kategorien der Harnser-Skala stehen, bestehen aus einem Lower Interval Limit (LIL) sowie einem Upper Interval Limit (UIL). Demzufolge besteht ein Vulnerabilitäts-Score aus zwei Anteilen, LIL und UIL. Jedes Vulnerabilitäts-Score-/LIL-Wert-Paar und Vulnerabilitäts-Score-/UIL-Wert-Paar kann als Punkt interpretiert und in ein Koordinatensystem eingetragen werden. Diese Punkte können jeweils für die LIL-Werte und UIL-Werte durch eine mathematische Funktion für die Vulnerabilität abgebildet werden. Diese mathematischen Funktionen werden in dieser Arbeit für die Beschreibung der Vulnerabilität verwendet.

Für die Exploitability-Bewertung wird ebenfalls eine viergliedrige Skala entwickelt, welche sich auf dem CVSS-basierten Ansatz in Braband (2019) stützt. Insofern angenommen wird, dass die Rücktransformation der Score-Summen wahren Exploitability-Beiträgen entspricht, können hinter die Kategorien der Exploitability-Skala ebenso vermutete Wahrscheinlichkeitswerte (LIL und UIL) geschrieben werden. Der quantitative Exploitability-Wert, welcher zu dem niedrigsten Score einer Kategorie gehört, kann als untere vermutete Wahrscheinlichkeit für die Exploitability (LIL) definiert werden, der höchste Score dagegen als obere vermutete Wahrscheinlichkeit für die Exploitability (UIL). Zu jeder Skalenkategorie kann ein Exploitability-Score für die semi-quantitative Scoring-Metrik von „1“ bis „4“ geschrieben werden. Auch der Exploitability-Score besteht aus zwei Teilen, LIL und UIL. Jedes Exploitability-Score-/LIL-Wert-Paar und Exploitability-Score-/UIL-Wert-Paar kann als Punkt interpretiert und in ein Koordinatensystem eingetragen werden. Diese Punkte können jeweils für die LIL-Werte und UIL-Werte durch eine

mathematische Funktion für die Exploitability abgebildet werden. Diese mathematischen Funktionen werden in dieser Arbeit für die Beschreibung der Exploitability verwendet.

In einem letzten Schritt werden die mathematischen Funktionen für die Vulnerabilität bzw. für die Exploitability und die Auswirkungen in die Risikogleichungen („R = V · I“ und „R = E · I“) eingesetzt und anschließend logarithmiert. Die Basis, zu welcher der Impact-Beitrag logarithmiert wird, wird beispielhaft zu 10 für beide Bewertungen gewählt. Die Basis, zu welcher der Vulnerabilitäts-Beitrag und der Exploitability-Beitrag jeweils logarithmiert werden, wird in Anlehnung an Braband (2019) zu 0.6 für beide Bewertungen gewählt Im Ergebnis resultieren je zwei Risikofunktionen für das physische Risiko und für das IT-Risiko, R_{LIL} und R_{UIL}. Mit der ersten Risikofunktion wird beispielsweise das physische Risiko unter Annahme der LIL-Werte für die Vulnerabilität berechnet. Mit der zweiten Risikofunktion wird das physische Risiko wird dann entsprechend unter Annahme der UIL-Werte für die Vulnerabilität berechnet. Werden z. B. Scores für die Vulnerabilität sowie die Scores für die Auswirkungen in die erste Risikofunktion (R_{LIL}) eingesetzt und das Ergebnis anschließend mittels der Umkehrfunktion des Logarithmus rücktransformiert, dann ergibt sich ein quantitativer Wert für das Risiko. Dieser Wert entspricht einem wahren Risikoniveau.

In dieser Arbeit kann gezeigt werden, dass durch (geschicktes) Logarithmieren Verwerfungen innerhalb multiplikativer Scoring-Metriken reduziert werden können. Insgesamt kann gezeigt werden, dass es möglich ist, die Risikobewertungen anzugleichen, indem eine Harmonisierung der Skalen der Risikobeiträge durchgeführt wird. Das funktioniert jedoch nur, wenn die wahren Werte der Risikobeiträge tatsächlich bekannt sind. Außerdem wird angenommen, dass die Exploitability-Scores oder die Vulnerabilitäts-Scores für die multiplikative Risiko-Scoring-Metrik nicht durch Experten unmittelbar angegeben werden können. Vielmehr ist sind die Anwendung einer Vulnerabilitätsmetrik in der physischen Sicherheitsbewertung und die Anwendung einer Exploitability-Metrik in der IT-Sicherheitsbewertung erforderlich, um ein Vulnerabilitätsniveau bzw. Exploitability-Niveau festlegen zu können. Der vorgeschlagene Ansatz funktioniert, wenn die vermuteten Wahrscheinlichkeitsintervalle, welche hinter den Skalenkategorien stehen, an objektive Vulnerabilitäts- bzw. Exploitability-Stufen angepasst werden können. Das setzt in beiden Security-Domänen jeweils eine quantitative Metrik voraus, mit welcher objektive Vulnerabilitätswerte respektive Exploitability-Werte ermittelt werden können. In der IT-Security ist eine solche Metrik jedoch schwerlich zu finden.

Damit eine domänenübergreifende Sicherheitsbewertung gelingen kann, bedarf es einer Möglichkeit zur Bewertung von Szenarien aus der physischen Sicherheit und der IT-Sicherheit, zwischen denen es Wechselwirkungen geben kann. Für die Bewertung des Schweregrads einer Wechselwirkung zwischen IT-Szenarien und physischen Szenarien wird die Bewertungsgröße IT Impact on Physical Vulnerability (ITIPV) eingeführt. Der ITIPV beschreibt die Beeinträchtigung von physischen Sicherheitsfunktionen durch ein IT-Szenario. Diese Beeinträchtigung resultiert in der Erhöhung physischer Vulnerabilität. Zur Bestimmung des IT Impacts auf die physische Vulnerabilität wird die Durchführung zweier Berechnungen vorgeschlagen. Das physische Szenario wird einmal ohne und einmal unter Berücksichtigung einer Wechselwirkung von Experten bewertet, um über den ITIPV die Schwere der Wechselwirkung zu bemessen. Die Vulnerabilitäts-Scores werden in beiden Fällen auf der viergliedrigen Bewertungsskala einsortiert und es werden die Kategorien für beide Szenarien miteinander verglichen. Diese Vorgehensweise wird als sinnvoll erachtet, weil weder die Harnser-Metrik noch die ICM die Berücksichtigung von IT-Bedrohungen kennt. Weil die Skala der Harnser-Metrik mittels konkreter ICM-Varianten quantitativ konform gemacht wird, kann aus der Bewertung der Beeinträchtigung physischer Sicherheitsfunktionen über das Scoring auf ein reales Vulnerabilitätsniveau geschlossen werden.

Darüber hinaus werden Möglichkeiten aufgezeigt, wie Security-Level hergeleitet werden können, sodass sich die Produktentwicklung an einem Vulnerabilitätsniveau, das hinter einem konkreten Level steht, orientieren kann. Security-Level legen den Umfang fest, um Komponenten oder Systeme vor bestimmten Angriffen zu schützen. In der ISO/SAE 21434 (IT-Security) beispielsweise wird der Cybersecurity Assurance Level (CAL) für die Klassifizierung von Sicherheitsstufen verwendet. Die Einstufung des CAL erfolgt über eine tabellarische Zuordnung vom Angriffsvektor zu den Auswirkungen eines Bedrohungsszenarios. Es wird zunächst vorgeschlagen, die Auswirkungsskala – wie bei der Zusammenführung der Risikobewertungen in der physischen Sicherheit und in der IT-Sicherheit dargelegt – für beide Domänen gleich aufzubauen und in Anlehnung an ISO/SAE 21434 viergliedrig aufzustellen. Dieser Schritt wird als notwendig erachtet, damit sich sowohl Auswirkungen von Bedrohungsszenarien aus der physischen Security als auch Auswirkungen von Bedrohungsszenarien aus der IT-Security in der Auswirkungsskala wiederfinden lassen. Gleichzeitig schafft eine normalisierte Auswirkungsskala eine Voraussetzung, um erstens Risikoniveaus in der physischen Security und in der IT-Security besser vergleichen zu können und zweitens Security-Level für beide Security-Domänen in gleicher Weise zu bestimmen.

Zuallererst wird überlegt, die physischen Sicherheitslevel (Physical Assurance Level, PAL) wie die CAL (Cybersecurity Assurance Levels) gem. ISO/SAE 21434 zu bestimmen: Der Angriffsvektor (Kontext eines Angriffs) wird tabellarisch mit den Auswirkungen verknüpft. Nicht alle IT-Angriffsvektoren sind eine Teilmenge der physischen Angriffsvektoren, d. h. hier sind nur PAL-Einstufungen für die Kombination des Attack Vectors „Physical" mit den Auswirkungen zulässig. In der CAL-Matrix sind die Impact-/Attack-Vector-Paare „Major-Physical" und „Moderate-Physical" mit demselben CAL (CAL „1") besetzt. Das bedeutet, dass zwei Auswirkungsstufen demselben Sicherheitslevel zugeordnet werden. Zu fragen ist nun, wie eine mögliche PAL-Matrix definiert werden kann. Es wird in dieser Arbeit festgestellt, dass die PAL-Matrix und die CAL-Matrix unter der Voraussetzung einer tabellarischen Verknüpfung des Attack Vectors mit den Auswirkungen unterschiedlich aufgebaut sein müssen, damit sich in beiden Bewertungen z. B. Security-Level „1" bis „4" wiederfinden lassen. Es wird aufgrund dessen nach einer Möglichkeit gesucht, die Security-Level-Matrix so aufzubauen, dass sie für beide Security-Domänen gleich ist.

Danach wird versucht, die Matrix zur Bestimmung der Security Level für die physische Sicherheit und für die IT-Sicherheit wie die Automotive Safety Integrity Levels (ASIL) Matrix aus der ISO 26262 aufzubauen: Die Auswirkungen und die Frequency werden gegen die Controllability tabellarisch verknüpft, d. h. jedes Triplet (bestehend aus einem Auswirkungs-, Frequency- und Controllability-Rating) entspricht einer Sicherheitseinstufung. Die Controllability ist eine Größe aus ISO 26262 und beschreibt die Möglichkeit, einen (weiteren) Schaden zu vermeiden, wenn eine gefährliche Situation eintritt. Diese Bewertungsgröße wird für den Bereich der Security als Möglichkeit zur Postvention interpretiert: Inwiefern kann ein Betreiber eines Systems nach einem Angriff Schadensbegrenzung betreiben, z. B. durch Notfallpläne, die Remote-Entziehung von Berechtigungen, etc.? Da hinter einem Sicherheitslevel ein Vulnerabilitätsniveau stehen soll, darf die Frequency nicht z. B. durch das Vulnerabilität-Rating substituiert werden. Ebenso ist es auch mit Herausforderungen verbunden, wenn anstelle der Frequency die Bedrohungswahrscheinlichkeit geschrieben wird. Das liegt darin begründet, dass Bedrohungen epistemisch sind. Die Durchführung eines Angriffs unterliegt der Willkür eines Angreifers. Zudem liegt bei Security-Bewertungen, in denen Szenarien betrachtet werden, die nicht aufgetreten sind, keine Evidenz vor, um statistische Abschätzungen zu machen.

Aus diesem Grund wird stattdessen eine Matrix entwickelt, in der die Auswirkungen eines Bedrohungsszenarios mit der sog. Controllability ins Verhältnis gesetzt wird. Jedes einzelne Aus-

wirkungs-/Controllability-Paar entspricht einer physischen respektive IT-Sicherheitsstufe zwischen „1“ (niedriges Level) und „4“ (hohes Level). Die Levels „1“ bis „4“ werden in einem weiteren Schritt zu Vulnerabilitätsniveaus zugeordnet: Level „4“ wird das niedrigste Vulnerabilitätslevel „Very Low“ zugewiesen, usw. Hinter den vier Vulnerabilitätslevels werden in dieser Arbeit die vermuteten Wahrscheinlichkeitsintervalle der quantitativ konformen, viergliedrigen Harnser-Metrik zur Variante ICM 1 (moderate Streuungen) angenommen. Die Wahl einer viergliedrigen Skala liegt darin begründet, dass der internationale Standard ISO/SAE 21434 eine viergliedrige Einstufung von Vulnerabilität vorschlägt. Die Vulnerabilitätslevels können grundsätzlich von Anwendungsfall zu Anwendungsfall unterschiedlich definiert werden. Hierzu ist die Konsultation von Experten aus der Produktentwicklung erforderlich.

Für die Zuweisung von Sicherheitslevels zu physischen Szenarien und IT-Szenarien, zwischen denen es domänenübergreifende Wechselwirkungen gibt, wird in dieser Arbeit vorgeschlagen, im Falle einer Beeinträchtigung physischer Sicherheitsmechanismen das IT-Szenario mit einem gleichen Level wie beim physischen Szenario oder einem höheren Level zu besetzen. Aus wirtschaftlichen Gründen wird eine Regel eingeführt, die Anwender dabei unterstützen können, das Sicherheitslevel für das IT-Szenario unter Berücksichtigung des ITIPV zu modifizieren. Der CAL wird in Abhängigkeit von der Schwere einer Wechselwirkung hochgestuft. Die erarbeiteten Scoring-Systeme für die physische Sicherheit und IT-Sicherheit werden anschließend als Teil einer Risikobewertung in eine strukturierte Vorgehensweise zur Bedrohungsanalyse und Risikobewertung (Threat Analysis and Risk Assessment, TARA) nach ISO/SAE 21434 überführt. Diese wird anschließend in ein Bayes’sches Netz übertragen, um zu zeigen, dass das Expertenwissen über die Sicherheitsfähigkeit eines cyberphysischen Systems innerhalb der Domänen Physical Security und IT Security probabilistisch konsistent verknüpft werden kann. Zudem wird gezeigt, dass in einem Bayes’schen Netz auch Wechselwirkungen abgebildet werden können. Darüber hinaus werden Möglichkeiten zur Synthese von Modell-Input-Größen anhand von Expertenwissen über einen Gewichtungsansatz dargelegt. Experten, die mehr Vertrauen in ihre Wahrscheinlichkeitsangaben haben als andere, werden stärker im Gesamtergebnis berücksichtigt als Experten, die weniger Vertrauen in ihre Wahrscheinlichkeitsangaben haben. Das ist insofern nützlich, da so mehrere Experteneinschätzungen in das Bayes’sche Netz einspeist werden. Es zeigt sich, dass die Komplexität des Netzes im Falle mehrerer Angriffsszenarien die Praxistauglichkeit dieser Methode einschränken kann.

