BERGISCHE
UNIVERSITÄT
WUPPERTAL

Partizipatives Modell zur Evaluierung und Priorisierung von informationstechnischen Schwachstellen und Verwundbarkeiten in Prozess-Netzwerken der technischen Basisinfrastrukturen

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

in der
Fakultät für Maschinenbau und Sicherheitstechnik

der

Bergischen Universität Wuppertal

vorgelegt von
Erfan Koza M. Sc.
aus Teheran

Wuppertal 2024

Meiner lieben Mutter gewidmet.

Kurzfassung

Die Bewertung von Hard- und Softwareschwachstellen in der Operational Technology (OT), respektive industriellen Steuerungs- und Überwachungssystemen, ist auf vielfältige Weise eine Herausforderung, insbesondere im Kontext von Kritischen Infrastrukturen. In der Praxis unterstützen verschiedene internationale Standards und Tools das Schwachstellenmanagement und das Incident Response Management, um ein systematisches Vorgehen zum frühzeitigen Erkennen von Vulnerabilitäten sowie deren Priorisierung auf Basis der vorhandenen Kritikalität zu ermöglichen. Allerdings reicht es in der Regel nicht aus, nur die theoretischen Konzepte der internationalen Normen und Standards zu verstehen. Entscheidend für das Erreichen der in diesen Konzepten angestrebten Ergebnissen ist die Frage, wie ein Verfahren mit mehreren Methoden, ein Rahmenwerk oder ein Standard in einem praktischen Kontext umgesetzt wird. Eine wesentliche Aufgabe kommt der Effizienz der Modelle und Werkzeuge zu, welche letztlich für die Umsetzung und Erfüllung der Standards von essenzieller Natur sind. In der hier geführten wissenschaftlichen Debatte wird ein Kohärenzmodell und das dazugehörige Incident Response Evaluation Tool (IRET) vorgestellt, welches primär für OT-Netzwerke in der Energie- und Wasserwirtschaft entwickelt und in einer industriellen Umgebung bezüglich Machbarkeit und Validität evaluiert wurde. IRET ermöglicht die Bewertung von Schwachstellen und CVE in OT-Netzwerken anhand objektiver und system-, architektur- und anwendungsbasierter Fakten zu treffen und die Entscheidungsfindungsprozesse somit unabhängig der subjektiven Wahrnehmung, Salienz und Verhaltensabsicht der einzelnen Entscheidungsträger zu ermöglichen. IRET hilft insbesondere hierbei, die Anzahl der False Positives, aber auch gleichzeitig die Anzahl der False Negatives zu reduzieren, um auch die endlichen Kapazitäten an personellen, fachlichen und finanziellen Ressourcen zielgerichtet zur Behebung von True Positives einzusetzen. Hierbei dient die modifizierte Observe-Orient-Decide-Act-Schleife als Hauptrahmen für IRET, um das Kohärenzmodell in den Kontext des Schwachstellenmanagements der Institutionen zu integrieren.

Summary

The assessment of hardware and software vulnerabilities in Operational Technology (OT), which are industrial control and monitoring systems, is challenging in many ways, especially in the context of Critical Infrastructure. In practice, various international standards and tools support vulnerability management and incident response management to enable a systematic approach for the early detection of vulnerabilities and their prioritization based on existing criticality. However, it is usually insufficient to understand only the theoretical concepts of international norms and standards. Important to achieving the outcomes is the question of how a method or standard is integrated in a practical context. Operationally efficient models and tools, which are ultimately responsible for the implementation of standards, play an essential role here. This dissertation presents a coherence model and the corresponding Incident Response Evaluation Tool (IRET), which was primarily developed for OT networks in the energy and water industries and evaluated in an industrial environment with respect to feasibility and validity. IRET enables the assessment of vulnerabilities and CVE in OT networks based on objective, system, architecture, and application-based facts, thus enabling decision-making processes that are independent of the subjective perception, salience, and behavioral intent of individual decision makers. IRET helps to reduce the number of false positives, but also at the same time the number of false negatives, to use the finite capacities of human, technical, and financial resources in a targeted manner to eliminate true positives. The modified Observe-Orient-Decide-Act loop serves as the main framework for IRET to integrate the coherence model into the context of institutional vulnerability management.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABU	Abwasserbeseitigungsunternehmen
BAO	Besondere Aufbauorganisation
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDEW	Bundesverband der Energie- und Wasserwirtschaft e. V.
BMI	Bundesministerium des Innern
BNetzA	Bundesnetzagentur
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
B3S	Branchenspezifischer Sicherheitsstandard
CERT	Computer Emergency Response Team
CIS CSC	Center for Internet Security Critical Security Controls
CVE	Common Vulnerabilities und Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DIN	Deutsches Institut für Normung e.V.
DIS	Draft International Standard
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik
DMZ	Demilitarisierte Zone
DVGW	Deutscher Verein des Gas- und Wasserfaches e.V.
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V.
eEPK	erweiterte, ereignisgesteuerte Prozesskette
EN	Europäische Norm
ENWG	Energiewirtschaftsgesetz
EPSS	Exploit Prediction Scoring System
ERP	Enterprise Resource Planning

EVU	Energieversorgungsunternehmen
FDIS	Final Draft International Standard
FIRST	Forum of Incident Response and Security Teams
FL	Forschungsleitlinie
FN	False Negative
FP	False Positive
gDoA	global Definition of Applicability
HMI	Human-Machine-Interface
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IKT	Informations- und Kommunikationstechnik
IP	Internetprotokoll
IRET	Incident Response Management Tool
IRM	Incident Response Management
IRT	Incident Response Team
ISA	International Society of Automation
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
IT-SiG	IT-Sicherheitsgesetz
KMU	Kleine und mittlere Unternehmen
KPI	Key Performance Indicators
KRITIS	Kritische Infrastrukturen
LAN	Local Area Network
MES	Manufacturing Execution Systems
MOM	Manufactoring Operation Management
MS	Microsoft
MTU	Master Terminal Unit

NAMUR	Normenarbeitsgemeinschaft für Mess- und Regeltechnik
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIAC	National Infrastructure Advisory Council
NIST CSF	National Institute of Standards and Technology Cyber Security Framework
NIST SP	National Institute of Standards and Technology Special Publication
NVD	National Vulnerability Database
OODA	Observe, Orient, Decide Act
OSI	Open Systems Interconnection
OT	Operational Technology
P-A-P	Paketfilter-Application-Level Gateway-Proxies
PDCA	Plan, Do, Check, Act
PERA	Purdue Enterprise Reference Architecture
POC	Proof-of-Concept
PS	Prozessschritt
RM	Risikomanagement
RMF	Risk Management Framework
SCADA	Supervisory Control and Data Acquisition
SPOF	Single Point of Failure
SPS	Speicherprogrammierbare Steuerungen
TN	True Negative
TP	True Positive
TCP	Transmission Control Protocol
UKD	Universitätsklinikum Düsseldorf
UML	Unified Modeling Language
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen
ÜNB	Übertragungsnetzbetreiber
VBA	Visual Basic for Application
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VDI	Verein Deutscher Ingenieure e. V.