Die tabellarische Zusammenfassung der Risikoanalyseschritte in einem Risikoregister, wie z. B. in Harnser (2010, B6, S. 66) zu sehen, wird anstelle der Anwendung eines Bayes’schen Netzes empfohlen, weil das Bayes’sche Netz unübersichtlich werden kann, wenn viele Bedrohungsszenarien (mit domänenübergreifenden Auswirkungen) abgebildet werden. Im Gegenzug zur tabellarischen TARA bietet die Anwendung des Bayes’schen Netzes jedoch den Vorteil, dass die Spreizung in den Ergebnissen einer Risikobewertung aufgrund unterschiedlicher Expertenmeinungen zu allen Input-Größen aufgedeckt werden kann. Während in der tabellarischen TARA nur ein Experten-Rating notiert wird, können in dem Bayes’schen Netz durch Anwendung des präsentierten Gewichtungsansatzes beliebig viele Expertenmeinungen berücksichtigt werden. Insofern nach einer Expertenbefragung und Einspeisung der Expertenaussagen in das Netz festgestellt wird, dass z. B. 90 % Risiko-Score „1“ vorliegt und zu 10 % Risiko-Score „2“, kann seitens der Produktverantwortlichen überlegt werden, ob eine Akzeptanz möglich ist oder die Notwendigkeit einer detaillierteren Analyse besteht. Nach der domänenübergreifenden Risikobewertung können, wie in ISO/SAE 21434 vorgeschlagen, folgende Schritte durchgeführt werden: Festlegung der Art der Risikobehandlung (Security Claims), Definition von Security-Zielen (Security Goals), Definition von Security-Maßnahmen (im Falle der Risikobehandlungsoption Mitigation) und Ableitung von Sicherheitsanforderungen erfolgen.

Zusammenfassend gibt es zur Reduktion von Verwerfungen innerhalb einer Metrik verschiedene Möglichkeiten. Wie in dieser Arbeit demonstriert, kann eine Möglichkeit darin bestehen, die Verteilung von Zahlenwerten über eine Transformation zu ändern. Eine weitere Option ist, den Informationsgehalt von Risikobeiträgen respektive Vulnerabilitätsbeiträgen aufzubereiten und die Konsistenz von Bewertungsschritten zu überprüfen. Sinn und Zweck dieser Aufbereitung ist es, z. B. ungültige oder fehlerbehaftete Werte und Schritte in der Risikobewertung aufzudecken und zu entfernen. In der klassischen Harnser-Metrik beispielsweise werden Protektion, Detektion und Intervention gescort. Die Detektion ist jedoch ein zusammengesetztes Ereignis, welches aus Protektionsanteilen und Observationsanteilen besteht. Zu hinterfragen ist, ob Experten zusammengesetzte Ereignisse ohne eine bekannte, darunterliegende Metrik sofort bewerten können.

Zudem würde bei einem Scoring von Protektion, Detektion und Intervention die Protektion zweimal einfließen, einmal über das Scoring der Protektion sowie einmal über das Scoring der Detektion. Durch eine Substitution des Bewertungsparameters Detektion durch die Observation werden die elementaren Bestandteile des physischen Wirkmechanismus bewertet. Inkompatibilitäten zwischen zwei Sicherheitsmetriken aus unterschiedlichen Domänen können reduziert werden, indem zunächst die Risikobeiträge priorisiert und durch (geschickt gewählte) Annahmen aus der Risikobetrachtung ausgeklammert werden. Wenn z. B. Disjunktheit zwischen den Risikobeiträgen Bedrohung, Vulnerabilität und Auswirkungen in der Risikobeschreibung „R = Bedrohung x Vulnerabilität x Auswirkungen“ angenommen und definiert wird, dass strenge Unabhängigkeit zwischen den Risikobeiträgen vorliegen, dann darf multipliziert werden. Insofern die Sicherheitsfähigkeit eines Systems im Angriffsfall bewertet wird (Bedrohungswahrscheinlichkeit = 100 %), können die mit epistemischen Unsicherheiten behafteten Bedrohungsanteile im Rahmen der vorgeschlagenen Vorgehensweise zur Durchführung einer prospektiven Risikoanalyse ausgeklammert werden. Weitere Maßnahmen zur Reduktion von metrischen Inkompatibilitäten können sein:

1. Die Metriken werden normalisiert, d. h. die Beiträge einer Risikometrik bzw. Beiträge einer Vulnerabilitätsmetrik werden auf eine vergleichbare Skala gebracht. Eine Möglichkeit, Zahlenwerte auf eine vergleichbare Skala zu bringen, ist die Anwendung einer geeigneten Datentransformation. Ein Bespiel dafür ist die Min-Max-Normalisierungsmethode: Zahlenwerte werden so umgewandelt, dass sie allesamt in einem gemeinsamen Bereich liegen, z. B. zwischen 0 und 1 oder zwischen 0 und 1000. Eine weitere Möglichkeit besteht auch in der logarithmischen Transformation, wie in dieser Arbeit demonstriert.
2. Die Metriken werden in eine gemeinsame Risikobeschreibung konvertiert, z. B. „Risiko = (Bedrohung x) Vulnerabilität x Auswirkungen“ und eine gemeinsame Einheit, beispielsweise für die Vulnerabilität [%] und für die Auswirkungen [Euro]. Diese Maßnahmen verbessern den Vergleich von zwei Metriken.
3. Eine neue Sicherheitsmetrik wird entwickelt, welche im eine Idealfall quantitative, wirksamkeitsbasierte Bewertung zulässt und Informationen aus beiden Metriken verbinden kann. Risikobeiträge werden bei dieser neuen Metrik auf einer gemeinsamen Skala abgebildet.

In Tabelle 71 werden Möglichkeiten und Grenzen der domänenübergreifenden Zusammenführung von Physical Security und IT Security aufgeführt. Der erarbeitete systematische Ansatz leistet einen Beitrag, Werkzeuge zur Durchführung einer domänenübergreifenden Risikobewertung bereitzustellen.

Möglichkeiten	Grenzen
Anpassung der Skalen(einteilung), Anpassung der Dimensionierung und Ausprägungen der Scores, Vereinheitlichung des Bewertungsprozesses (siehe Kapitel 3, 4).	Kein domänenübergreifendes Modell mit darunterliegender, wirksamkeitsbasierter Metrik realisierbar, weil der Wirkmechanismus in der IT fehlt (siehe Kapitel 3.3.1).
Überführung quantitativer Parameter in konsistente Scores möglich (siehe Kapitel 3.1).	Güte der Ergebnisse auf Basis des IT-Bewertungssystems nicht mit Metrik aus der IT validierbar (siehe Kapitel 3.3.3, 8.1).
Domänenübergreifende Sicherheitsanalyse mit Wirkrichtung IT-physisch abbildbar (siehe Kapitel 3.3.4, 4.3).	Emulierter, Barriere-basierter Ansatz schwerlich anwendbar in der Praxis. Protektion, Observation und Intervention müssen auf Performanz-lastige Barrieren zurückgeführt werden (siehe Kapitel 3.2.2).
Probabilistisch konsistente Zusammenführung des Wissens über die Sicherheitsfähigkeit von physischen und IT-Systemelementen in einem Bayes'schen Netz. Darüber hinaus kann Expertenwissen in das Netz eingespeist werden (siehe Kapitel 4.7, 4.8).	Domänenübergreifende Sicherheitsanalyse mit Wirkrichtung physisch-IT nicht abbildbar (siehe Kapitel 3.3.4).
Angleichung der Skalenstufen der Vulnerabilitätsbeiträge aus der physischen Sicherheitsbewertung an die Skalenstufen der Vulnerabilitätsbeiträge aus der IT-Sicherheitsbewertung (siehe Kapitel 3.3.3).	Angleichung der Skalenstufen der Vulnerabilitätsbeiträge aus der IT-Sicherheitsbewertung an die Skalenstufen der Vulnerabilitätsbeiträge aus der physischen Sicherheitsbewertung nur bedingt möglich (siehe Kapitel 5).
Herleitung von Sicherheitslevels für die Domänen Physical Security und IT Security (siehe Kapitel 3.3.4).	Beliebige Komprimierung oder Erweiterung von Skalenkategorien, sodass stark unterschiedliche Dimensionierung in Skalen angeglichen werden können, ist schwerlich darstellbar (siehe Kapitel 3.2.3).
Festlegung von Sicherheitslevels für ein IT-Szenario, wenn es einen Impact auf die physische Vulnerabilität hat (siehe Kapitel 3.3.4)	

Tabelle 71: Möglichkeiten und Grenzen in der domänenübergreifenden Zusammenführung. Quelle: Eigene Tabelle.

6 Zusammenfassung und Anschlussforschung

In dieser Forschungsarbeit wird insgesamt ein Mixed-Methods- bzw. Mixed-Metric-Ansatz zur Risikobewertung von MAS eingeführt. Im Sinne eines kontinuierlichen Verbesserungsprozesses kann der generische Ansatz entsprechend der jeweiligen Bedrohungslage repetitiv verwendet werden. Es zeigt sich, dass eine domänenübergreifende Bewertung unter Berücksichtigung der Wirkrichtung von IT-Szenarien auf physische Szenarien möglich ist, weil in der physischen Sicherheit Vulnerabilität wirksamkeitsbasiert mit einer quantitativen Metrik, z. B. der ICM nach Lichte et al. (2016), bewertet werden kann. Andersherum ist die domänenübergreifende Bewertung nicht möglich, weil in der IT-Security eine wirksamkeitsbasierte, quantitative Bewertung schwerlich zu finden ist, d. h., wenn nach einem CAL entwickelt wird, kann kein hinreichender Nachweis erfolgen, dass die Exploitability, welche hinter einem CAL stehen könnte, auch tatsächlich erreicht wird. In der physischen Sicherheit ist das dagegen möglich.

Diese Forschungsarbeit hat einen Lösungsweg identifizieren können, wie die Harnser-Metrik nach Harnser (2010) an die ICM nach Lichte et al. (2016) angepasst werden kann, sodass aus beiden Bewertungen vergleichbare Vulnerabilitätseinstufungen resultieren. Inkompatibilitäten zwischen diesen beiden Metriken können reduziert werden, indem die Harnser-Skalenkategorien durch vermutete Wahrscheinlichkeitsintervalle erweitert und diese an quantitative Vulnerabilitätswerte nach der ICM angepasst werden. Verwerfungen innerhalb der Harnser-Metrik (Harnser 2010) und innerhalb des CVSS (First.org, 2022) werden qualitativ analysiert und durch geeignete Maßnahmen reduziert. Aufseiten der Harnser-Metrik wird z. B. der Bewertungsparameter Detektion durch den Bewertungsparameter Observation ersetzt. Für die CVSS-Metrik wird z. B. vorgeschlagen, die Bewertungsgrößen PR und UI zu einer Bewertungsgröße zusammenzuführen, weil sie im Kern dasselbe aus unterschiedlichen Gesichtspunkten beschreiben.

Die Scorings nach Harnser (2010) und nach CVSS (First.org, 2022) werden über eine die log-Transformation und die Harmonisierung der Skalenkategorien angeglichen, sodass für beide Domänen auf Verfahrensebene eine Einordnung von Vulnerabilitäts-Scores auf einer – wie in dieser Arbeit vorgeschlagenen, viergliedrigen Skala – gelingen kann. Sicherheitslevels für die Domänen Physical Security und IT Security können über eine für beide Domänen gleich aufgebaute Matrix ermittelt und im Falle einer vorliegenden Wechselwirkung in Abhängigkeit von der Schwere dieser Wechselwirkung aufeinander abgestimmt werden. Die vorgeschlagene Harnser-Metrik und die vorgeschlagene CVSS-Metrik werden als Baustein für das Attack Path Rating in eine Bedrohungsanalyse und Risikobewertung integriert, die sich an den internationalen Standard ISO/SAE 21434 orientiert. Es kann darüber hinaus gezeigt werden, wie Expertenwissen über die Sicherheitsfähigkeit in den Domänen Physical Security und IT Security probabilistisch konsistent innerhalb eines Bayes'schen Netzes verknüpft werden kann.

Die Erkenntnisse dieser Arbeit leisten einen Beitrag zur risikogerechten Gestaltung von Sicherheitsmetriken. Sie können im Rahmen einer Anschlussforschung genutzt werden, um die Entwicklung einer neuen IT-Security-Metrik voranzutreiben, die eine Quantifizierung von IT-Vulnerabilität zulässt und auf die wirksamkeitsbasierten Bewertungsgrößen aus der physischen Sicherheitsbewertung, Protektion, Observation und Intervention, zurückgeführt werden kann. Die Ergebnisse dieser Arbeit können 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. Ferner können die vorgestellten Ansätze verwendet werden, um die Zusammenführung von Metriken aus der Functional Safety und Physical Security oder IT Security zu ermöglichen.

7 Literatur

7.1 Printquellen

Verweis im Text	Quellenangabe
Abendroth (2004)	Abendroth, J. (2004). Aktive Strategien zur Schutzzielverletzungserkennung durch eine kontrollierte Machtteilung in der Zugriffskontrollarchitektur. 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). Die Erhebung perzeptueller Prominenz auf Silben- und Wortebene: der Einfluss von Bewertungsskalen, Bewertungsebenen und Normalisierung.

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 für Infrastrukturanlagen-Energie und Wasser*. Berlin: Springer.

Bandow & Holzmüller (2009) — Bandow, G., & Holzmüller, H. H. (2009). *Das ist gar kein Modell!*. Wiesbaden: Gabler.

Becker et al. (2019) — Becker, W., Stradtmann, M., Botzkowski, T., Böttler, L., Voigt, K. I., Müller, J. M., & Veile, J. W. (2019). Ökonomische Risiken von Industrie 4.0. *Geschäftsmodelle in der digitalen Welt: Strategien, Prozesse und Praxiserfahrungen*, 493-515.

Bennett (1977) — Bennett, H. A. (1977). *EASI approach to physical security evaluation* (No. SAND--76-0500). Sandia Labs.

Bertsche & Lechner (2006) — Bertsche, B., & Lechner, G. (2004). *Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten*. Berlin, Heidelberg: Springer.

Bormann et al. (2018) — Bormann, R., Fink, P., Holzapfel, H., Rammler, S., Sauter-Servaes, T., Tiemann, H., & Weirauch, B. (2018). *Die Zukunft der deutschen Automobilindustrie* (No. 03). WISO Diskurs.

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). Beschränktes Risiko. In: *QZ. Qualität und Zuverlässigkeit*, 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, 7-9th February 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 Evaluation 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). *Projektorganisation und Management im 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.

Drucker (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-Universität 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 evaluation of physical protection systems*. Elsevier.

Geisberger & Broy (2012) — Geisberger, E., & Broy, M. (Eds.). (2012). *agendaCPS: Integrierte Forschungsagenda Cyber-Physical Systems* (Vol. 1). Springer-Verlag.

Gigerenzer (2014) — Gigerenzer, G. (2014). *Risiko: wie man die richtigen Entscheidungen trifft*. 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). *Anwendungsbeispiele für Kryptographie*. Universität Koblenz-Landau.

Grimm (2019) — Grimm, J. (2019). *Key Management for dummies*. A Wiley Brand. Entrust Special Edition.

Grossert (1989) — Grossert, E. (1989). *Untersuchungen zum Tragverhalten von Massivbrücken mit zweizelligem Kastenquerschnitt*. 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 evaluation*. Auerbach publications.