VM	Vulnerability Management
VNB	Verteilnetzbetreiber
VPN	Virtual Private Network
WAN	Wide Area Networks
WHG	Wasserhaushaltsgesetz
WIP	Work in Progress
WVU	Wasserversorgungsunternehmen

1. Einleitung

„Polizei ermittelt nach Hacker-Angriff in einem Todesfall“ (Ernst, 2020, o. S.). So lautete die Aufmachung der Süddeutschen Zeitung am 17.09.2020, nach dem das Universitätsklinikum Düsseldorf (UKD) am 09. September 2020 Opfer eines Ransomware-Angriffs wurde. Im Falle des UKD haben Cyberkriminelle eine logische Schwachstelle in der Citrix-Umgebung des UKD ausgenutzt und die internen Systeme mit einem Loader infiltriert, um diese später am sogenannten „Action Day“ zu reaktivieren und den Verschlüsselungstrojaner nachzuladen. In der Folge waren die UKD-Daten verschlüsselt und das Krankenhausinformationssystem war außer Kraft gesetzt (vgl. UKD, 2020, o. S. | Krempl, 2022, o. S.). Das UKD ist jedoch kein Einzelfall. Bereits im Jahre 2017 erschütterte ein weltweit koordinierter Ransomware-Angriff namens „WannaCry“ über 150 Länder und 200.000 Unternehmen. Auch in Europa waren zahlreiche Unternehmen, darunter auch das Logistikunternehmen Deutsche Bahn Schenker, der Automobilkonzern Renault sowie der Telekommunikationskonzern Telefónica, Opfer dieses Cyberangriffs (vgl. Neller et al., 2017, o. S.).

Die Konsequenzen derartiger Kompromittierungen bewegen sich monetär in einem sechsstelligen Bereich und erstrecken sich sogar bis hin zu nicht messbaren Schäden, wie bspw. Gefahr für Leib und Leben oder auch Gefahr der Unterbrechung der Versorgungkontinuität von kritischen Dienstleistungen wie der „Patientenversorgung“. Wird die digitale Anfälligkeit der Kritischen Infrastrukturen (KRITIS) in den Vordergrund der Betrachtung gestellt, so zeigt sich, dass KRITIS vor einigen Herausforderungen, insbesondere im Bereich des Schwachstellenmanagements und den damit verbundenen Prozessen wie der Evaluierung, Priorisierung und Behebung derartiger systemkritischer Verwundbarkeiten stehen. Hier fehlt es an personellen und technischen Ressourcen, um der ständig wachsenden Fragilität und Vulnerabilität der KRITIS im Kontext der Informationssicherheit entgegenwirken zu können.

Welche der identifizierten Schwachstellen in den eigesetzten Hard- und Softwareprodukten wie bspw. in den Netzleit- und Prozessleitsystemen sollen unverzüglich oder rechtzeitig beseitigt und behandelt werden? Das ist die wichtigste Frage im Bereich des Vulnerability Managements (VM) der informationstechnischen Systeme. Das erste Dilemma hierbei ist allerdings, dass praktisch jeden Tag neue Schwachstellen in den einzelnen Systemen entdeckt und bekannt werden. Diese identifizierten globalen Schwachstellen sind jedoch unterschiedlicher Herkunft und werden somit – wohlgemerkt global – unterschiedlich nach der erreichten Kritikalität bewertet. Das zweite Dilemma beschreibt die Tatsache, dass gegenüber der Vielzahl der entdeckten und bewerteten Schwachstellen eine endliche Kapazität an personellen und finanziellen Ressourcen zur Verfügung stehen, die nur für die Beseitigung eines Bruchteiles der entdeckten Schwachstellen ausreicht. Dem ersten und zweiten Dilemma folgt nun die Hauptaufgabe: Wie können KRITIS eine Priorisierungsstrategie entwickeln, mit dessen Hilfe sie nun befähigt werden, ihre wichtigen und kritischsten Schwachstellen, also die, die als Verwundbarkeiten gelten, gegenüber nicht kritischen Schwachstellen auszudifferenzieren? Denn nicht jede Schwachstelle kann und muss unmittelbar zu einer direkten oder indirekten Ausnutzung oder zu Systemkompromittierungen führen.

1.2 Motivation

Eine Vielzahl von informationstechnischen Systemen zur Überwachung und Steuerung von industriellen Prozessen und Anlagen interagiert in einem globalen Netzwerk mit 24/7-Verfügbarkeit und ist in ein bi- oder multidirektionales Kommunikationsnetz eingebettet. Solche informationstechnischen Systeme werden aus einem wichtigen Grund eingesetzt: zur Sicherung der wirtschaftlichen Prosperität, die durch Prozessoptimierung, Effizienzsteigerung und Senkung der Produktions- und Personalkosten in Einklang gebracht werden kann. Hierbei wird die Funktion eines Systems, das zu einer Effizienzsteigerung führen soll, in den Vordergrund gestellt. Dabei werden allerdings einige Sicherheitsbetrachtungen außer Acht gelassen: Ist die Software sicher kodiert? Haben die Entwickler methodische Ansätze zur Entwicklung sicherer Systeme berücksichtigt (z.B. Security by Design)? Wurden die Systeme im Hinblick auf ihre funktionale Sicherheit getestet? Denn solche Sicherheitsprozesse führen zu steigenden Entwicklungszeiten und -kosten und verteuern die Produkte. Werden nun die Mechanismen in der freien Marktwirtschaft betrachtet, so könnte das folgende Postulat aufgestellt werden: Wenn es keine Nachfrage nach sicherer Informationstechnik (IT) gibt, wird es auch kein Angebot dafür geben. Die Folgen, unabhängig davon, wer an diesem Dilemma die Schuld trägt, spiegeln sich in der Anfälligkeit und Verwundbarkeit dieser Systeme wider.

KRITIS wenden viele Soft- und Hardwareprodukte an, deren Sicherheitsniveau aufgrund von Codierungsfehlern, unsicheren Schnittstellen, logischen Schwachstellen oft als unzureichend bezeichnet werden kann. Daher sind das VM und Incident Response Management (IRM) Schlüsselthemen für die Verteidigung von Operational Technology (OT) und IT-Systemen. Bei VM und IRM werden gezielte Prinzipien und Anforderungen entwickelt, um potenzielle Schwachstellen und die daraus resultierenden Bedrohungen zu erkennen, bevor sie ausgenutzt werden.

Die gegenwärtigen Sicherheitspraktiken und -standards in VM und IRM beschreiben, was getan werden muss. Sie gehen jedoch nicht darauf ein, wie solche Schwachstellen individuell anhand von objektiven Kriterien priorisiert und behandelt werden müssen. Bevor solche Schwachstellen behoben werden können, müssen sie zunächst erkannt werden.

Diese Erkennung kann intern (innerhalb der Grenzen einer Organisation) mit Hilfe von Intrusion Detection Prevention Systemen oder Security Information Event Management Systemen durchgeführt werden. Für die globale Erkennung solcher Schwachstellen existiert das so genannte Common Vulnerability Scoring System (CVSS), ein System, das Schwachstellen weltweit unter dem Begriff Common Vulnerabilities and Exposures (CVE) identifiziert und mit einem globalen Rating in einem Skalensystem von 0-10 nach ihren Schadensauswirkungen nach dem Prinzip „one size fits all“ quantifiziert. Allerdings ist hier zu berücksichtigen, dass die globale CVE-Bewertung nur einen Orientierungsrahmen darstellt, der eine organisationsspezifische Bewertung und Priorisierung mit Bezug auf die eigene OT-Netzwerklandschaft erfordert.

Folglich gibt es ein paar grundlegende Problematiken, wenn es um die Behebung von Schwachstellen in den IT- und OT-Systemen geht. Erstens existieren zu viele Schwachstellen, um sie sofort zu beheben. Zweitens können Unternehmen auf Grund ihres endlichen Kontingents und ihren Kapazitäten nur einen marginalen Anteil der bekannten Schwachstellen innerhalb eines Monats bzw. einer festgelegten Periode beheben. Drittens wird nur ein kleiner Teil der veröffentlichten Schwachstellen auch tatsächlich in der Praxis ausgenutzt. Daraus ergibt sich der Bedarf an guten Priorisierungsmethoden- und -strategien, da ohne diese Priorisierungen von Schwachstellen, KRITIS unpräzise Bewertungen haben, die möglicherweise zu umfangreichen Abhilfemaßnahmen führen, die nicht notwendig sind. So verpassen die KRITIS es, genau die Schwachstellen zu beheben, die für ihre Prozesse wirklich kritisch sind. Das Ergebnis ist: Viel Aufwand, minimale Resilienz.

1.3 Zielsetzung

OT-Netzwerke stellen im Vergleich zu klassischen Büro-Netzwerken (IT) ein komplexes Betrachtungsfeld dar. OT-Komponenten werden in der Regel zur zentralen und dezentralen Steuerung und Überwachung von Anlagen, Maschinen, Aggregaten etc. eingesetzt. Es findet also eine interdisziplinäre und vertikale Vernetzung der Elektrotechnik und IT statt.

Der aus dieser Vernetzung generierte Nutzen führt zu einer Kostenminimierung, Prozessagilität sowie Prozesszuverlässigkeit. Dadurch entsteht jedoch auch eine Steigerung der IKT-Abhängigkeit, die unter anderem dazu führen kann, dass der Ausfall oder die Beeinträchtigung der Informations- und Kommunikationstechnik (IKT) einen unmittelbaren Einfluss auf die Prozessverfügbarkeit haben. Durch die steigende Komplexität der OT-Netzwerke, Heterogenität der eingesetzten Software- und Hardwarekomponenten sowie der zuvor beschriebenen IKT-Dependenz gewinnt der Schutz der OT-Netzwerke zur Erhöhung der Resilienz dieser Systeme zunehmend an Bedeutung. Die Entscheidung zur Sicherstellung und Aufrechterhaltung der OT-Netzwerke spiegelt jedoch die Effektivität, also „das Richtige tun“ dar.

Diese Effektivität kann mit der Einführung von sicherheitstechnischen Regelwerken wie bspw. der Implementierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß der internationalen Norm ISO/IEC 27001 oder auch des nationalen Standards IT-Grundschutz-Kompendiums erfolgen (vgl. Koza, 2021, S. 820).

Die Effizienz dieser Entscheidung erfolgt durch die wirksame Umsetzung der Sicherheitsmechanismen. Diese Sichtweise beschreibt die Maxime „das Richtige richtig tun.“ Daraus ergibt sich eine Kernanforderung, die eine essenzielle Rolle beim nachhaltigen und wirksamen Schutz der OT-Netzwerke darstellt. Die Effizienz der Maßnahmen in den OT-Netzwerken kann nicht in der Analogie zu Büro-Netzwerken betrachtet werden. Die klassischen Lösungsansätze, Präventionen und Mechanismen der Büro-Netzwerke greifen nur bedingt, da der strukturelle Aufbau der OT-Netzwerke, die Kommunikationsprotokolle, die personellen und fachlichen Kapazitäten sowie die Art der operativen Ausführung der IT-Tätigkeiten, wie bspw. die Konfiguration, Administration und Wartung der Systeme in OT-Netzwerken anders durchgeführt werden.

Um die Effizienz der Maßnahmen sicherstellen zu können, müssen der Umfang und die Tiefe dieser Maßnahmen genauer definiert werden. Zudem muss bestimmt werden, welche fachlichen und zeitlichen Aufwände entstehen und vor allem welche möglichen negativen Folgen sich ergeben können.

Diese Betrachtung gewinnt insbesondere dann eine Bedeutung, wenn die Cybersicherheitsingenieure in den OT-Netzwerken vor der Entscheidung stehen, welche der anfallenden Sicherheitsmeldungen und identifizierten Schwachstellen sofort oder zeitnah behandelt werden müssen, um die personellen und fachlichen Kapazitäten effizient einzusetzen. Hierbei geht es primär um die Aufrechterhaltung und Sicherstellung der Betriebsfähigkeit der Prozesse, also um die Aspekte des IRM: Umgang mit den Schwachstellen.

Um diese Entscheidung auf Faktenbasis validierbar und nachvollziehbar treffen zu können, müssen die Entscheidungskriterien, die Zusammenhänge und die Dependenzen der einzelnen Kriterien untereinander und deren wechselseitigen Auswirkungen in ein Metamodell integriert werden, um hieraus ein adaptives Entscheidungsmodell entwickeln zu können.

Die Zielsetzung dieses Entscheidungsmodells ist es, den Fachanwendern die objektiven Kriterien zur Kategorisierung und Priorisierung der Schwachstellen nach der Kritikalität der Zeit, Ausfallfolgen und Aufwandabschätzung in einem Modell zur Verfügung zu stellen, mit dessen Hilfe sie ihre anfallenden Sicherheitsmeldungen individuell bewerten und zur operativen Umsetzung initiieren können.

Hierfür wurde ein Ausführungstool entwickelt und unter reellen Bedingungen getestet. Das Ausführungstool dient in diesem Zusammenhang als ein intelligenter Lösungsansatz, um die Machbarkeit und Korrektheit des Kohärenzmodells durch die Cybersicherheitsingenieure und Netzwerkanalysten zu evaluieren. Ferner dient dieses Tool ebenfalls als Effizienzfaktor, mit dessen Hilfe die Prozesse zur Erfassung, Bewertung und Dokumentierung der Schwachstellen beschleunigt werden und damit wirksame Zeitersparnisse in den jeweiligen Bewertungs- und Priorisierungsprozess erfolgen.

Weitere Betrachtungen bzgl. einer vollständig-automatisierten Lösung, der Zusammenführung von mehreren unterschiedlichen Ereignissen, darunter die physische und umgebungsbezogene Sabotage oder auch Meldungen über unternehmenseigene Informationssicherheitsvorfall-Meldewege, werden in der vorliegenden Dissertation nicht betrachtet.