Hoffmeister (2017) — Hoffmeister, C. (2017). *Digital business modelling: digitale Geschäftsmodelle entwickeln und strategisch verankern*. 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). Industrie 4.0 und Wandel von Industriearbeit–revisited. Forschungsstand und Trendbestimmungen. In *Digitalisierung industrieller Arbeit* (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.

Klipper (2015) — Klipper, S. (2015). *Information Security Risk Management*. Springer Fachmedien Wiesbaden.

Koch (2013) — Koch, K. R. (2013). *Einführung in die Bayes-Statistik*. Springer-Verlag.

Kofler et al. (2018) — Kofler, M., et al. (2020). *Hacking & Security: Das umfassende Handbuch*. Rheinwerk Verlag.

König (2005) — König, H. (2005). *Peer-to-Peer Intrusion Detection Systeme für den Schutz sensibler IT-Infrastrukturen*. Gesellschaft für Informatik e.V.

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*. Mit Press.

Lehn et al. (2000) Lehn, J., Müller-Gronbach, T., Rettig, S., Lehn, J., Müller-Gronbach, T., & Rettig, S. (2000). Regression. *Einführung in die Deskriptive Statistik*, 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 ESREL 2017, 18.-22.06.2017, Portoroz, Slowenien.

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).* Hrsg. von 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 als Basisbaustein der Digitalisierung. In *2. Automobil Symposium Wildau: Tagungsband Technische Hochschule 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). *Konstruieren sicherheitsgerechter Produkte*. Springer.

Neugebauer (2018) Neugebauer, R. (2018). *Digitalisierung*. 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, abgerufen am 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). *Kryptografie verständlich*. 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-Risikomanagement: Identifikation, Quantifizierung und wirtschaftliche Steuerung*. Springer-Verlag.

Ponsard et al. (2021) — Ponsard, C., Ramon, V., & Deprez, J. C. (2021). Goal and Threat Modelling for Driving Automotive Cybersecurity Risk Analysis Conforming to ISO/SAE 21434. In *SECRYPT* (pp. 833-838).

Puhani (2020) — Puhani, J. (2020). *Statistik: Einführung mit praktischen Beispielen*. Springer-Verlag.

Puls et al. (2021) — Puls, T., Olle, W., Proff, H., Falck, O., Czernich, N., Koenen, J., & Möller, T. (2021). Strukturwandel in der Automobilindustrie–wirkt die Pandemie als Beschleuniger?. *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). *Leitfaden Automotive Cybersecurity Engineering*. Springer Fachmedien Wiesbaden.

Schwerdtfeger (2018) Schwerdtfeger, A. (2018). *Konzeption und Evaluierung eines Prozesses zur ganzheitlichen Sicherheitsbewertung von Mobile-Access-Systemen* (Dissertation, Universitätsbibliothek Wuppertal).

Shadbolt et al. (2015) Shadbolt, N. R., Smart, P. R., Wilson, J., & Sharples, S. (2015). Knowledge elicitation. *Evaluation 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). *Metriken–der Schlüssel zum erfolgreichen Security und 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). Standardnormalverteilung und z-Transformation. *Statistik für Erziehungswissenschaftlerinnen und Erziehungswissenschaftler: Konzepte, Beispiele und Anwendungen in SPSS und 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.

Termin 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.

Termin 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.

Termin 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). Hrsg. von 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). Zugriffskontrolle über Authentifizierung. *Rollen und Berechtigungskonzepte: Identity-und Access-Management im Unternehmen*, 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). Quantifizierung. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(Suppl 2), 287-312.

Voss (2013) — Voß, J. (2013). Was sind eigentlich Daten?. *LIBREAS. Library Ideas*, (23), 4-11.

Walz (1992) — Walz, G. (Ed.). (2013). *Handbuch der Sicherheitstechnik: Freigeländesicherung, Zutrittskontrolle, Einbruch- und Überfallmeldetechnik*. 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). *Entwicklung von Kennzahlensystemen*. 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). *Metriken für das Testreporting: Analyse und Reporting für wirkungsvolles Testmanagement*. 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.
Wurm (2022)	Wurm, M. (2022). *Automotive Cybersecurity: Security-Bausteine Für Automotive Embedded Systeme*. 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-Quellen

Verweis im Text	Quellenangabe
5Star (2021)	5StarProjects (2021). https://5starsproject.com/, abgerufen am 16.07.2021.
Airbnb (2021)	Airbnb (2021). https://www.airbnb.com/, abgerufen am 07.12.2021.
Autosec.se (2016)	Autosec (2016). *Security models.* https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf, abgerufen am 25.04.2022.
Azure (2021)	Micrososft Azure (2021). https://azure.microsoft.com/de-de/services/key-vault/, abgerufen am 11.11.2021.
Bayesfusion (2021)	Bayesfusion (2021). *GeNIe Modeler User Manual.* https://support.bayesfusion.com/docs/GeNIe.pdf, abgerufen am 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, abgerufen am 01.12.2021.
BayesiaLab (2012)	BayesiaLab (2012, 29. August). *Introduction to BEKEE, the Bayesia Expert Knowledge Elicitation Environment.* https://www.youtube.com/watch?v=6SkdFlR8FAA&t=2470s, abgerufen am 01.12.2021.
BHE (2021)	BHE (2021). *Perimetersicherheit.* https://www.bhe.de/publikationen/konzepte-and-broschueren/freigelaendeueberwachung, abgerufen am 16.07.2021
BKA.de (2021)	BKA (2021). *Kfz-Kriminalität.* https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Kfz-Kriminalitaet/kfz-kriminalitaet_node.html, abgerufen am 31.08.2021.
BMWi (2021)	BMWi (2021). *Der deutsche Gaia-X Hub.*

	https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html, 08.07-2021, abgerufen am 16.07.2021.
Brownlee (2020)	Brownlee (2020, 10. Juni). *How to Use StandardScaler and MinMaxScaler Transforms in Python.* https://machinelearningmastery.com/standardscaler-and-minmaxscaler-transforms-in-python/, abgerufen am 21.03.2021.
BSI (2016)	BSI-Bund (2016). *Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.html, abgerufen am 12.09.2021.
BSI-Branchenlagebild (2022)	BSI-Bund (2022, 19. September). *Branchenlagebild Automotive 2022.* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.pdf?__blob=publicationFile&v=8, abgerufen am 20.09.2022.
BSI-Glossar (2022)	BSI-Bund (2022). *Zero-Day Exploit.* https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html, abgerufen am 12.09.2022.
CC (2022)	CC (2022). *The Common Criteria.* https://www.commoncriteriaportal.org/, abgerufen am 18.06.2022.
Cert (2022)	Marty (2021, 1. April). *UNECE WP.29 / R155 - Wie sich Cyber Security ab Juni 2022 auf den Automobilmarkt auswirken wird.* https://certx.com/de/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/, abgerufen am 10.05.2022.
Charter Global (2020)	Charter Global (2020, 20. November). *Physische Sicherheitsstandards verstehen.* https://www.charter-global.com/physical-security-standards/, abgerufen am 21.10.2021.
Chester (2021)	Chester, J. (2021, 21. Oktober). *A closer look at CVSS scores.* https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/, abgerufen am 10.05.2022.
Cimpanu (2020)	Cimpanu, C. (2020, 18. Mai). *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/, abgerufen am 01.09.2021
CVE (2021)	CVE (2021). *CVE.* https://cve.mitre.org/, abgerufen am 16.07.2021.
CVSS Work Items (2022)	CVSS v4.0 Work Items (2022). https://docs.google.com/document/d/1qmmk9TQulW9d1cuipu_ziXDX0pUswbZ1WSQyynHbvKU/edit#, abgerufen am 11.05.2022.
Eddie (2021)	Eddie (2021, 18. März). *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/, abgerufen am 21.03.2021.
Elektronik-Kompendium (2021)	Elektronik-Kompendium (2020, November). *Client-Server-Architektur.* https://www.elektronik-kompendium.de/sites/net/2101151.htm, abgerufen am 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, abgerufen am 18.06.2022.

ENISA (2021) ENISA (2021, 27. Oktober). *ENISA Threat Landscape 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021, abgerufen am 27.06.2022.

EPSS (2021) First.org (2021). *Exploit Prediction Scoring System.* https://www.first.org/epss/, abgerufen am 11.05.2022.

Euro NCAP (2021) Euro NCAP (2021). https://www.euroncap.com/de, abgerufen am 16.07.2021.

EVITA (2022) EVITA (2022). https://www.evita-project.org/objectives.html, abgerufen am 27.06.2022.

FAIR (2021) FAIR Institute (2021). *The Standard Quantitative Model for Information Security and Operational Risk.* https://www.fairinstitute.org/, abgerufen am 16.07.2021.

First.org (2022) FIRST SIG (2019, 12. März). *FIRST is the global Forum of Incident Response and Security Teams.* https://www.first.org/, abgerufen am 16.01.2022.

flaticon.com (2021) Flaticon (2021). *Access 9.7M+ vector icons & stickers.* https://www.flaticon.com/, abgerufen am 08.10.2021.

Flinkey.de (2021) WITTE Automotive (2021). *Digitaler Fahrzeugzugang.* https://www.flinkey.com/, abgerufen am 08.10.2021.

Gabler (2021) Lackes, R. (2021). *Expertenwissen.* https://wirtschaftslexikon.gabler.de/definition/expertenwissen-34831, abgerufen am 21.12.2021.

Gabler (2022) Bendel, O. (2021). *Cyberecurity.* https://wirtschaftslexikon.gabler.de/definition/cybersecurity-99856, abgerufen am 31.05.2022.

Geiger (2021) Geiger, M. (2021). *Safety vs. Security: Der Unterschied einfach erklärt (und wie Sie beide Ziele kombinieren können).* https://www.sichere-industrie.de/safety-security-unterschied-erklaert-kombination-ziele-industrial-security/, abgerufen am: 05.05.2020.

Gulp (2022) Feralisch, J. (2022, 09. Dezember). *Junior vs. Senior: Die Erfahrung macht den Unterschied.* https://www.gulp.de/knowledge-base/18/ii/auswertung-junior-oder-senior-die-erfahrung-macht-den-unterschied.html, abgerufen am 21.12.2022.

Hafi.de (2015) HAFI (2015, Januar). *Amokprävention.* https://hafi.de/wp-content/uploads/2019/04/hafi-protect_20190503.pdf, abgerufen am 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/, abgerufen am 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, 11. Februar). *Identity Assurance Profiles Bronze and Silver.* https://incommon.org/wp-content/uploads/2019/04/IAP.pdf, abgerufen am 04.02.2021.

ISF München (2021) ISF München (2021, 8. Juni). *Forschungsreport Umbruch in der Automobilindustrie.*

https://www.isf-muenchen.de/wp-content/uploads/2021/06/Forschungsreport-Umbruch-in-der-Automobilindustrie.pdf, abgerufen am 30.12.2021.

Kantara (2021) Kantara (2021). *Identity Assurance*. https://kantarainitiative.org/idassurance/, abgerufen am 16.07.2021.

KBA (2021) KBA (2021). *Typgenehmigungserteilung*. https://www.kba.de/DE/Themen/Typgenehmigung/Typgenehmigungserteilung/typgenehmigungserteilung_node.html, abgerufen am 02.10.2021.

MaaS Alliance (2022) MaaS Alliance (2022, Oktober). *Mobility Data Spaces and MaaS*. https://maas-alliance.eu/wp-content/uploads/2022/10/MaaS-Alliance-Whitepaper-on-Mobility-Data-Spaces-1.pdf, Zugriff am 10.10.2022.

MDS (2022) MDS (2021). *Data Sharing Community*. https://mobility-dataspace.eu/de, abgerufen am 24.05.2022.

MEI (2021) Microsoft (2021). *The Microsoft Exploitability Index*. https://www.microsoft.com/en-us/msrc/exploitability-index, abgerufen am 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, abgerufen am 16.02.2022.

NIST (2021) NIST (2021). *National Vulnerability Database*. https://nvd.nist.gov/, abgerufen am 16.07.2021.

NIST CVSS (2022) NIST (2022). *Common Vulnerability Scoring Calculator*. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, abgerufen am 10.08.2022.

NIST Vulntology (2021) NIST (2021). https://github.com/usnistgov/vulntology, abgerufen am 11.05.2022.

Pohlmann (2015) Pohlmann, N. (2015). *Wirkung von IT-Sicherheitsmaßnahmen - Die neue Herausforderung*. 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, abgerufen am 16.11.2021.

Pohlmann (2021) Pohlmann, N. (2021). *Authentifikation*. https://norbert-pohlmann.com/glossar-cyber-sicherheit/authentifikation/, abgerufen am 16.07.2021.

RAND (2021) RAND (2021). *Delphi Method*. https://www.rand.org/topics/delphi-method.html, abgerufen am 29.11.2021.

RCAR (2021) RCAR (2021). https://www.rcar.org/, abgerufen am 16.07.2021.

Red Hat (2021) Red Hat (2021). *Understanding Red Hat security ratings*. https://access.redhat.com/security/updates/classification, abgerufen am 11.05.2022.

Risk-based Security (2017) Risk-based Security (2021, 05. Januar). *CVSS v3 Newer is besser right*. https://www.riskbasedsecurity.com/2017/01/05/cvssv3-newer-is-better-right/, abgerufen am 11.05.2022.

Samcurry.net (2023) Curry, S. (2023, 3. Januar). 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/, abgerufen am 04.01.2023.

Schneider (1999) Schneider, B. (1999, Dezember). *Attack Trees*.

	https://www.schneier.com/academic/archives/1999/12/attack_trees.html, abgerufen am 12.07.2022.
Sicherungssysteme (2021)	Institut für Sicherungssysteme (2021). *Konstituierung neuer Fachausschuss im VDI: Synthese von Safety und Security.* http://www.sicherungssysteme.net/de/aktuell/fachausschussimvdi.html, abgerufen am 21.10.2021.
Sifo.de (2023)	SIFO (2023). https://www.sifo.de/sifo/de/home/home_node.html, abgerufen am 02.01.2023.
SoQrates (2022)	SoQrates (2022). *SoQrates Softwareoffensive Bayern.* https://soqrates.eurospi.net/index.php, abgerufen am 11.05.2022.
SSVC (2021)	CERTCC (2021). *SSVC.* https://github.com/CERTCC/SSVC, abgerufen am 11.05.2022.
Statista (2011)	Statista (2011, April). *Prognose zur Anzahl der vernetzten Geäte weltweit.* https://de.statista.com/statistik/daten/studie/479023/umfrage/prognose-zur-anzahl-der-vernetzten-geraete-weltweit/, abgerufen am 12.08.2021.
SUSRS (2021)	Microsoft (2021). *Security Update Severity Rating System.* https://www.microsoft.com/en-us/msrc/security-update-severity-rating-system, abgerufen am 11.05.2022.
Thatcham (2021)	Thatcham (2021). *Thatcham Security Certification.* https://www.thatcham.org/what-we-do/security-certification/, abgerufen am 16.07.2021.
Tony O'Hagan (2021)	O'Hagan, T. (2021). *The Sheffield Elicitation Framework (SHELF).* http://www.tonyohagan.co.uk/shelf/, abgerufen am 29.11.2021.
TÜV (2021)	TÜV (2021). *TÜVRheinland.* https://www.tuv.com/germany/de/, abgerufen am 16.07.2021.
Uber (2021)	Uber (2021). *Uber – Get in the driver's seat and get paid.* https://www.uber.com/de/en/, abgerufen am 07.12.2021.
VDA (2022)	Perl, A. (2022). *Das NCAP-Programm.* https://www.vda.de/de/themen/automobilindustrie/standards-und-normung/euro-ncap-anforderungen, abgerufen am 07.07.2022.
Williams (2022)	Williams, J. (2022). *OWASP Risk Rating Mythodology.* https://owasp.org/www-community/OWASP_Risk_Rating_Methodology, abgerufen am 09.05.2022.