1.4 Struktur der Dissertation

Um die in Abschnitt 1.2 formulierte Zielsetzung der Arbeit zu realisieren, werden die Schritte zur Darstellung des Themenfeldes, der wissenschaftlichen Einordnung, die Forschungshypothese und die Forschungsleitlinien sowie die Ergebnisse sequenziell aufgeführt. Zunächst erfolgt eine Einleitung in Kapitel 1.

In Kapitel 2 der Arbeit wird zunächst die Relevanz der Energie- und Wasserwirtschaft als KRITIS dargestellt. Zudem wird aufgeführt, welche Bedeutung die Informations-und Kommunikationstechnik für diese Sektoren hat und welche Abhängigkeiten und dadurch Gefahren existieren.

Kapitel 3 ermittelt den Stand der Forschung und stellt zudem das identifizierte Forschungsdefizit in dieser Dissertation dar. Zu diesem Zweck wird eine Dokumenten- und Inhaltsanalyse durchgeführt, die eine Übersicht über die aktuelle Forschung, Standards und Normen in der OT-Umgebung darstellt. Die wichtigsten dieser Forschungsarbeiten und -resultate, Standards und Normen werden in Unterkapiteln aufgeführt.

Die Ergebnisse werden in Kapitel 4 auf die konkrete Zielsetzung bezogen und die Forschungshypothese sowie die Forschungsleitlinien zur Überprüfung der Forschungshypothese werden formuliert. Die einzelnen Forschungsphasen werden hier in einem V-Modell illustriert. Darauffolgend werden in Kapitel 5 die Schritte der empirischen Forschung mehrteilig aufgeführt. Zunächst wird das Kohärenzmodell mit den Metaebenen und Subdeterminanten als das übergeordnete Modell vorgestellt. Im zweiten Schritt wird das Berechnungsmodell aufgeführt, mit dessen Hilfe das Kohärenzmodell zur Evaluierung von Schwachstellen und CVE operationalisiert werden kann. Anschließend erfolgt im dritten Schritt die tatsächliche Operationalisierung des Kohärenzmodells, indem die acht Standard-Subdeterminanten in das Berechnungsmodell überführt werden. Zwecks Operationalisierung wird im vorletzten Schritt des Gestaltungsprozesses die John Boyd OODA-Schleife modifiziert und als Rahmenwerk des Kohärenzmodells adaptiert.

Zudem erfolgt die Zusammenführung der bisher erreichten Ergebnisse, indem das Kohärenzmodell und die OODA-Schleife in Form einer toolbasierten Lösung (IRET) als Prototyp definiert und zwecks Evaluation in eine industrielle OT-Umgebung in der Energiewirtschaft (Kohleförderung, Energieerzeugung und Energieeinspeisung) integriert und ausgewertet werden. Dadurch werden die Machbarkeit und der empirische Nutzen des Kohärenzmodells in einer Erfolgsevaluierung ermittelt. Diese Ergebnisse werden in Kapitel 6 aufgeführt und im Anschluss konsolidiert.

Die Niederschrift schließt in Kapitel 7 mit einer kritischen Diskussion über die erreichten Ergebnisse ab und gibt einen Ausblick auf weitere Forschungsmöglichkeiten.

Bild 1 fasst die oben aufgeführten Schritte methodisch zusammen.

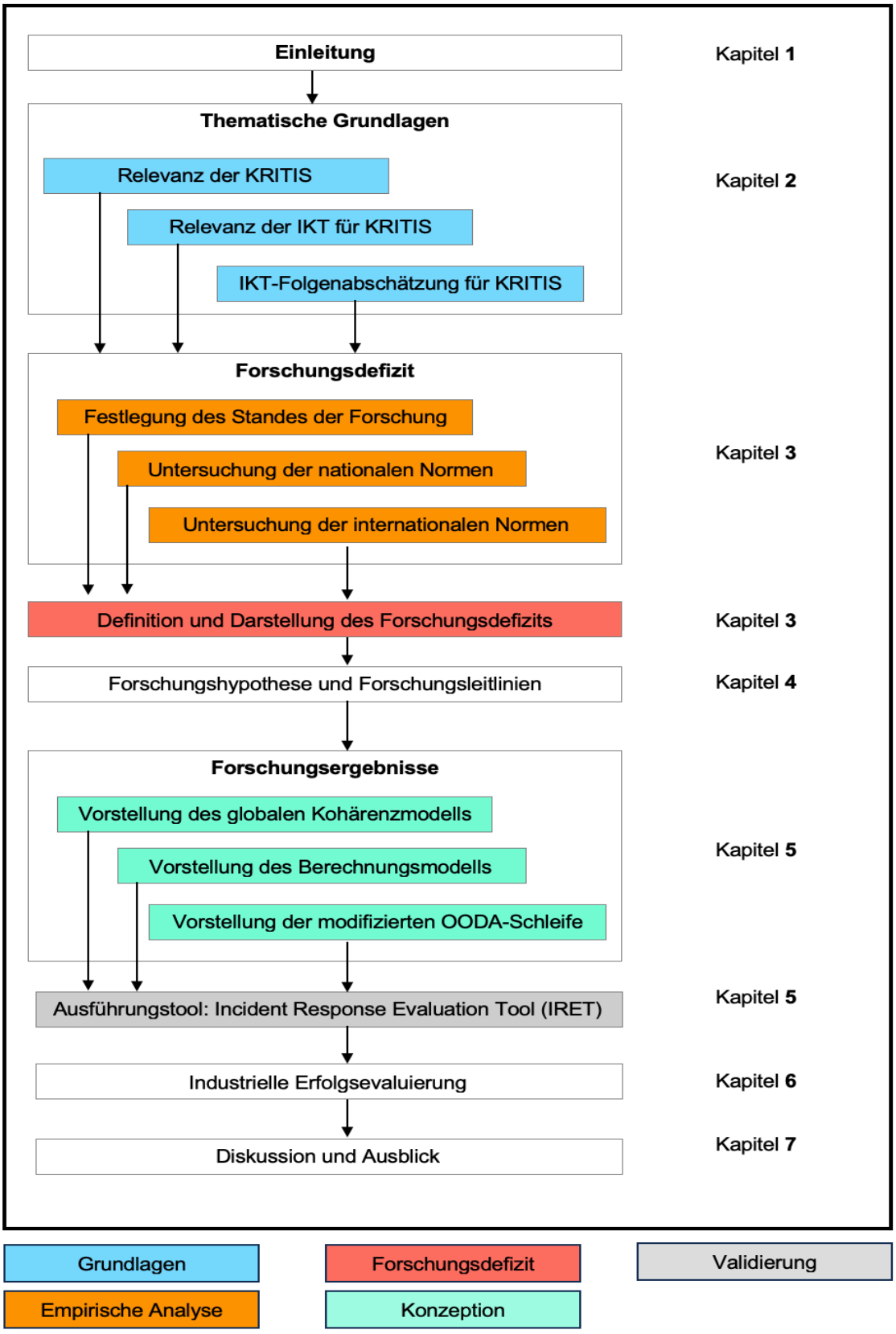


Bild 1: Struktur der Dissertation

2. Thematische Grundlagen

In den nachfolgenden Abschnitten wird eine thematische Einführung in die KRITIS gegeben. Dazu wird Bezug zu der Relevanz der Aufrechterhaltung von kritischen Dienstleistungen sowie die Sicherstellung von IKT im Energie- und Wassersektor genommen.