7.3 Richtlinien und Standards

Verweis im Text	Quellenangabe
47 CFR Part 15.247	U.S. Government Publishing Office (2010, 1. Oktober). 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, abgerufen am 25.02.2021.
BSI (2020)	BSI (2020, 17. Dezember). *IT-Grundschutz-Kompendium (Edition 2021).* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html, abgerufen am 12.11.2021.
CCC (2021)	Car Connectivity Consortium (CCC) (2021). https://carconnectivity.org/, abgerufen am 16.07.2021.
DIN e.V. (2018)	DIN e.V. (2018, August). DIN-Taschenbuch 408. *Informationssicherheitsmanagement.* BEUTH-Verlag.
DIN EN 1627	DIN e.V. (2021a). DIN EN 1627:2021-11. *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung; Deutsche und Englische Fassung prEN 1627:2019.* https://www.beuth.de/de/norm-entwurf/din-en-1627/299758611, abgerufen am 16.07.2021.
DIN EN 1628	DIN e.V. (2021b). DIN EN 1628:2021-11. *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter statischer Belastung; Deutsche und Englische Fassung prEN 1628:2019.* *https://www.beuth.de/de/norm-entwurf/din-en-1628/299762309*, abgerufen am 16.07.2021.
DIN EN 61508	DIN e.V. (2011). DIN EN 61508-1:2011-02; VDE 0803-1:2011-02. *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010.* https://www.beuth.de/de/norm/din-en-61508-1/135302584, abgerufen am 17.12.2021.
DIN EN ISO 9000	DIN e.V. (2015a). DIN EN ISO 9000:2015-11. *Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015.* https://www.beuth.de/de/norm/din-en-iso-9000/235671064, abgerufen am 13.12.2021.
DIN EN ISO 9001	DIN e.V. (2015b). DIN EN ISO 9001:2015-11. *Qualitätsmanagementsysteme - Anforderungen (ISO 9001:2015); Deutsche und Englische Fassung EN ISO 9001:2015.* https://www.beuth.de/de/norm/din-en-iso-9001/235671251, abgerufen am 25.02.2021.
DIN ISO/TR 22100	DIN e.V. (2014). DIN ISO/TR 22100-2:2014-09. Sicherheit von Maschinen - Beziehung zu ISO 12100. https://www.beuth.de/de/technische-regel/din-iso-tr-22100-1/252378999, abgerufen am 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, abgerufen am 10.05.2022.

DSGVO (2021) Europäische Union (2018, 25. Mai). *Datenschutz-Grundverordnung (DSGVO).* https://dsgvo-gesetz.de/, abgerufen am 16.07.2021.

IATF 16949 IATF (2016). IATF 16949:2016-10. *Anforderungen an Qualitätsmanagementsysteme für die Serien- und Ersatzteilproduktion in der Automobilindustrie.* https://www.beuth.de/de/technische-regel/iatf-16949/263942493, abgerufen am 25.02.2021.

IDSA (2016) IDSA (2016). *International Data Spaces Standard (IDS).* https://internationaldataspaces.org/, abgerufen am 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, abgerufen am 22.10.2021.

IEC 62368 IEC (2021). DIN EN IEC 62368-1:2021-05. *Einrichtungen für Audio/Video-, Informations- und Kommunikationstechnik - Teil 1: Sicherheitsanforderungen (IEC 62368-1:2018); Deutsche Fassung EN IEC 62368-1:2020 + A11:2020.* https://www.beuth.de/de/norm/din-en-iec-62368-1/336074670, abgerufen am 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, abgerufen am 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, abgerufen am 25.04.2022.

ISO 26262 ISO (2018). ISO 26262-1:2018 - ISO 26262-10:2018. *Straßenfahrzeuge - Funktionale Sicherheit.* https://www.beuth.de/de/erweiterte-suche/272754!search?alx.searchType=complex&alx.search.autoSuggest=true&searchAreaId=1&query=ISO+26262-1+&facets%5B276612%5D=&hitsPerPage=10, abgerufen am 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, abgerufen am 10.05.2022.

OSS Association (2021) OSS Association (2021). *Standard Offline by OSS Application.* https://www.oss-association.com/standards/oss-standard-offline/, abgerufen am 23.09.2021.

RSS 247 Government of Canada (2017, Februar). RSS 247. *Digital Transmission Systems (DTSs), Frequency Hopping Systems (FHSs) and Licence-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, abgerufen am 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, abgerufen am 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, abgerufen am 25.04.2022.

SPICE (2015) Automotive SIG (2015, 16. Juli). *Automotive SPICE Process Assessment / Reference Model.* https://www.automotivespice.com/fileadmin/software-download/Automotive_SPICE_PAM_30.pdf, abgerufen am 25.04.2022.

UNECE R 155 UNECE (2021, 22. Januar). *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, abgerufen am 25.04.2022.

VDA (2020) VDA (2020). ACSMS:2020-12. *ACSMS 2020_DEUTSCH.* https://webshop.vda.de/QMC/de/acsms-de_2020, angerufen am 25.04.2022.

8 Anhänge

8.1 Diskussion der Problemstellung

> 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, S. 5).

Ein zentrales Problem bei der Risikobewertung von Mobile-Access-Systemen (MAS) ist die domänenübergreifende Bewertung von physischer Security und IT-Security in konkreten Use Cases mittels einer geeigneten Metrik. Diese Metrik soll im Idealfall an die physische Domäne und die IT-Domäne andocken sowie das physische Szenario mit dem IT-Szenario verbinden können, sodass eine Aufdeckung und Bewertung von Wechselwirkungen möglich gemacht wird. Durch ein Modell, das Ursache-Wirkungs-Beziehungen quantitativ abbilden würde, könnte die Wirkung von Maßnahmen im Verbund beleuchtet werden, sodass eine Cost-Benefit-Optimierung auf quantitativem Wege möglich wäre. Mittels einer geeigneten Bewertung müssen Sicherungsmaßnahmen jedoch richtig im cyberphysischen Verbund abgebildet werden können, um eine domänenübergreifende Security-Betrachtung unabhängig von generischen Bedrohungsszenarien möglich zu machen. Es stellt sich die Frage, wie die Prinzipien aus beiden Domänen zusammengebracht können, damit eine domänenübergreifende Bewertung für die Security dazu beitragen kann, MAS schon im Entwicklungsprozess sicher(er) zu gestalten.

In Wang et al. (2017) wird dargelegt, dass es einen Mangel an effektiven (d. h. objektiven, wirksamkeitsbasierten) Security-Metriken gibt, mit denen Angriffe auf Netzwerke (quantitativ) bewertet werden können: „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). Diese Aussage wird darin begründet, dass sich existierende Metriken, wie z. B. CVSS (First.org, 2022), auf die Messung einer individuellen und i.d.R. bekannten Schwachstelle beziehen, jedoch die Interaktion einer Schwachstelle mit anderen Schwachstellen (anderer Systemeinheiten) von Administratoren herausgefunden werden muss (Wang et al., 2017, S. 3). Es werden mehrere Gründe aufgeführt, warum die Erarbeitung einer effektiven Metrik in der IT-Security schwer ist (Wang et al., 2017, S. vii, viii, 2, 54, 65):

- Es müssen zusätzlich zu bekannten Schwachstellen und Angriffen auch noch nicht eingetretene Szenarien bewertet werden.
- Immer mehr neue Sicherheitsschwachstellen werden wöchentlich veröffentlicht, die Administratoren berücksichtigen müssen. Daraus resultiert die Frage: Wie geht der Risikomanager mit neuen Informationen um?
- Angreifer führen z. T. komplexe, mehrschrittige Angriffe durch.
- Bisherige Detektionsmethoden können nicht mit der Komplexität von Angriffen umgehen.
- Sicherheit muss konsistent bewertet werden können, um einen Vergleich von Risiken sowie eine Abwägung zuzulassen und um die Einleitung von Minderungsmaßnahmen, welche knappen Ressourcen unterliegen, begründen zu können.
- Es gibt mitunter große Unsicherheiten in der Bewertung einzelner Risikobeiträge. Daraus folgt die Frage: Wie geht der Risikomanager mit großen Unsicherheiten um?

In Cheng et al. (2014, S. 8) werden weitere Herausforderungen aufgeführt:

- Fehlen einer „Echtzeit-Reaktion" auf Angriffe.

- Mangelndes Verständnis der Auswirkungen von Ereignissen auf den Betrieb.
- Mangel an quantitativen Metriken und Maßnahmen für eine umfassende Sicherheitsbewertung.
- Mangelnde Einbeziehung menschlicher (analytischer) Erkenntnisse in das cyber-physikalische Situationsbewusstsein.

In Wang et al. (2017, S. 2, 6) wird erklärt, dass das Zusammensetzen von Metriken zu einem globalen Maß nicht trivial und einfach ist. Die Folge einer „naiven" Zusammensetzung kann zu irreführenden Ergebnissen führen, da

- unterschiedliche Metriken nicht unbedingt konsistent aufgebaut und kompatibel sind, weil unter Umständen im Kern etwas Anderes bewertet wird.
- nicht mit Scores gerechnet werden sollte. Das liegt am Fehlen eines absoluten Größenbezugs.
- weniger Schwachstellen nicht gleich sicherer bedeutet.
- mit scheinbar zunächst unkritischen Schwachstellen geschäftsrelevante Ressourcen kompromittiert werden können. Es gibt Wechselwirkungen zwischen Einheiten.
- mit der Ausnutzung einer oder mehrerer Schwachstellen erst nach einiger Zeit die Kompromittierung (weiterer) geschäftsrelevanter Ressourcen einhergehen kann.
- es nicht auf den ersten Blick ersichtlich ist, welche Ursachen zu einer bestimmten Folge führen können. Zu bewertende Systeme sind, je nach Use Case, in ihrem Aufbau bzw. ihren immanenten Strukturen verschieden.
- der Bezug zur Hardware oft unberücksichtigt bleibt.

Die Berücksichtigung von Cybersecurity zusätzlich zur physischen Security bringt folgende vier Herausforderungen mit sich:

„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, S. 7).

Um Sicherheitsmaßnahmen gezielt implementieren zu können, muss zuallererst das Zusammenspiel zwischen den Komponenten eines Netzwerks verstanden werden (Wang et al., 2017, S. 2). Das ist eine Herausforderung, der nicht nur im Rahmen einer domänenspezifischen Betrachtung begegnet werden muss, sondern auch im Zuge einer domänenübergreifenden Betrachtung von Physical Security und IT-Security oder Safety und Physical Security oder IT-Security. In der Safety werden klassischerweise über die Festlegung von z. B. Safety Integrity Level (SIL) Anforderungen an das System definiert, die erfüllt werden müssen, um das entsprechende SIL zu erreichen.

Durch den zunehmenden Einsatz von IT in Safety-relevanten Anwendungsbereichen müssen gem. den Überlegungen in Lyu et al. (2020) aber neben Anforderungen an die Safety auch Anforderungen an die IT-Security beim Systemdesign berücksichtigt werden, da durch ausgebeutete IT-Schwachstellen Safety-Funktionen kompromittiert werden können. Systembetreiber werden hinsichtlich des quantitativen Nachweises von Ausfallraten im Verbund von Safety und IT-Security vor Herausforderungen gestellt, weil in der IT-Security Bedrohungen und Vulnerabilität nicht wirklich quantifiziert werden können. Die Anforderungen an Safety und Physical Security oder IT-Security können zudem widersprüchlich sein. Darüber hinaus gibt es unterschiedliche Nomenklaturen und Assessment-Rahmenwerke, welche die Zusammenführung erschweren (Macher et al., 2020a). Es stellt sich die Frage nach der Metrik zur Bewertung eines solchen Systems, welches Sicherheitsmerkmale aus mehreren Domänen vereint. Eine

zentrale Schwierigkeit liegt darin, ein korrespondierendes IT-Sicherheitslevel für beispielsweise „Safety Integrity Level drei" aus der Safety zu definieren bzw. auch andersherum. Es müssen insbesondere Schnittstellen zwischen Systemeinheiten und Wechselwirkungen erfasst und bewertet werden können. Bewertungen werden typischerweise mithilfe von Modellen vorgenommen (Bandow & Holzmüller, 2009, S. vii). Dabei gibt es zum einen Annahmen und zum andern Metriken, die den Bewertungen zugrunde liegen. Wenn nun eine Bewertung z. B. für die Safety oder Physical Security und IT Security im Verbund durchgeführt werden soll, stellen sich auf Seiten des Risikomanagers folgende Fragen:

- Wie lassen sich Eigenschaften, technologische Artefakte und Maßnahmen in einem Modell abbilden?
- Welche Bewertungsmetriken können konkret verwendet werden, um auch Wechselwirkungen von Safety, Physical Security und IT Security zu bewerten?
- Wie lassen sich Unsicherheiten berücksichtigen und wie lässt sich Expertenwissen einbinden?
- Wie kann Vergleichbarkeit geschaffen werden, um z. B. aufeinander abgestimmte Risikoniveaus zu erreichen?