2.1 Relevanz der Energie- und Wasserwirtschaft als KRITIS

Das Bundesministerium des Innern und für Heimat (BMI) definiert im Dokument: „Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)“ den Begriff „KRITIS“ als „[…] Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (BMI, 2009, S. 3). Die konzeptionelle Einstufung der KRITIS lässt sich auf ihre strukturellen, funktionellen und technischen Eigenschaften zurückführen (Bild 2). Demnach werden KRITIS in zwei wesentliche Bereiche unterteilt (vgl. BMI, 2009, S. 5):

i) Technische Basisinfrastrukturen *und*
ii) Sozioökonomische Dienstleistungsstrukturen.

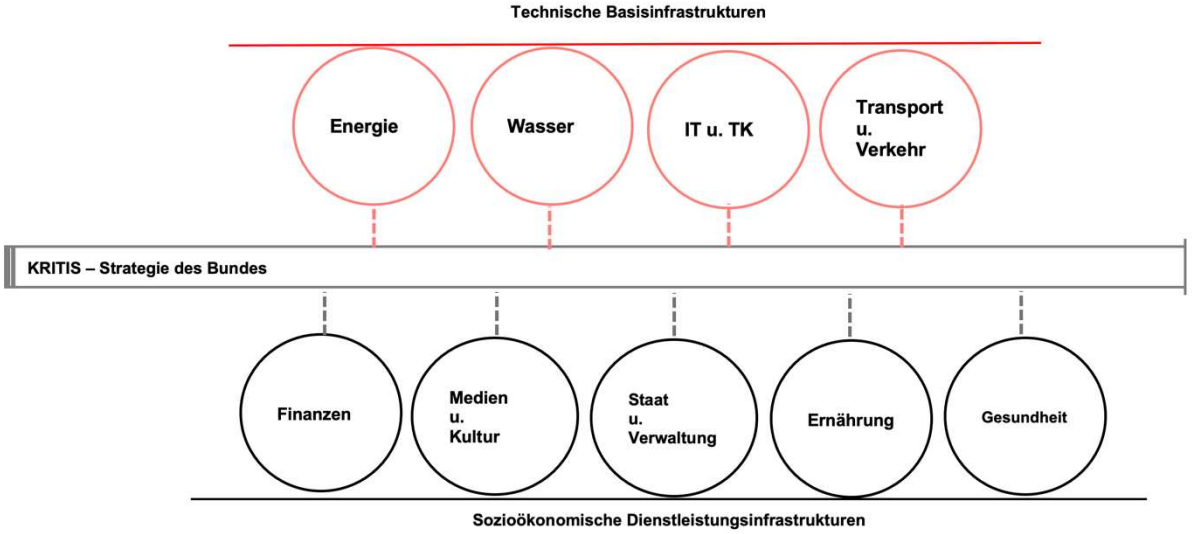


Bild 2: KRITIS-Infrastrukturbereiche (Quelle: In Anlehnung an BMI, 2009, S. 5)

Dieser Betrachtung zufolge lässt sich konstatieren, dass bspw. Energieversorgungsunternehmen (EVU), Wasserversorgungsunternehmen (WVU) und Abwasserbeseitigungsunternehmen (ABU) eine Vielzahl an kritischen Dienstleistungen erbringen, welche für die Sicherstellung und Aufrechterhaltung der technischen Basisinfrastrukturen eine bedeutende Rolle spielen.

Die „Kooperation Umsetzungsplan KRITIS“ (UP KRITIS) ist eine öffentlich-private Partnerschaft zum Schutz von KRITIS und definiert im Dokument: „UP KRITIS Grundlagen und Ziele“ den Begriff der kritischen Dienstleistungen wie folgt:

„Kritische Dienstleistungen sind für die Bevölkerung wichtige, teils lebenswichtige Güter und Dienstleistungen. Bei einer Beeinträchtigung dieser kritischen Dienstleistungen würden erhebliche Versorgungsengpässe, Störungen der Öffentlichen Sicherheit oder vergleichbare dramatische Folgen eintreten“ (UP KRITIS, 2014, S. 41).

In Anbetracht ihrer funktionellen und technischen Priorisierung im Gesamtgefüge der KRITIS werden die Sicherstellung und Aufrechterhaltung von kritischen Dienstleistungen als eine substanzielle und evolutionäre Aufgabe verstanden, dessen Zielsetzung in der nachhaltigen und effizienten Sicherstellung der Daseinsvorsorge liegt (vgl. BSI, 2015a, S. 37 | BSI, 2015b, S. 10). Vor diesem Hintergrund wird die Gewährleistung der öffentlichen (Trink-) Wasserversorgung gemäß der Definition des Wasserhaushaltgesetzes (WHG) als „eine Aufgabe der staatlichen Daseinsvorsorge“ manifestiert (§ 50 Absatz 1 WHG). Die Erfüllung dieser Aufgabenstellung wird jedoch von WVU sichergestellt, deren versorgungstechnische Relevanz auch anhand der bestehenden intra- und intersektoralen Dependenzen verdeutlicht werden kann. Während die intrasektorale Dependenz die Abhängigkeit bzw. die Folgen eines Ausfalles der kritischen Dienstleistung innerhalb des betroffenen Sektors betrachtet, umfasst der Begriff intersektorale Dependenz die Abhängigkeit und Betrachtung der Folgen eines Ausfalls auf andere kritische Sektoren respektive nachgelagerte kritische Dienstleistungen und Prozesse. Als Beispiel für eine intrasektorale Dependenz können die zwei übergeordneten kritischen Branchenzweige innerhalb der Wasserwirtschaft „Trinkwasserversorgung“ und „Abwasserbeseitigung“ herangezogen werden. Aus prozessualer Sicht greifen die beiden Branchenzweige mit ihren technischen Prozessen ineinander ein und stellen in ihrer Gesamtheit einen in sich geschlossenen Kreislauf dar. Hierbei wird das verbrauchte Wasser als Abwasser zusammengetragen, gereinigt und wieder zur Gewinnung von Trinkwasser in den Kreislauf zurückgefördert. Fällt die reguläre Trinkwasserversorgung aus, so fällt auch teilweise der für den Abwassertransport notwendige physikalische Druck aus. Infolgedessen kann der Abwassertransport über das angeschlossene Kanalisationsnetz zu den Kläranlagen nicht mehr reibungslos realisiert werden. Die Beeinträchtigung der Trinkwasserversorgung kann also unmittelbar zu einer Beeinträchtigung der Abwasserbeseitigung führen, da hierdurch der Wasserkreislauf gestört wird (vgl. BSI, 2015a, S. 74). Bei den intersektoralen Dependenzen handelt es sich hingegen um eine Verknüpfung zwischen zwei Infrastrukturen unterschiedlicher Herkunft.