Dass die naive Zusammenführung von z. B. Safety (mit Modellen und Metriken aus der Safety), Physical Security (mit Modellen und Metriken aus der physischen Sicherheit) und IT Security (mit Modellen und Metriken aus der IT) in einer domänenübergreifenden Bewertung nicht sinnvoll ist, davor wird in Wang et al. (2017, S. 2) gewarnt. Wirksamkeitsbasierte Bewertungsmetriken für die domänenübergreifende Bewertung von Safety und IT-Security oder Physical Security und IT-Security sind schwerlich zu finden, wie beim Stand der Richtlinien und Standards gezeigt wird. Ein klassischer Ansatz bei der Auslegung von Systemen unter Berücksichtigung von Unsicherheiten ist die Annahme von Worst Cases und die Festlegung von Sicherheitszuschlägen (Harnser, 2010, B, S. 2; First.org, 2022). Ein Zuviel an Sicherheit kann jedoch unwirtschaftlich werden. „Produkte mit übertriebenen Schutzmaßnahmen sind für diese Branche zu teuer und deshalb nicht wettbewerbsfähig", wird in Wurm (2022, S. 37) festgestellt. Zu wenig Sicherheit dagegen wäre fahrlässig. Hier stellt sich die Frage nach einem guten Cost-Benefit sowie nach der Rechtfertigung des Invests vor dem unternehmerischen Management. Das Hinzufügen von Sicherheitszuschlägen ist aber auch nur so lange praktikabel, solange ein Risikomanager keine Risiken vergleichen muss. Um Risiken vergleichen zu können, müssen Risiken im Idealfall quantifiziert werden. Herausforderungen liegen darin, dass dafür in den Domänen nicht dieselben Voraussetzungen vorliegen:

Bei semi-quantitativen Ansätzen, wie sie in der IT-Security-Bewertung verwendet werden, z. B. beim Common Vulnerability Scoring System (CVSS, First.org, 2022) oder OWASP Risk Assessment (OWASP, 2022), gibt es an keiner Stelle des Bewertungsprozesses eine Metrik, die sagt, wie Bewertungsgrößen bemessen werden. Wenn ein Risikoanalyst einen Experten zu einem Vulnerabilitätsbeitrag befragt und daraufhin eine semi-quantitative Einschätzung zwischen „null" (Minimum) und „zehn" (Maximum) erhält, dann fehlt eine Zuordnung dieser Scores zu einem konkreten Größenbezug. Nach der Bewertung liegt lediglich eine „Reihung von Zahlen" vor. Es handelt sich damit um eine monotone Funktion, d. h. wenn die Eingangsgrößen groß sind, dann sind auch die Ausgangsgrößen groß. Diese Art der Zuordnung ist z. B. beim DuPont-Schema nach Harnser (2010) – der Harnser-Metrik – der Fall (siehe Kapitel 2.5). Damit kann jedoch kein quantitativer Zusammenhang hergestellt werden, der besagt, dass z. B. der Score „drei" doppelt so schlimm ist wie der Score „vier". Folglich kann mit diesen semi-quantitativen Größen nicht wirklich gerechnet werden, da eine quantitative Metrik mit objektivem Wirkmechanismus zur Beschreibung des Schutzeffekts im Sinne einer Vulnerabilitätsreduktion dahinter fehlt. Das wird in der gängigen Praxis aber zuhauf getan, wie in Krisper (2021) erklärt wird.

Wenn bei den Scores nun eine Metrik hinterlegt wird, z. B. Zentimeter, dann hat ein Experte ein Vergleichsmaß, mit dem gerechnet werden kann. Insofern eine Metrik, wie sie in der physischen Security auf Basis der Zeit vorliegt (siehe das Vulnerabilitätsmodell in Kapitel 2.5), in der IT-Security nicht da ist, kann mit den Scores nicht einfach gerechnet werden. Das liegt daran, dass auf Scores Rechenoperationen nicht vernünftig angewendet werden können. In der IT-Security fehlt dafür ein objektiver Wirkmechanismus zur Beschreibung des IT-Schutzeffekts. Das IT-Scoring, z. B. CVSS (First.org, 2022), stellt nur sicher, dass eine Zahl größer, gleich oder kleiner ist als eine andere Zahl. Bewerten ferner zwei Experten unabhängig voneinander ein System, dann müssen sie sich einig sein, was ein konkreter Score-Wert bedeutet. Wenn eine darunterliegende Metrik vorhanden ist, dann ist eine Quantifizierung, auch unter Berücksichtigung von Unsicherheiten, möglich (z. B. Lichte et al. (2016)). Diese Voraussetzung ist in der IT-Security aber nicht gegeben (Schneider et al., 2019; siehe auch Kapitel 2.5).

Weiterhin stellt sich die Frage, wie wirksam IT-Maßnahmen sind. Daraus folgt wiederum die Frage, auf Basis welcher Mechanismen Wirksamkeit in der IT-Security bemessen werden kann. Das ist in der physischen Sicherheit ganz klar definiert über eine Verzögerungs- und Detektionszeit, sodass ein Risikoanalyst über eine gewisse Zeitbasis, welche als Intervention zur Verfügung steht, sagen kann, was die Wahrscheinlichkeit der Vulnerabilität ist. Die Wahrscheinlichkeit für die Vulnerabilität bedeutet demnach ganz genau, dass die Restüberwindungszeit kleiner ist als die Intervention, wie das Vulnerabilitätsmodell nach Lichte et al. (2016) veranschaulicht. Das ist eine ganz klare Definition von Vulnerabilität bzw. einem erfolgreichen Angriff im Sinne einer Metrik. Diese Voraussetzung hat ein Risikoanalyst in der IT nicht, weil er mit behelfsnumerischen Größen – Scores – nicht richtig rechnen kann (Braband, 2019). Wie kann nun eine konsistente Bewertungsgrundlage für die Bewertung von CPS aussehen? Der Stand der Forschung zur cyberphysischen Security (siehe Kapitel 2.2) wird hier klaren Handlungsbedarf aufzeigen.

Für diese Forschungsarbeit muss die Frage gestellt werden: Kann diese Zuordnung für beide Domänen in irgendeiner Form vorgenommen werden, wenn ja, was sind die Voraussetzungen? Die Abbildung von Wechselwirkungen geht nicht beliebig komplex über eine Metrik, daher werden nur Abschätzungen in der Praxis gemacht (Wang et al., 2017). In diesem Zusammenhang können Annahmen zur Vereinfachung herangezogen werden (Lichte et al., 2019). Durch das Vorliegen disjunkter Ereignisse könnte die Bedrohung beispielsweise gänzlich aus den Betrachtungen ausgeschlossen werden, weil sie besonders schwer zu quantifizieren ist. Es geht also nur noch um Vulnerabilitäten, wenn davon ausgegangen wird, dass Auswirkungen quantifizierbar sind. In diesem Fall wäre eine Bewertung zugänglich und grundsätzlich darstellbar. Hierbei gibt es jedoch ein Problem: In der IT-Security liegt keine vernünftige Beschreibung des (zeitlichen) Prozesses in Bezug auf die Vulnerabilität vor. Deswegen kann eine quantitative Metrik für die physische Vulnerabilitätsbewertung nicht wirklich an den IT-Angriffsprozess angedockt werden.

Die Gegenüberstellung der Bewertung von beispielsweise Tripple DES (Data Encryption Standard, 3DES) und DES (Paar & Pelzl, 2016, S. 72, 78) zeigt ganz klar die Herausforderung: Wie viel länger braucht der Angreifer, um DES bzw. 3DES zu überwinden? Wenn ein Risikoanalyst diese Basis hätte, dann kann eine quantitative Metrik erzeugt werden, um das eine Risiko mit dem anderen vergleichen zu können. Das hat ein Risikoanalyst nicht, wie am Beispiel der Verknüpfung von Vulnerabilitäts-Anteilen und Impact-Anteilen bei CVSS gezeigt wird (First.org, 2022). CVSS erzeugt zwar Zahlen, über diesen müssten aber Kategorien geschrieben werden. Mit diesen Zahlen wird sogar operiert, wie zuvor beschrieben. Das sollte nicht getan werden, da ein konkreter Bezugspunkt nicht da ist. Das ist im Kern ein Problem, mit dem bei der konsistenten Bewertung von CPS umgegangen werden muss. Eine zentrale Frage ist folglich: Wie kann das aufgelöst werden? Ein Anschauungsbeispiel für diese Problematik ist der Zielkonflikt zwischen

Safety und Security bei einer Tür: Safety bedeutet „eine Person ist schnell genug draußen", Security dagegen bedeutet, dass ein Angreifer lange genug aufgehalten wird, bevor er z. B. an einer schützenswerten Systemfunktion, auch Asset[80] genannt, angelangt ist. Jetzt kann ein Experte mittels der Vulnerabilitätsbewertung nach Lichte et al. (2016) Überwindungszeiten für die physischen Barrieren festlegen. Es liegt demnach eine Metrik vor, mit welcher Vulnerabilität quantifiziert werden kann. Darüber müssen auch Wechselwirkungen abgebildet werden können. Die Berücksichtigung von Wechselwirkungen mittels einer quantitativen Metrik gibt es aber weder in der physischen Sicherheitsbewertung noch in der IT-Sicherheitsbewertung. Die Frage steht im Raum, wie physische Sicherheit und IT-Sicherheit zusammen in einem konsistenten Ansatz richtig bewertet werden können. Es gibt weiterhin unterschiedliche Szenarien, wenn zwei Security-Domänen betrachtet werden.

Angenommen, es gibt erst einmal keine Wechselwirkungen. Trotzdem müssen Sicherheitslevel für die physische Sicherheit und IT-Sicherheit aufeinander abgestimmt werden können, sodass ein Systemanbieter sagen kann: Wenn z. B. IT-Security-Level „drei" gegeben ist, dann braucht es die gleiche Form von physischer Security, also auch Level „drei". Das ist notwendig, damit die Vulnerabilität in der physischen Sicherheit nicht die Auslegung in der IT-Security zunichtemacht, und vice versa. Ein IT-Angriffspfad beispielsweise sollte mit dem gleichen Sicherheitsniveau aus physischer Sicht abgesichert werden. Daraus ergibt sich die Frage: Wie kann dasselbe Sicherheitsniveau in beiden Domänen definiert und erreicht werden? Wenn ein Betreiber vorgibt, dass Sicherheitslevel „vier" benötigt wird, dann können die Experten aus der physischen Sicherheit und die Experten aus der IT-Sicherheit fragen: Wie kann das Security-Level der IT-Security mit der physischen Sicherheit vernünftig und konsistent zusammengebracht werden? Was für ein Ansatz könnte es leisten, Sicherheitsniveaus aufeinander anzupassen?

Wenn das vorherige Tür-Beispiel (Zielkonflikte von Safety und Security) betrachtet wird, dann ist das logisch: Je länger ein Angreifer braucht, um die Tür zu überwinden, desto besser ist das für die Security, wenn sie nur die Eigenschaft der Überwindungszeit hat, und desto schlechter gleichzeitig für die Safety. Türen können jedoch auch andere Eigenschaften haben. Moderne Türen von Bildungseinrichtungen erlauben es beispielsweise, einen Raum über die Tür leicht zu verlassen, wenn jemand nach draußen möchte. Ein Eintreten ist dann aber wiederum schwerer als das Verlassen (Hafi.de, 2015). Diese Besonderheit kann in einer Metrik bisher nicht abgebildet werden. Wenn eine konsistente Metrik zur Bewertung von CPS-Sicherheit aufgrund der inkompatiblen Bewertungsansätze nicht da ist, können beide Domänen nicht ohne Weiteres verbunden werden. Jetzt ist die Frage, wie das aufgelöst werden kann, sodass Wechselwirkungen, welche möglicherweise da sind, zum einen abgebildet werden können. Zum andern möchte ein Betreiber kohärente Sicherheitsniveaus erzielen. Wenn unter Annahme einer konsistenten Metrik nun z. B. ein Sicherheitsniveau „zwei" in der physischen Domäne vorliegt, dann muss ein Risikoanalyst nur zeigen, dass die Risikominderung in der IT-Domäne auf dem gleichen Niveau liegt, sofern es keine dezidierten Wechselwirkungen zwischen diesen Domänen gibt.

Wenn im Idealfall völlig separierte Angriffspfade betrachtet werden, dann gibt es Wechselwirkungen gar nicht. Das bedeutet, dass es lediglich die Möglichkeit gibt, über die physische Sicherheit oder über die Möglichkeiten in der IT an ein Asset zu gelangen, aber nichts, was jetzt miteinander kombiniert wäre. In der Realität muss das Vorliegen von Wechselwirkungen durch Experten eingeschätzt werden. Es wäre folglich sinnvoll, die IT-Security und physische

[80] Ein Asset ist etwas von besonderem Wert, das durch geeignete Sicherheitsmaßnahmen gegen missbräuchliche Verwendung geschützt werden soll.

Security gleichzeitig und durchgängig zu bewerten. Die Einzelbewertungen und cyberphysischen Verknüpfungen müssen dann zu einem konsistenten Ganzen zusammengeführt werden. Dafür wird idealerweise eine Metrik benötigt, mit der Risikoniveaus bzw. Vulnerabilitätsniveaus, z. B. anhand der Wirksamkeit von Maßnahmen, eins zu eins verglichen werden können. Wenn ein Risikoanalyst Experten weiterhin fragt, wie sich eine IT-Maßnahme auf das physische Risiko oder eine physische Maßnahme auf das IT-Risiko auswirkt, dann kann er nicht zu einem konsistenten Gesamtergebnis kommen, ohne eine darunterliegende, quantitative Metrik zu haben. Innerhalb einer Metrik bzw. Domäne ist das dagegen unter Einschränkungen, wie sie in Wang et al. (2017, S. 2, 6) formuliert werden, möglich. Es können beliebig komplexe, metrische Konstrukte oder Modelle aufgebaut werden, aber es muss beantwortet werden, wie beide Domänen im Kern zusammengebracht werden können. Kurzum bereitet das Zusammenbringen Probleme (siehe Kapitel 2.2). Zielstellung wäre es, auf Basis einer Risikominderung in einer Domäne eine äquivalente Widerstandsfähigkeit in der anderen Domäne zu erreichen, sodass z. B. die ermittelte Vulnerabilität seitens des Betreibers akzeptiert wird.

Auf der einen Seite sind IT-Prozesse, auf der anderen Seite sind physische Prozesse. Die Prozesse in der IT-Domäne und die Prozesse in der physischen Domäne müssen zu ähnlichen Risikoabschätzungen kommen, folglich zu ähnlichen Risiko-Metriken. Das bedeutet etwa, dass ganz schwere, mittelschwere und leichte Fälle ungefähr die gleiche Bemessung haben. Das ermöglicht es auch, Risiken zu priorisieren. Weil MAS als CPS kategorisiert werden können, gibt es eine physische Security-Ebene und eine IT-Security-Ebene, welche in einer Risikoanalyse zu berücksichtigen sind. Wenn jetzt die Metriken in der physischen Domäne und in der IT-Domäne die gleichen physikalischen Vorgänge beschreiben würden, dann wäre das die natürliche Ebene, auf der die physischen Metriken und IT-Metriken zusammengebracht werden. Das bedeutet: Beschreibt die physische Sicherheitsmetrik beispielsweise, wie wahrscheinlich eine Tür zu ist, und die Safety-Metrik, wie wahrscheinlich diese Tür offen sein muss, dann können diese beiden Metriken anhand der physischen Gegebenheiten zusammengeführt werden, weil ein Bezug auf diese physischen Gegebenheiten da ist.

Erschwerend kommt hinzu, dass es weder in der physischen Security noch in der IT-Security nur die eine Metrik bzw. die eine Parameterverknüpfung oder nur das eine Modell gibt, das von allen Risikomanagern in jedem Anwendungsfeld gleich verwendet wird (siehe Kapitel 2.5). Folglich steht ebenso die Herausforderung im Raum, ein geeignetes Modell – insofern möglich – und eine geeignete Metrik oder eine Kombination von Metriken zu finden, welche es ermöglichen können, Wechselwirkungen so abzubilden, dass sich beispielsweise die Wirkung von Maßnahmen auf die Vulnerabilität wiederfinden lässt. Eine berechtigte Frage ist, wie das Problem der domänenübergreifenden Vulnerabilitätsbewertung von physischer Security und IT-Security für CPS auf metrischer Ebene aufgelöst werden kann, um eine fundierte Entscheidungsunterstützung in Form eines Risikobewertungsprozesses zu schaffen, auf deren Basis Risiken, z. B. im Falle MAS für Fahrzeuge, bewertet und gegeneinander abgewogen werden können.