Eine besondere Art dieser Dependenzen sind die Input-Output-Abhängigkeiten. Nach Rinaldi et al. (2001, S. 13 ff.) und Lewis/Petit (2019, S. 6) entsteht dann eine derartige Abhängigkeit, wenn der Output einer kritischen Dienstleistung unmittelbar von dem Input einer anderen abhängig ist. So kann bspw. ein großräumiger und andauernder Ausfall der Trinkwasserversorgung zu erheblichen monetären Schäden und wesentlichen Beeinträchtigungen der Versorgungsprozesse bis hin zu der Gefährdung der öffentlichen Gesundheit führen.

Mitunter kann ein derartiger Ausfall zum Kollaps der medizinisch-relevanten Prozesse und somit zur Gefährdung der Patientensicherheit und Patientenversorgung, zur Verschlechterung oder Entstehung einer epidemischen Lage oder zu gravierenden prozessualen Beeinträchtigungen und Engpässen in der Agrar- und Viehwirtschaft sowie zu Engpässen im Ernährungssektor führen (vgl. BSI, 2015a, zitiert nach Koza et al., 2021, S. 21).

Bei der Betrachtung der intra- und intersektoralen Dependenzen wird der Energiewirtschaft mit den Aufgabenfeldern zur Energieerzeugung und -übertragung und -verteilung ebenfalls eine bedeutsame und zentrale Rolle zugeteilt. Laut § 2 Absatz 1 EnWG müssen EVU die in § 1 EnWG definierten Gesetzesvorschriften erfüllen. Wörtlich heißt es, dass EVU „[…] eine möglichst sichere, preisgünstige, verbraucherfreundliche, effiziente und umweltverträgliche leitungsgebundene Versorgung der Allgemeinheit mit Elektrizität und Gas […]“ sicherstellen müssen (§ 1 Absatz 1 EnWG).

Der Energiesektor dient demzufolge sowohl der Sicherstellung eines reibungslosen gesellschaftlichen Lebens als auch der Verfügungsstellung von industriellen Produktionsfaktoren (vgl. BSI, 2015b, S. 13 ff). In der Folge lassen sich diese Art der Dienstleistungen als primäre kritische Dienstleistungen definieren, deren Ausfall weitreichende und unabsehbare Dominoeffekte (Kettenreaktionen) oder auch Kaskadeneffekte (Lawineneffekte) für eigene kritische Dienstleistungen, aber auch für alle andere kritische Sektoren auslösen könnte (vgl. Haacke/Endreß, 2022, S. 10. | BBK, o. J.).

So hält das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der KRITIS-Sektorstudie „Energie“ fest, dass ein „Ausfall der Energieversorgung […] schon nach kürzester Zeit zu einem Ausfall der meisten anderen Kritischen Infrastrukturen Deutschlands führen [würde]. So ist der Betrieb der Verkehrsinfrastruktur in weiten Teilen nicht ohne Elektrizität und eine verlässliche Kraftstoffversorgung möglich. Die Wasserwirtschaft und Abwasserbeseitigung sind für den Betrieb von Pumpen und Ventilen ebenfalls auf Strom angewiesen. Auch der Informations- und Telekommunikationssektor verbraucht einen zunehmenden Anteil der erzeugten Elektrizität in Rechenzentren und für den Betrieb von Daten-Netzwerken. In den KRITIS-Sektoren Gesundheit, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur ist eine Aufrechterhaltung der wesentlichen Dienstleistungen ohne die durchgängige Verfügbarkeit von Energie in der jeweils benötigten Form nicht möglich“ (BSI, 2015b, S. 13). Die intersektorale Betrachtung hilft in diesem Zusammenhang die Relevanz der Energie- und Wasserwirtschaft für das allgemeine und staatliche Wohlsein zu verstehen. Allerdings berücksichtigt diese Betrachtung lediglich eine einseitige Abhängigkeit, nämlich die Abhängigkeit von der Energie- und Wasserversorgung für eine unterbrechungsfreie Versorgung. Wie verhält sich diese Sachlage jedoch, wenn das sogenannte „System der Systeme“ als Ausgangslage mitberücksichtigt wird und in die Betrachtung einfließt? Wovon hängt die Verfügbarkeit der kritischen Dienstleistungen in der Energie- und Wasserwirtschaft ab?

2.2 Relevanz der IKT für die technischen Basisinfrastrukturen

Der Begriff „System der Systeme“ bezieht sich auf das Zusammenwirken der technischen Basisinfrastrukturen untereinander und auf die Betrachtung ihrer Wechselwirkungen. Diese Betrachtung wird durch den Begriff „Interdependenzen“ präzisiert. Per definitionem beschreibt der Begriff „Interdependenz“ eine bidirektionale Beziehung, welche zwischen zwei Infrastrukturen existiert, in der die Verfügbarkeit oder der Zustand der einen Infrastruktur den Zustand und die Verfügbarkeit der anderen beeinflusst und gleichzeitig mit dieser korreliert.

Besonders gefährlich sind demnach die multidimensionalen und wechselseitigen Dependenzen, wenn die Wirkungstiefe und der Wirkungsgrad des Ausfalls einer kritischen Dienstleistung zum Ausfall von weiteren kritischen Dienstleistungen führen, die ihrerseits jedoch das Grundfundament einer störungsfreien Dienstleistung der zuerst ausgefallenen Infrastruktur darstellt. In der empirischen Beobachtung können derartige wechselseitige Abhängigkeiten komplexe Beziehungen und Spektren erreichen, da diese sich über mehrere Infrastrukturen hinaus ausdehnen können (vgl. Lewis/Petit, 2019, S. 27 | Rinaldi et al., 2001, S. 14 | Koza et al., 2021, S. 22). Diese Komplexität ist durch multifache Verknüpfungen unter den Infrastrukturen, Feedback- und Feedforwardschleifen gekennzeichnet. Die Gesamtheit dieser wechselseitigen Abhängigkeiten und Beziehungen lässt sich in einem komplexen Netz als „System der Systeme“ visualisieren (Bild 3), indem je nach betroffenem Knotenpunkt mäßige Beeinträchtigungen bis hin zu globalen Blackouts und somit Systemversagen verursacht werden können. Aus dieser Perspektive heraus bietet die Betrachtung der Dependenzen zunächst die Möglichkeit ein grundlegendes Verständnis für die Relevanz der Energie- und Wasserwirtschaft zu entwickeln.

Da jedoch die Sicherstellung und Aufrechterhaltung der kritischen Dienstleistungen in der Energie- und Wasserwirtschaft nicht autark von ihrer Umwelt, bzw. anderen technischen oder organisatorischen Faktoren gewährleistet werden kann, müssen die wechselseitigen Abhängigkeiten der beiden Sektoren mit anderen kritischen Sektoren holistisch näherbetrachtet werden (vgl. Lewis/Petit, 2019, S. 25 | Rinaldi et al., 2001, S. 14).