8.2 Paradigmen in der physischen und IT-Sicherheit

8.2.1 Struktur und Eigenschaften des IT-Layers

IT-Sicherheit kann gem. dem Gabler Wirtschaftslexikon folgendermaßen definiert werden:

> Cybersecurity oder IT-Sicherheit ist der Schutz von Netzwerken, Computersystemen, cyberphysischen Systemen und Robotern vor Diebstahl oder Beschädigung ihrer Hard- und Software oder der von ihnen verarbeiteten Daten sowie vor Unterbrechung oder Missbrauch der angebotenen Dienste und Funktionen. Bei den Daten handelt es sich sowohl um persönliche als auch um betriebliche (die wiederum persönliche sein können). (Gabler, 2022).[81]

Daten spielen eine Schlüsselrolle für die Funktionalität und Sicherung eines Systems (Wheeler, 2011, S. 8; BSI-Bund, 2021). Sie sind einzelne beobachtbare, messbare Elemente, die, wenn sie aneinandergereiht werden, eine Information darstellen (Voss, 2013). Informationen werden in binären Einheiten, d. h. Nullen und Einsen, maschinenlesbar auf physischer Hardware gespeichert (Anderson, 2001, S. 365) und können in alphanumerischen Zeichen, Buchstaben, Ziffern und Symbole abgebildet werden. Diese sind vom Menschen lesbar und interpretierbar. Daten erlauben die Analyse, Synthese, Trennung, Auswertung, Speicherung, Verarbeitung und Übertragung (Bodendorf, 2016, S. 1-6). Sie werden zwischen mindestens zwei Akteuren über einen physischen oder drahtlosen Kanal transferiert. Das setzt zum einen geeignete Schnittstellen auf beiden Seiten voraus, ebenso müssen sich beide Parteien darauf einigen, nach welchen Regeln sie welche Daten wann austauschen (Paar & Pelzl, 2016, S. 5). Dafür sind Protokolle notwendig (Anderson, 2001, S. 63). Um sicherzustellen, dass Unbefugte Nachrichten nicht abhören und mitlesen können, werden Botschaften durch kryptographische Techniken verschlüsselt (Paar & Pelzl, 2016, S. 4). Das Geheimnis zur Entschlüsselung ist im Idealfall beiden Akteuren bekannt und muss vor Missbrauch geschützt werden (Paar & Pelzl, 2016, S. 6-7). Signaturen werden z. B. verwendet, um dem jeweiligen Gegenüber die Richtigkeit der eigenen Identität nachzuweisen (Paar & Pelzl, 2016, S. 335–338, 392-395). Das ist notwendig für die Gewährleistung von Vertrauen im Zuge der Kommunikation.

Daten bilden die Grundlage eines Identity- & Access-Management (IAM) und damit verbundenen Services (Indu et al., 2018). Sie werden von cyberphysischen Produkten, wie beispielsweise Mobile-Access-Systemen (MAS), empfangen, verarbeitet und in eine physische Aktion, z. B. eine Verriegelung oder Entriegelung eines Fahrzeugs durch die Betätigung eines Schließmechanismus, übertragen (Flinkey.de, 2021). Der Zugang zu Daten erfolgt über drahtlose oder kabelgebundene Schnittstellen. Auch diese müssen vor unbefugtem Zugriff geschützt werden (Ashibani & Mahmoud, 2017). Damit berechtige Personen Zugriff auf Funktionen zur Nutzung von Daten erhalten können, werden Komfortklappen in die Produktbarrieren zum Schutz der Daten implementiert. An diesen Komfortklappen muss sich ein Benutzer mit seinem Berechtigungsnachweis (Credential) authentifizieren (Tsolkas et al., 2017, S. 129-160). Credentials können Wissen, Besitz oder Merkmale sein (Pohlmann, 2021). Ist eine Authentifizierung erfolgreich, wird Zugang gewährt, andernfalls nicht. Darüber hinaus werden „Wächter" implementiert, die das Verhalten von Benutzern und Funktionsaufrufen observieren und Anomalien detektieren können (König, 2005; Kofler et al., 2018, S. 37-38). Das sind z. B. Firewalls oder Anti-Malware-Programme.

In der IT wird ein Spektrum an Daten i. d. R. geloggt (zu dt. protokolliert) (Sowa, 2011, S. 3). Das ist im Grunde genommen die Observation. Hat ein Betreiber vergessen, etwas nicht zu loggen,

[81] Wie der Definition entnommen werden kann, werden die Begriffe Cybersicherheit und IT-Sicherheit gleichgesetzt.

dann werden Aktivitäten rund um diese nicht erfassten Datenpunkte auch nicht observiert. Das Monitoring wiederum stellt die Handlungsableitung dar und ist somit die Detektion. Nach erfolgreicher Detektion kann ein Alarm ausgelöst werden, der i.d.R. nur für eine übergeordnete Instanz, z. B. einen Administrator, einsehbar ist. Dabei kann auf automatisierte Ansätze und normalisierte Log-Daten zurückgegriffen werden, sodass erfasste Daten von IT-Systemen verglichen werden können (Sowa, 2011, S. 5). Nach der Feststellung von Anomalien erfolgen automatisierte und/oder durch den Menschen eingeleitete Interventionsmaßnahmen, wie beispielsweise die Sperrung eines Benutzer-Accounts, um einen potenziellen Missbrauch von beispielsweise sensitiven (geschäftsrelevanten) Daten abzuwenden (Wheeler, 2011, S. 155). Nach Angriffen folgt klassischerweise ein Rückkopplungsprozess im Sinne eines Knowledge-Managements, d. h. es wird aus dem Angriff gelernt und die aus der Analyse und Bewertung gewonnenen Erkenntnisse fließen in die Optimierung des Designs von Security-Maßnahmen ein (Ritz, 2015, S. 15, 22, 43). Dieser Teil ist dem Resilienz-Management zuzuordnen.[82]

Seitens des Deutschen Instituts für Normung (DIN) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird grundsätzlich empfohlen, sich zunächst auf allen Ebenen (Mobile Device, Cloud, etc.) mit Best Practices aus Rahmenwerken[83] zu beschäftigen (DIN e.V., 2018, S. 81; BSI, 2020, S. 6). Dann können zusätzlich dazu Erfahrungen aus der Industrie bzw. branchenspezifische Erfahrungen und Erfahrungen aus Zwischenfällen (Incidents) die Best Practices ergänzen. Best Practices sind Maßnahmen, die ein Anbieter vorweggreifen kann, weil allgemein bekannt ist, dass in der Vergangenheit z. B. bei anderen Systemen Angriffe auf konkrete IT-Komponenten in bestimmter Art und Weise erfolgreich stattgefunden haben. Es gibt in diesem Zusammenhang z. B. OWASP[84]. Auf der Webseite der Non-Profit-Organisation werden „Top 10"-/"Top 100"-Schwachstellenlisten aufgeführt, beispielsweise auch für Mobile Devices, und etwa alle drei Jahre veröffentlicht. Schwachstellen, die dort aufgeführt sind, müssen also per Default geschlossen werden. Bei Best Practices braucht das System folglich nicht großartig analysiert werden. Wenn diese Schwachstellen nicht behoben (geschlossen) sind, dann ist es sehr wahrscheinlich, dass ein Angreifer diese ausnutzen wird. Das können z. B. organisatorische Vorgaben oder Vorgaben zu organisatorischen und technischen Prozessen sein (Sowa, 2011, S. 36). In der ISO 27002 gibt es beispielsweise einen Maßnahmenkatalog mit einer Vielzahl an präventiven, detektiven und reaktiven Maßnahmen (DIN e.V., 2018, S. 86-193).

Insgesamt verfolgen Anbieter (Provider) von datenbasierten Services den kontrollierten und beschränkten Zugriff auf schützenswerte Daten, sog. Daten-Assets (Balzer & Schorn, 2011, S. 365; Sowa, 2011, S. 24; BSI, 2020, S. 31). Um den Zugriff nur durch berechtigte Personen(gruppen) zu gewährleisten, werden drei wesentliche Schutzziele definiert, die durch geeignete Eigenschaften und Maßnahmen geschützt werden müssen (BSI, 2020, S. 13):

- Verfügbarkeit (Availability): Sicherstellung des Funktionserhalts.
- Vertraulichkeit (Confidentiality): Daten dürfen nur von berechtigten Personen eingesehen werden.
- Integrität (Integrity): Datenänderungen müssen nachvollziehbar und transparent erfassbar sein.

[82] Beim Resilienz-Management geht es im Kern um die Erholung und Anpassungsfähigkeit eines Systems nach einem Sicherheitsvorfall oder Angriff (Ritz, 2015, S. 22).
[83] Dies umfasst Standards mit Maßnahmenkatalogen, wie von Schwerdtfeger (2018) herausgearbeitet.
[84] Bei OWASP (Open Web Application Security Project) handelt es sich um Non-Profit-Organisation, welche die Sicherheit in der Entwicklung von internetbasierten Applikationen und Services durch Vorgaben, wie z. B. im Application Security Verification Standard (ASVS) dargestellt, verbessern möchte. Im Kern geht es um die Gewährleistung sicherer Programmierung durch Regelwerke, Schulungen und den Einsatz von Testwerkzeugen.

Wird ein cyberphysisches Schließprodukt oder werden alle weiteren notwendigen Einheiten zur Nutzung bzw. Bereitstellung des Access-Service (beispielsweise Cloud-Komponenten und mobile Endgeräte) durch einen Angreifer unmittelbar bedroht, sind aus IT-Perspektive die Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit gefährdet (Abendroth, 2004). In der IT wird eine systemimmanente Vulnerabilität über eine Schutzzielverletzung definiert (First.org, 2022). Mit einer Schutzzielverletzung geht einher, dass ein Angreifer Daten-Assets für seine eigenen, böswillig motivierten Zwecke nutzbar machen kann. Bei CPS gibt es grundsätzlich unterschiedlich wertvolle Daten-Assets. Der Betreiber eines CPS möchte weder dem Kunden noch Externen uneingeschränkten Zugriff auf (bestimmte geschäftsrelevante) Daten geben, wie einem gültigen digitalen Zertifikat, mit dem eine Verriegelung oder Entriegelung eines Fahrzeugs möglich ist. Aus diesem Grund werden Rollen und Befugnisse an Benutzer-Credentials geknüpft, so gibt es z. B. Entwickler, Administratoren und Benutzer, wobei die Rollen und Rechte verschieden ausdifferenziert sein können. Grundsätzlich werden die drei Funktionen „lesen", „schreiben" und „ausführen" für konkrete Use Cases unterschieden (Anderson 2001, S. 93-99). Diese definieren den jeweiligen Funktionsumfang von Benutzern und Maschinen. Sie werden in sog. „Policies" (zu dt. Richtlinien) definiert (Grimm, 2019, S. 22).

In der IT gibt es eine Mannigfaltigkeit an Rollen und Zugriffsrechten. Benutzer oder Maschinen mit hohen Befugnissen, z. B. Administratoren, kontrollieren und regeln die Rollen und Rechte von Benutzern und Maschinen mit geringeren Befugnissen. Ebenso haben sie Zugriff auf sensitivere Daten als einfache Benutzer. Im Gegenzug sollen zum einen subordinierte Entitäten hierarchisch höhergeordnete Akteure nicht modifizieren können, d. h. beispielsweise ein Benutzer mit Leserechten soll einen vollumfänglichen Administrator nicht seiner Rechte berauben können. Zum andern muss es subordinierten Einheiten verwehrt werden, Daten eines höheren Levels einzusehen. Dieses Prinzip wird als Multi-Level-Security bezeichnet (Anderson, 2001, S. 243). Die Sicherheit zwischen Einheiten, die hierarchisch auf der gleichen Ebene und damit koordiniert angeordnet sind, und das Prinzip mehrerer, hintereinander geschalteter Sicherungsmechanismen einer einzigen Entität, wie z. B. die Zwei-Faktor-Authentifizierung (Kofler et al., 2018, S. 51), umfassen die sog. Multi-Lateral-Security (Anderson, 2001, S. 276).

Die IT erlaubt systemische Konfigurationen mit unterschiedlich weiten Zugriffsumfängen, z. B. Internet-, Intranet- oder lokal angebundene Systeme (First.org, 2022). Grundsätzlich zeichnet sich diese Logik auch durch Wechselwirkung von Schichten einer Einheit und von systemischen Akteuren untereinander aus (Kumar et al., 2014). In der IT gibt es ein Standardkonzept, Server-Client-Modell genannt, das die Beziehung der Einheiten eines IT-Systems untereinander und die Aufgabenverteilung der IT-Einheiten beschreibt (DIN SPEC 27070). Bevor auf die Eigenschaften, Funktionen und die topologischen Strukturen des Server-Client-Modells und seine Ausprägungen eingegangen wird, werden folgende Begriffe in Anlehnung an das Harris (2021) definiert, um das Verständnis zu fördern:

1. Ein Server kann als Programm beschrieben werden, welches Clients Zugang zu Diensten (Services) ermöglicht.
2. Ein Client (zu dt. Dienstnutzer) kann Services bei einem Server anfordern. Dafür nutzt er ein Programm. Der Server stellt dem Client Services zur Verfügung.
3. Ein Programm ist eine Folge von definierten Anweisungen, um bestimmte Funktionen auf einem programmierbaren, datenverarbeitenden System auszuführen.
4. Ein Dienst (Service) ist eine Art Kommunikationsprotokoll zum Austausch von Daten zwischen dem Server und dem Client nach festen Regeln.

Darüber hinaus ist die Abgrenzung der Begriffe Request (zu dt. Anfrage) und Response (zu dt. Antwort) notwendig. Request beschreibt die Anfrage des Clients an den Server, einen Service

nutzen zu dürfen. Die Response dagegen ist die Antwort des Servers auf die Anfrage des Clients (siehe Abbildung 65).

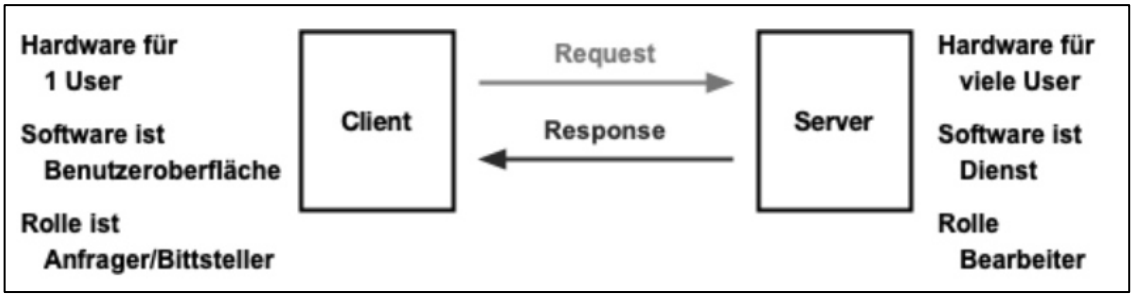


Abbildung 65: Grundaufbau und Grundprinzip einer Server-Client-Verbindung.
Quelle: Elektronik-Kompendium (2021).