Technische Basisinfrastrukturen sind in hohem Maße miteinander verbunden und auf komplexe physische und logische Weise voneinander abhängig. Ein Störfall in einer Infrastruktur kann sich durch kaskadenartige und eskalierende Ausfälle direkt und indirekt auf andere Infrastrukturen auswirken (vgl. Lewis/Petit, 2019, S. 27 | Koza et al., 2022, S. 19 f.).

Bild 3 illustriert eine derartige wechselseitige Beziehung, die zwischen den technischen Basisinfrastrukturen innerhalb der Energiewirtschaft, Wasserwirtschaft, IKT und dem Transport und Verkehr vorkommt. Durch die holistische Betrachtung können komplexe Interdependenzen zwischen den technischen Basisinfrastrukturen einfacher veranschaulicht werden. Dadurch wird die Beziehung zwischen den einzelnen kritischen Dienstleistungen ersichtlich, in der jede unten aufgeführte technische Basisinfrastruktur auf eine oder mehrere andere kritische Dienstleistungen aus anderen technischen Basisinfrastrukturen angewiesen ist.

Rinaldi et al. (2001, S. 14-16) und Lewis/Petit (2019, S. 7) definieren vier wesentliche Interdependenzen, wobei drei dieser Interdependenzen auf physikalische, logische (in diesem Zusammenhang als politische und gesellschaftliche Beziehungen) und geographische Interdependenzen (raumbezogener Aspekt mit Zusammenhang zu natürlichen und elementaren Umweltgefährdungen) zurückgeführt werden.

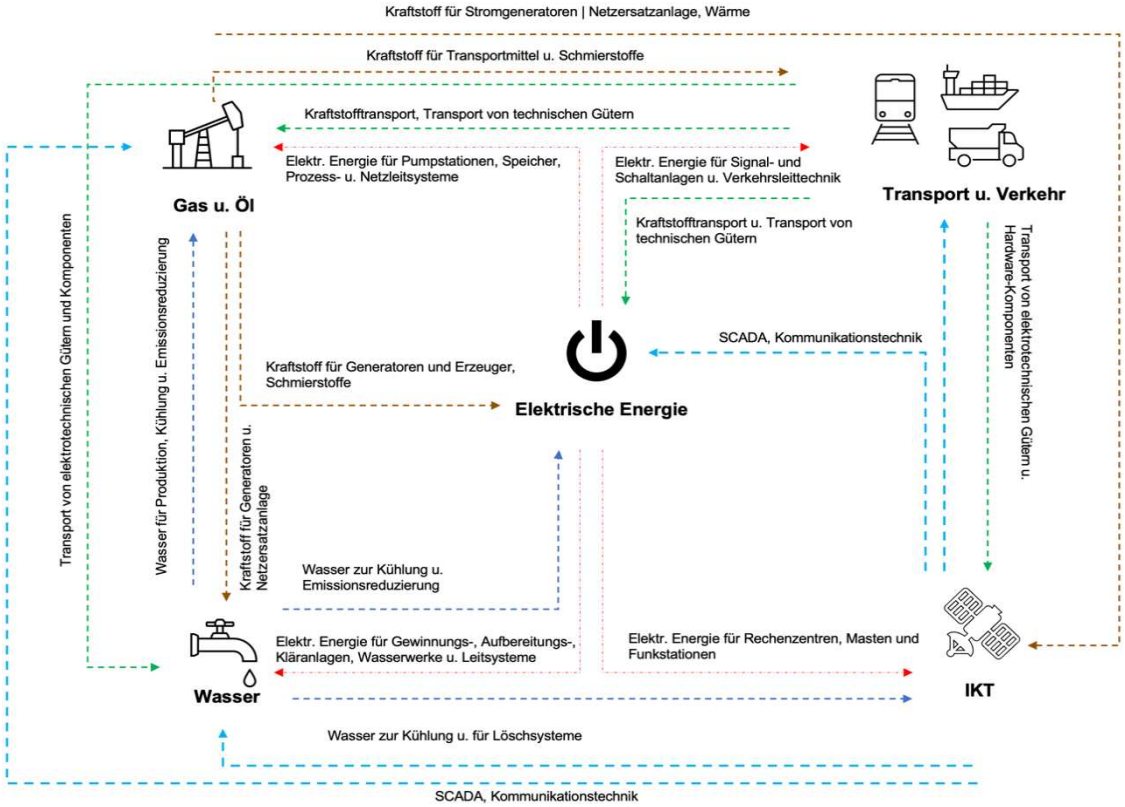


Bild 3: Beispiele für Interdependenzen innerhalb der technischen Basisinfrastrukturen (Quelle: In Anlehnung an Lewis/Petit, 2019, S. 8 f. | Rinaldi et al., 2001, S. 15 | BBK, o. J.)

Die vierte wechselseitige Abhängigkeit wird als „IKT-Interdependenz“ bezeichnet, in der die Verfügbarkeit einer technischen Basisinfrastruktur auch von der Verfügbarkeit bzw. dem Zustand der informationstechnischen und kommunikationstechnischen Dienstleistungen des IKT-Sektors abhängig ist und mit dieser korreliert. Die IKT-Interdependenzen lassen sich als Resultat und natürliche Folge der steigenden Digitalisierung und Automatisierung definieren, welche in den vergangenen Jahrzehnten durch den Einsatz der Automatisierungstechnik und IT kontinuierlich zugenommen haben und fortlaufend fortgesetzt werden (vgl. Rinaldi et al., 2001, S. 15 | BSI, 2016, S. 38 | BSI, 2017a, S. 4-10).

In diesem Zusammenhang stellt dieses Paradigma keinen statischen Zustand dar. Dies muss vielmehr als ein kontinuierlicher, inkrementeller und iterativer Prozess verstanden werden, welcher mit Licht (Effizienzsteigerung und Innovation) und Schatten (wechselseitige Abhängigkeit und Verwundbarkeit) zugleich verbunden ist. Dabei muss auch die Vielfältigkeit dieser wechselseitigen Abhängigkeit und Verwundbarkeit genauer betrachtet werden.

Die grundsätzliche Fähigkeit zur Vernetzung, welche durch den Betrieb und die Verfügbarkeit des Telekommunikations-, Satelliten- und Funknetzes erst ermöglicht wird, ist ein Teil dieser Abhängigkeit. Zu dieser Betrachtung gehört auch die Verfügbarkeit des Mediums „Internet“. Hierdurch ergibt sich nun zwangsläufig eine besonders kritische Beziehung, welche sich nach Dierich et al. (2020, S. 23 f.) im Dokument: „Analyse von Interdependenzen zwischen KRITIS“ unter „infrastrukturbereichs-interne Beziehungen“ konkretisieren lässt.