Die Beziehung und Kommunikation zwischen Servern – oder allgemein Service-Anbietern – und Clients – den Service-Nutzern – kann unterschiedliche Ausprägungen annehmen. Eine gängige Abgrenzung ist die Einteilung in das Peer-to-Peer-Netzwerk (P2P) und das klassische Server-Client-Netzwerk (Harris, 2021). Ein P2P-Netzwerk zeichnet sich durch dezentral angeordnete Computer aus. Ziel des Einsatzes eines solchen Netzwerks ist es, Informationen entweder mit allen oder ausgewählten Benutzern zu teilen. Alle Computer sind hierbei gleichwertig, d. h. jeder Teilnehmer hat grundsätzlich Zugang zu allen verfügbaren Services bzw. Ressourcen. Jeder Knoten ist berechtigt, Services anbieten und auch Services von anderen zu beziehen. Jeder Teilnehmer kann damit Client und Server zugleich sein. Anderen Knoten kann mitgeteilt werden, was für Services genutzt werden sowie zu welchen weiteren Knoten eine Konnektivität besteht. Im Gegensatz zum P2P-Netzwerk ist das Client-Server-Modell eine zentralisierte Struktur (siehe Abbildung 66).

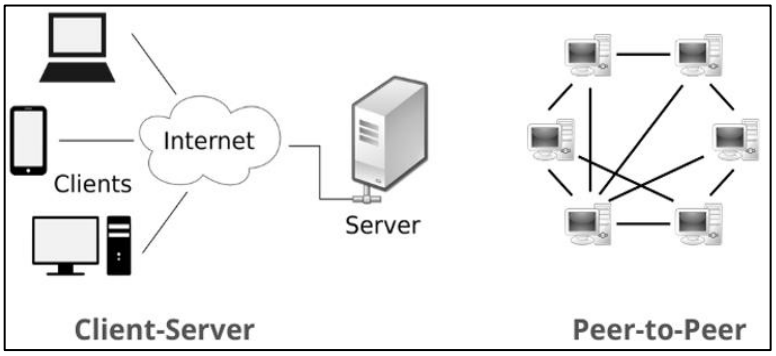


Abbildung 66: Darstellung des Client-Server- und P2P-Netzwerks.
Quelle: Harris (2021).

Ein Server managt Ressourcen und Services und stellt diese den Clients, z. B. Computern, bereit, welche allesamt mit dem Server in einem Netzwerk verbunden sind. Ein Netzwerk ist beispielsweise das Internet. Der Server ist somit beim Server-Client-Modell der Vermittler im Netzwerk und wartet, bis Clients Services bzw. Ressourcen anfragen – erst dann antwortet klassischerweise der Server. Das Verständnis dieser Grundstrukturen ist insofern relevant für eine Security-Bewertung, weil durch die innewohnenden Charakteristiken und die Topologie des Netzwerks u. a. folgende sicherheitsrelevante Punkte definiert werden:

- Anzahl der Teilnehmer
- Anordnung, physische Zugänglichkeit und IT-Zugänglichkeit[85]

[85] In der Regel werden die Computer von menschlichen Benutzern verwendet.

- Rollenkonzept bzw. Funktionen, Aufgaben und Zugriffsrechte (lesend, schreibend, ausführend)
    - Usermanagement
    - Berechtigungsmanagement
    - Key Management
    - Usw.
- Schnittstellen zu anderen Knoten und Benutzerschnittstellen
- Datenmodell
    - Protokolle (feste Kommunikationsregeln) zur Speicherung, Verarbeitung, Bearbeitung und Übertragung von Daten
    - Synchronisation, Update und Aktualisierung
    - Service- und Ressourcenmanagement
- Sicherheitsmaßnahmen, um Vertraulichkeit, Verfügbarkeit und Integrität sicherzustellen

Im Kern definiert ein Use Case IT-seitig den Funktionsumfang an Services, Akteuren und technischen Einheiten sowie deren Schnittstellen untereinander, das Rollenkonzept, das Datenmodell (d. h. den Umgang mit Daten) sowie technische Sicherheitsmaßnahmen. Zusammenfassend gibt es auf der einen Seite Service-Anbieter und auf der anderen Seite Service-Nutzer. Online-Vermittlungsdienste von Wohnungen oder Fahrzeugen beispielsweise bieten ihren Kunden eine einfache Buchung und Bezahlung via App an (siehe z. B. Uber (2021) und Airbnb (2021)). Es stellt sich jedoch die Frage, wie die Kunden in das Fahrzeug oder die Wohnung gelangen. Zwar könnte eine Übergabe des physischen Schlüssels durch den Besitzer oder Vormieter erfolgen, im Falle einer hohen Fluktuation von Mietern – insbesondere rund um den Globus – ist das jedoch ggf. wenig praktikabel. Aus diesem Grund braucht es eine Möglichkeit, den gebuchten Miet-Service von der Online-Welt (der App) in die physische Welt zu transferieren. Hierbei kommen MAS eine Schlüsselrolle zu. Ein Mieter könnte z. B. eine Wohnung buchen und er erhält nach der Bezahlung ein digitales Zertifikat, mit dem er sich beim Schließsystem in der Tür authentifizieren kann, um in die Wohnung zu gelangen. Das MAS setzt den digitalen Service also physisch um. Hinsichtlich des Zugriffs auf MAS können auch grundsätzlich unterschiedliche Rollenkonzepte realisiert werden. Es wäre denkbar, dass es Administratoren gibt, die Berechtigung manuell für bestimmte Benutzer, z. B. Putzkräfte, vergeben.

Das klassische Client-Server-Modell, das lediglich die logische Struktur auf IT-Ebene darstellt, kann also durch den physischen Vertreter eines Services (das Schließgerät) erweitert werden (siehe Abbildung 67). Im Grunde handelt es sich bei dem physischen Vertreter auch um eine Art Client, der im Auftrag des Servers bestimmte Aktionen (z. B. Verriegelung oder Entriegelung) nach festgelegten Regeln (ein Benutzer muss im Besitz eines gültigen digitalen Zertifikats sein) ausführt. Darüber hinaus könnte es Verbindungen zwischen den einzelnen Clients geben, wobei auch eine direkte Verbindung zwischen dem Schließgerät und dem Server möglich wäre, um z. B. die Uhrzeit und die Liste gesperrter Benutzer zu aktualisieren.

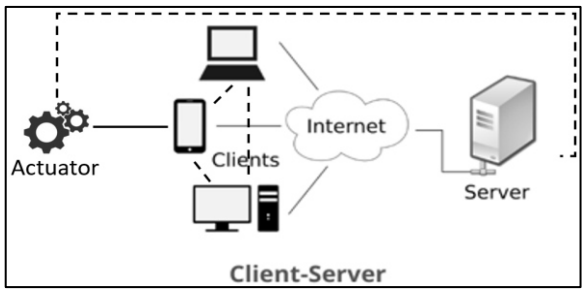


Abbildung 67: Erweiterung des Client-Server-Modells durch die physische Komponente und Interkonnektivitäten zwischen den Clients.
Quelle: Eigene Abbildung in an Harris (2021).

Wenn eine Architektur nun aus beliebig kompliziert miteinander verbundenen Einheiten besteht, die in mehrere subordinierte Server eingeteilt werden können, welche wiederum verschiedene Services einer Vielzahl an Clients anbieten, dann wird in diesem Zusammenhang von Edge-Computing gesprochen (Luo et al., 2020) (siehe Abbildung 68). Edge-Computing ist eine Ausprägung des Cloud-Computings, wobei das klassische Server-Client-Modell dem Cloud-Computing zugrunde liegt. Hinter den Servern und Clients stehen i.d.R. Benutzer. Benutzer haben unterschiedliche Rollen und damit verbundene Funktionen. Gleichzeitig geht mit dem Server-Client-Modell implizit die Verwaltung unterschiedlicher Aufgaben einher.

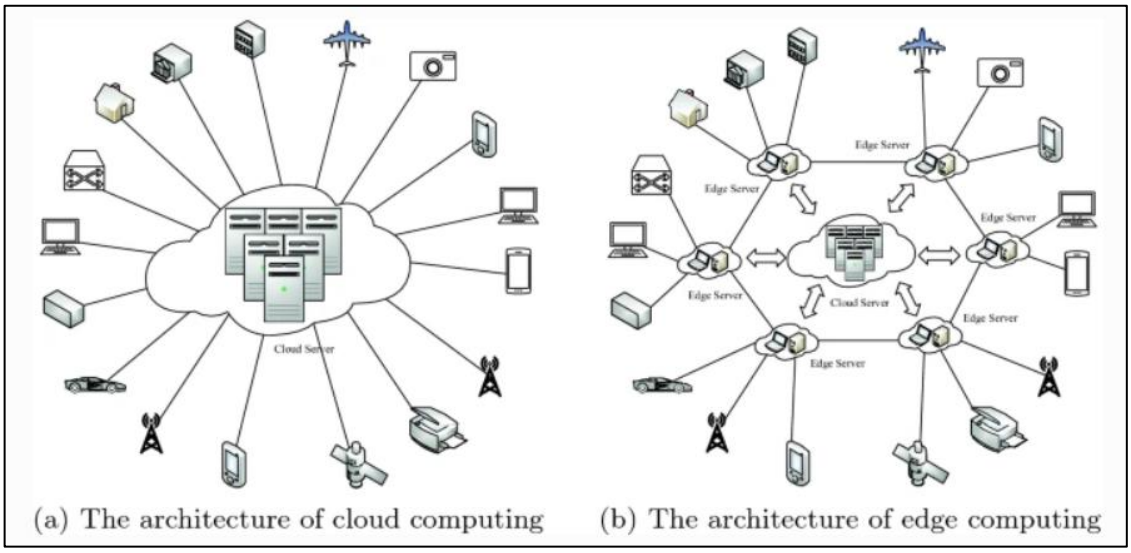


Abbildung 68: Gegenüberstellung von Cloud- und Edge-Computing.
Quelle: Luo et al. (2020).

Die Bündelung von Prozessen und Abläufen, sodass bestimmte Aufgaben gemäß konkreten Anforderungen durchgeführt werden können, wird nach DIN EN ISO 9000:2015-11 (DIN e.V. 2015a) als „Managementsystem" bezeichnet. Managementsysteme im Kontext Access bestehen aus den Elementen Benutzermanagement, Device-Management, Key-Management, Schnittstellenmanagement (API-Management) und Berechtigungsmanagement (Grimm, 2019, S. 36). Benutzer- und Device-Management werden auch unter dem Begriff „Identity-Management" zusammengefasst. Key-Management, Schnittstellenmanagement (API-Management) und Berechtigungsmanagement werden zusammenfassend mit dem Begriff „Access-Management" beschrieben (Sharma et al., 2015). MAS sind durch diese Einteilung Identity- und Access-Managementsysteme (IAM). Unterschiedliche Teile der Managementsysteme können von verschiedenen Einheiten der Architektur administriert werden.

Eine Einheit kann z. B. das Key-Management und das Schnittstellenmanagement als Service offerieren, während eine andere Einheit für das Benutzer- und Device-Management zuständig ist. Die Aufgabenteilung muss aber nicht immer scharf abgegrenzt sein. Services und damit verbundene Daten können ferner von einer oder mehreren Instanzen gehostet werden. Ein Host kann z. B. Server besitzen und deren Nutzung seinen Clients in Form eines Service anbieten. Clients eines Hosts können diese Services nutzen und ihren eigenen Clients weitere Services offerieren, die an die Host-Services andocken. Warum aber ist das Verständnis über die Aufgabenverteilung und die Interdependenzen innerhalb einer Architektur wichtig für eine Security-Bewertung? Die architekturellen Strukturen zeigen einerseits Akteure, deren Funktionsumfang und Schnittstellen auf, andererseits liefern sie einen Hinweis auf mögliche Einsprungpunkte, Angriffspfade und mögliche Auswirkungen auf die Bereitstellung bzw. Nutzung von Services im Falle eines erfolgreichen Angriffs (Kofler et al., 2018, S. 31-35; Möller et

al., 2019, S. 308). Bei CPS wird angenommen, dass sich erfolgreiche Angriffe auf Daten-Assets grundsätzlich immer auch in der physischen Domäne manifestieren.

Gelingt es einem Angreifer beispielsweise, an Administratorrechte zu gelangen, können Sicherungsmechanismen außer Kraft gesetzt, Rollenrechte anderer Benutzer entzogen oder modifiziert oder Hintertüren implementiert werden, um sich langfristigen Zugang zu Daten- oder physischen Assets zu sichern. Bei automobilen MAS steht beispielsweise der Diebstahl eines oder mehrerer Fahrzeuge im Raum. Der physische Angriff könnte durch die Kompromittierung einer IT-Einheit begünstigt werden. Aus diesem Grund und teils wegen mangelnder Maßnahmen zur gezielten Observation und Intervention setzt die IT-Sicherheit i.d.R. zu 100% auf Protektion (Wheeler, 2011, S. 18). Zudem entwickelt sich die IT kontinuierlich (in immer kürzeren Zeitabständen) weiter, was dazu führt, dass bisher als sicher geltende Sicherungsmaßnahmen als obsolet klassifiziert werden. In der IT-Sicherheitsbewertung wird deshalb eine starke binäre Sichtweise vertreten, d. h. ein System ist entweder gesichert oder unsicher und muss in regelmäßigen Abständen geprüft werden (Kofler et al., 2018, S. 29). Darüber hinaus kann zwar eine Methode allgemein als theoretisch sicher gelten, jedoch bestimmt erst die Implementierung in Hardware bzw. Software die Sicherheit in der Praxis (BSI-Bund, 2021b).[86] State-of-the-Art-Sicherungsmechanismen gelten als hinreichend sicher, solange keine neuen, ausbeutbaren Schwachstellen (sog. Zero Days) veröffentlicht werden, z. B. bei der National Vulnerability Database (NIST, 2021; Kofler et al., 2018, S. 47-48). Hier könnte es ebenfalls direkt Maßnahmen zur Begegnung solcher Fälle geben, z. B. in Form eines Administrators, der in Foren unterwegs ist und damit sofort mitbekommt, wenn es veröffentlichte Zero Days gibt. Durch die Up-to-Date-Sein-Maßnahme kann die Reaktionszeit generell optimiert werden, sodass eine Aufrüstung des eigenen Systems möglich ist. Es wird jedoch grundsätzlich immer eine Verzögerung zwischen der Detektion und der Umsetzung (Implementierung eines Fixes) geben (First.org, 2022).

8.2.2 Struktur und Eigenschaften des physischen Layers

Physische Sicherheit, auch Objektschutz genannt, ist ein elementarer Bestandteil der IT-Sicherheit, da Elemente zur Speicherung, Verarbeitung und Übertragung von Daten an physische Hardware gebunden sind (Anderson, 2001, S. 365-388). Ziel der physischen Sicherheit ist es, durch Einsatz von Technologien Personen, Eigentum und Vermögenswerte, zu denen auch Daten-Assets gehören, zu schützen (Garcia, 2007, S. 8). Physische Assets sind schützenswerte Güter von Wert für einen Betreiber oder einen Benutzer (Klipper, 2015, S.75). Kriminalitätsprävention kann allgemein durch „Environmental Design" (Fennelly et al., 2016, S. 4) erfolgen. Bei der Bewertung physischer Security wird physisches Risiko anhand der physischen Vulnerabilität betrachtet, d. h. es werden die Eigenschaften und Mechanismen zur Protektion, Observation respektive Detektion und Intervention im Falle eines physischen Angreifers im Use Case bewertet (Fennelly et al., 2016, S. 18). Dafür wird das Zusammenspiel aus physischen Barrieren, Sensoren und der Bearbeitung von Alarmen betrachtet (Garcia, 2007, S. 87). Physische Zu-

[86] Dass eine unzureichend sichere Implementierung geschäftsrelevante Folgen haben kann, zeigt insbesondere der Artikel von ZDNet (Cimpanu, 2020). Der Quellcode für Smart-Car-Komponenten von Mercedes-Benz-Kleintransportern wurde, so die Nachrichten-Webseite ZDNet, online „geleakt". Dieser Leak entstand, nachdem Till Kottmann, ein Software-Ingenieur aus der Schweiz, ein sog. Git-Webportal der Mercedes-Benz AG entdeckt hatte. „Kottmann sagte gegenüber ZDNet, dass er in der Lage war, ein Konto auf dem Code-Hosting-Portal von Daimler zu registrieren und dann mehr als 580 Git-Repositories herunterzuladen, die den Quellcode von Onboard Logic Units (OLU) enthalten, die in Mercedes-Transportern installiert sind", schreibt Cimpanu auf ZDNet (Cimpanu, 2020). Problematisch an diesem Leak war, dass keine der Repositories eine Open-Source-Lizenz besaß, d. h. es handelt sich um geschützte Informationen, die nicht für die Öffentlichkeit bestimmt waren. In der Vulnerabilitätsbewertung von MAS muss sich solch ein Szenario wiederfinden lassen.

gangssysteme machen als Komfortklappe die Nutzung eines Fahrzeugs erst möglich. Zugangssysteme werden in der physischen Welt benötigt, um sicherzustellen, dass nur berechtigte Personen Zugang zu physischen Assets erhalten. Hierbei können unterschiedliche Möglichkeiten zum Einsatz kommen, um die Berechtigung zum physischen Zugang nachzuweisen, z. B. biometrisch (Merkmal), mechanisch (Besitz/Wissen) oder kontaktlos (Wissen, z. B. Losungsworte) (Pohlmann, 2021).

Das grundlegende Prinzip physischer Sicherheit wird als Defense in Depth (DiD) oder auch als Protection in Depth (PiD) bezeichnet (Harnser, 2010, C3, S.14; Garcia, 2007, S. 59). Physische Barrieren sind, ähnlich Zwiebelschalen, topologisch hintereinander angeordnet und umschließen das physische Asset im Nukleus. Jede Barriere ist mit einem oder mehreren Zugangssystemen ausgestattet. Bei der Bewertung physischer Bedrohungen werden Angriffspfade durch die Barrieren bis zum physischen Asset betrachtet (Harnser, 2010, B4, S. 50). Es geht bei der physischen Sicherheit darum, wie Assets mit Barrieren ausgestattet werden müssen, sodass konkrete Angreifer so lange wie möglich aufgehalten werden können, damit noch eine rechtzeitige Intervention seitens des physischen Verteidigers ermöglicht werden kann. In Harnser (2010, S. 7) wird dieser Schritt in der Design-Phase, auch „Konzeptionierung" (von Sicherheitsmaßnahmen) genannt, vorgenommen. Angreifer können ferner bei der Realisation eines Angriffs erkannt werden, insofern geeignete Detektionsmaßnahmen vorhanden sind. Sensorsysteme beispielsweise erkennen, ob sich jemand nähert oder versucht, sich (missbräuchlich) physischen Zugang zu etwas zu verschaffen (Harnser, 2010, C3, S. 17).

Zu berücksichtigen ist beispielsweise die Fehlerrate von Detektionsmaßnahmen (BHE, 2021). Wird ein Angreifer rechtzeitig erkannt, dann kann potenziell noch interveniert werden, bevor der Angreifer sein Ziel erreicht. Was nach einem Angriff passieren kann, wird insbesondere bei kritischen Infrastrukturen (KRITIS) bewertet (Harnser, 2010, B3, S. 40). In dem klassischen Vulnerabilitätsmodell, wie in Garcia (2005) und Lichte et al. (2016) vorgeschlagen, wird der Angriffsprozess nur bis zur Asset-Erreichung bewertet. Ein Teil der betrachteten Bestandteile des physischen Wirkmechanismus in der physischen Sicherheit ist die Überwachung. Zunächst ist dafür eine Observation notwendig, d. h. durch Technologien oder Menschen muss kontinuierlich überprüft werden, ob ein potenzieller Angriff stattfindet (Lichte et al., 2016). Observation ist also eine Art Identifikation in der Form, dass etwas wahrgenommen wird, was zur Bedrohung werden kann. Wird ein Angriff dann tatsächlich durchgeführt, muss dieser als solcher erkannt werden. Das ist wiederum die Detektion (Garcia, 2007, S. 58). Erst wenn eine Detektion erfolgt, kann eine Intervention eingeleitet werden, z. B. in Form einer eingreifenden Wachmannschaft (Harnser, 2010, B4, S. 47). Der Angreifer muss lange genug aufgehalten werden, sodass er entweder von selbst von seinem Vorhaben ablässt oder von einer Interventionseinheit aufgehalten wird. Der Wirkmechanismus, der hierbei betrachtet wird, ist die Protektion (Harnser, 2010, B4, S. 47).

Protektion kann durch Schutzmaßnahmen erreicht werden, wie beispielsweise mittels einer Panzerung an einer Tür. Im Gegensatz zu einer Schutzmaßnahme, die sich auf den Zustand einer Barriere bezieht, um das Eindringen zu erschweren („Tür geschlossen"), beschreibt eine Sicherungsmaßnahme, dass die Barriere überhaupt vorhanden ist bzw. diese eine bestimmte Vulnerabilität hat („Fenster von definierter Sicherheitsstufe eingebaut") (Harnser, 2010, C2, S.10). Der Zugangskontrolle sowie der Authentifikation von Benutzern mittels Zugangssystemen kommt eine entscheidende Rolle zu (Harnser, 2010, C3, S.15). Die Sicherheitsfunktion der mit einem physischen System verbundenen Komponenten wird über Metriken bewertet. Ein physischer Angriff kann durch einen zeitlichen Ablauf beschrieben werden, im Zuge dessen der Angreifer eine definierte Anzahl an n Barrieren überwinden muss, um an das physische Asset zu gelangen (Garcia, 2007, S. 58) (siehe Abbildung 69).

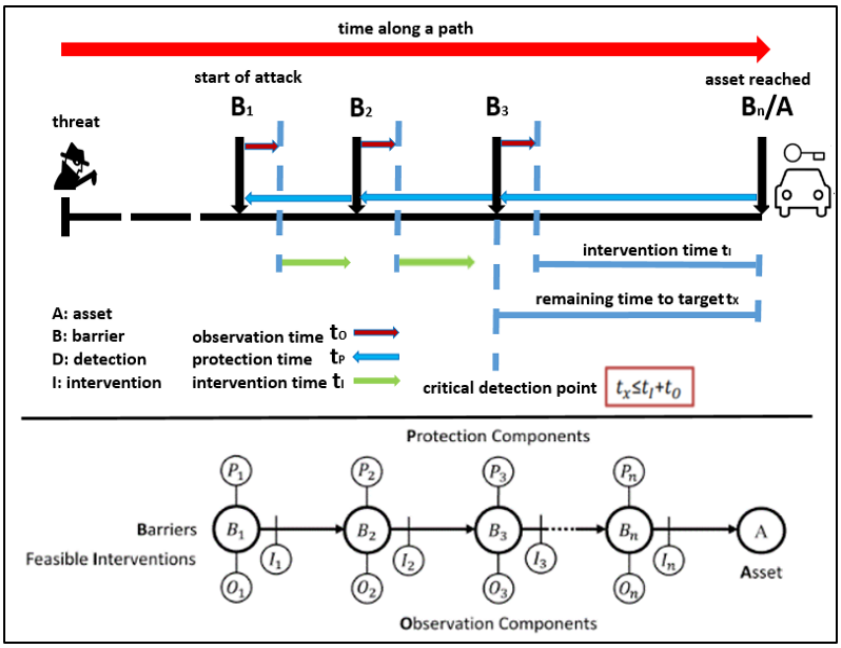


Abbildung 69: Physisches Vulnerabilitätsmodell.
Quelle: Eigene Abbildung in Anlehnung an Garcia (2005) und Lichte et al. (2017); Bildquelle: Flaticon.com (2021) und Flinkey.de (2021).

Barrieren verzögern, dass ein Angreifer sein Ziel erreicht. Wird der Angreifer früh detektiert, hat der Verteidiger noch genug Zeit, entsprechende Interventionsmaßnahmen einzuleiten. Die mittlere Interventionszeit muss hierbei kleiner als die sog. Restüberwindungszeit des Angreifers sein (Lichte et al., 2016). Die Restüberwindungszeit ist die Zeit, die der Interventionseinheit noch bleibt, um den Angreifer von seinem Vorhaben abzubringen, bevor er dem Asset Schaden zufügen oder dieses entwenden kann. Es wird in der physischen Sicherheit folglich das Zeitspiel zwischen der Eindringzeit und der Reaktionszeit bewertet. Im Umkehrschluss heißt das: Wenn die Intervention zu lange dauert, muss sich beispielsweise der Betreiber überlegen, welche Maßnahmen in welcher Form – d. h. mit welcher Wirksamkeit – getroffen werden müssen, sodass der Angreifer am Erfolg gehindert werden kann (Garcia, 2007, S. 58, 66).

Das ist bei der prospektiven Analyse z. B. mittels der Szenario-Technik wichtig, da dann noch die Chance besteht, das System hinsichtlich der Vulnerabilität zu optimieren, bevor ein Worst Case Ereignis eingetreten ist. Es geht bei der Risikoanalyse zunächst um die Identifikation von möglichen Schwachstellen bzw. vulnerablen Pfaden, die durch den Angreifer ausgenutzt werden können (Klipper, 2015, S. 97-106). Dabei kann grundsätzlich davon ausgegangen werden, dass der Angreifer sich vor dem Angriff mit Wegen zur Zielerreichung auseinandersetzt und er den schwächsten Pfad wählt (Ingoldsby, 2016). Das physische Sicherheitsmanagement und das IT-Sicherheitsmanagement orientieren sich beide am Plan-Do-Check-Act-Modell (PDCA) (BSI, 2020, S. 93; Fennelly et al., 2016, S. 5; Schwerdtfeger, 2018, S. 21).

8.3 Domänenübergreifende Zusammenführung in anderen Disziplinen

Die Problematik der Angleichung und Zusammenführung von Metriken aus zwei Domänen ist auch außerhalb der Sicherheitsforschung zu beobachten, z. B. in der Physik. Es wird daran gearbeitet, eine „Weltformel" zu entwickeln. Ziel der Physik ist es, ein universelles Modell zu finden, mit der alle grundlegenden Wechselwirkungen zwischen den Grundkräften der Physik (Gravitation, Elektromagnetismus, schwache Wechselwirkung sowie starke Wechselwirkung) erklärt und in einer Theorie zusammengeführt werden können (Laughlin et al., 2000). Hierbei gibt es jedoch ebenso Hürden, wie das nachfolgende Beispiel kurz skizziert: Die Grundkraft Schwerkraft ist gem. Einsteins Relativitätstheorie eine Theorie der Geometrie von Raum und Zeit, auch Raumzeit genannt. Es geht dabei vereinfacht um Distanzen, die quantitativ genau gemessen werden können. Das ist in der Welt des Großen gut möglich. In der Welt des ganz Kleinen, der Quantenwelt, können sowohl die Distanzen zwischen sog. Punktteilchen[87] als auch die Geschwindigkeiten dieser Teilchen nicht genau gemessen werden (Conlon, 2016, S. 11-20). In diesem Zusammenhang wird von der sog. Unschärferelation gesprochen. Aus diesem Grund ist die Theorie der Schwerkraft, einfach gesagt, nicht mit der Quantentheorie kompatibel.

In der Physik wurde deswegen die Theorie der Strings eingeführt. Elementarteilchen und auch die Schwerkraft können laut dieser Theorie über Schwingungsformen eines Strings beschrieben werden (Conlon, 2016, S. 67). Zwar wurde diese Theorie zunächst als mögliche Weltformel populär, jedoch funktioniert eine mathematisch konsistente String-Theorie nicht in dem Universum, wie es Einstein mit drei räumlichen und einer zeitlichen Dimension beschrieben hat. Es sind insgesamt zehn Dimensionen möglich. Aussagen der String-Theorie konnten bisher nicht experimentell nachgewiesen werden (Conlon, 2016, S. 107-208). Auf Basis dessen wurden theoretische Modelluniversen konstruiert, in denen die Springtheorie angewandt werden konnte (Woit, 2011). Es wurde überlegt, die sechs überzähligen Dimensionen herauszustreichen, um das bekannte Universum abzubilden. Das ist jedoch nicht gelungen. In Hawking & Mlodinow (2010) wird die Weltformel daher als „schwer fassbar" bezeichnet. Schlussfolgernd liegen vergleichbare Herausforderung in der Zusammenführung von Metriken, wie sie in dieser Arbeit am Beispiel Physical Security und IT Security dargelegt werden, ebenfalls in anderen Domänen vor.

[87] Punktteilchen bedeutet vereinfacht, dass Teilchen als Punkte im Raum interpretiert werden. Über die individuelle Masse und Ladung von Teilchen können präzise Wechselwirkungen berechnet werden.

Lebenslauf

Der Lebenslauf ist aus Gründen des Datenschutzes nicht enthalten.

Konferenzen

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). Hrsg. von Mário P. Brito, Terje Aven, Piero Baraldi, Marko Cépin und 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). Hrsg. von 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*; 28. November 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, 19.-23. Sept. 2021). Hrsg. von 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, 1.–6. Nov. 2020). Hrsg. von 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, 1.–6. Nov. 2020). Hrsg. von P. Baraldi; F. Di Maio; E. Zio; ISBN / doi: 978-9981-14-8593-0.

Gastbeiträge

Mühl, Kim Y. (2020). AGILITÄT & OPEN SOURCE FÜR EINE ERFOLGREICHE DIGITALE TRANSFORMATION, *In: Bionic Wealth: Die nächste Generation der Vermögensanlage ist inspiriert vom Leben.* S. 130-133. Self-Publishing.

Mutschler, A., Alexandropoulos, K., Termin, T., & weitere (2023). Research Paper AUTOMOTIVE. Why you should reorient your automotive business model, now. *20blue edition*. 20blue Projekt GmbH 2023.