Industrielle Kontrollsysteme (engl. Industrial Control Systems (ICS)), zu denen Überwachungs- und Datenerfassungssysteme (engl. Supervisory Control and Data Acquisition, (SCADA)), verteilte Steuerungssysteme, bzw. Prozessleitsysteme (engl. Distributed Control Systems, (DCS)) und andere Steuerungssystemkonfigurationen wie speicherprogrammierbare Steuerungen (SPS) (engl. Programmable Logic Controllers) gehören, sind häufig in industriellen Produktionssteuerungsbereichen aufzufinden. ICS werden typischerweise in Branchen wie Elektrizität, Wasser und Abwasser, Erdöl und Erdgas, Transport, Chemie, Pharmazie, Zellstoff und Papier, Lebensmittel sowie in der Fertigungsindustrie (z. B. in der Automobil-, Luft- und Raumfahrtindustrie) eingesetzt (vgl. Dierich et al., 2020, S. 23 f. | BSI, o. J.).

SCADA-Systeme werden zur Steuerung verteilter Anlagen mittels zentraler Datenerfassung und übergeordneter Steuerung verwendet. DCS werden zur Steuerung von Produktionssystemen innerhalb eines lokalen Bereichs, z. B. einer Energieerzeugungsanlage oder eines Wasserwerkes, unter Verwendung von Überwachungs- und Regelungsfunktionen eingesetzt. SPS-Komponenten wiederum werden für die dedizierte Vor-Ort-Steuerung spezifischer Anwendungen eingesetzt und dienen in der Regel der Regulierungssteuerung. Diese Steuerungssysteme sind für den Betrieb der KRITIS in Deutschland, bei denen es sich oft um stark vernetzte und voneinander abhängige Systeme handelt, von entscheidender Bedeutung (vgl. DIN EN ISO/IEC 27019, 2020, S. 10 | BSI, 2013, S. 11-13).

So werden bspw. sowohl in der Stromübertragungs- als auch in der Stromverteilungsbranche geografisch verteilte SCADA-Technologien eingesetzt, um hochgradig vernetzte und dynamische Systeme zu betreiben, die aus einer Vielzahl an dezentralen peripheren Stationen besteht. Einige SCADA-Systeme überwachen und steuern die Stromverteilung, indem sie aus einer zentralen Netzleitstelle Befehle an geografisch weit entfernte Feldsysteme bzw. Prozesssysteme erteilen.

SCADA-Systeme werden auch zur Überwachung und Steuerung der Wasser-, Erdöl- und Erdgasverteilung, einschließlich Pipelines-, Verkehr- und Eisenbahnsystemen, sowie zur Überwachung und Steuerung von Kanalisationsnetzen und Kläranlagen eingesetzt. SCADA-Systeme und DCS sind häufig miteinander vernetzt (z.B. die Stromsteuerungszentrale mit den dezentralen Stromerzeugungsanlagen). Mit dem Ausfall der kritischen Dienstleistungen im IKT-Sektor, in diesem Kontext z. B. der Wegfall der Datenanbindungen und Datenschnittstellen oder der Telekommunikationsnetze, kann der zentrale Zugriff der SCADA-Systeme mittels vernetzter Computertechnologie nicht mehr aufrechterhalten werden (Bild 4).

In diesem Beispiel verlieren die Übertragungsnetzbetreiber (ÜNB) und Verteilnetzbetreiber (VNB) die Verbindung zu ihren dezentralen Umspannwerken, Netzkoppelpunkt- und Netzübergabestationen und sind nicht mehr in der Lage, die zugeteilten Netzgebiete in Echtzeit zu überwachen und zu steuern. Das kann mitunter dazu führen, dass die Netzbetreiber ihre netzdienlichen und relevanten Geschäftsprozesse nicht mehr in der erforderlichen Qualität sicherstellen können, sodass ein negativer Einfluss auf die Versorgungssicherheit entstehen kann.

Die Sicherstellung der Versorgungssicherheit ist eine komplexe und vielfältige Aufgabenstellung und umfasst eine Vielzahl an technischen Aufgaben, welche unmittelbar mit der Netzstabilität im Zusammenhang stehen. Die Netzstabilität ist eine Frage des Gleichgewichts und hängt von zwei Elementen ab: der Netzfrequenz und der Netzspannung (vgl. Dena, 2020, S. 22 | BSI, 2015b, S. 20). Um die Netzstabilität aufrechterhalten zu können, müssen diese beiden Größen in einem zuvor ausbalancierten Wertebereich (50 Hertz) gehalten werden. Werden diese beiden Größen instabil (unzulässige Überschreitung oder Unterschreitung von den festgelegten Grenzbereichen), so kann die Netzstabilität nicht mehr aufrechterhalten werden. Dadurch kann es folglich zu Versorgungsausfällen kommen (vgl. BSI, 2015b, S. 21). Demnach kann bspw. ein kleiner Fehler wie eine nicht rechtzeitig „angepasste Abschaltung einer Elektrizitätsübertragungsnetzleitung [zu einer] Großstörung im europäischen Stromnetz [führen]“ (BSI, 2015b, S. 171). Dem Beispiel aus Bild 4 entnommen, kann die Nichtverfügbarkeit des Übertragungsmediums „Internet“ und der Kommunikationsnetzwerke im Rahmen der Betrachtung der Kausalitätskette zum Nichtvorhandensein von Strom führen, was wiederum zur Nichtverfügbarkeit der IKT-Dienstleistungen führt, da diese für ihren regulären Rechenzentrumsbetrieb auf die elektrische Versorgungskontinuität angewiesen sind.

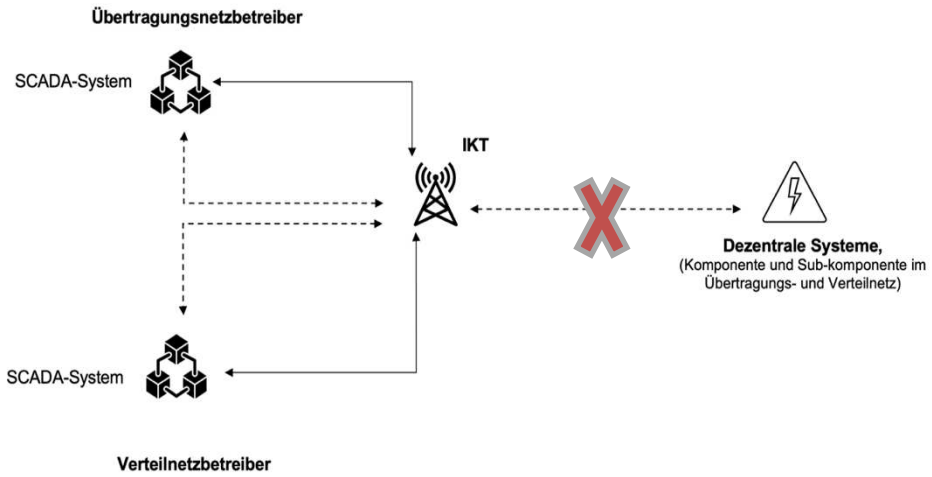


Bild 4: IKT-Interdependenzen am Beispiel von Energienetzbetreibern und IKT (Quelle: In Anlehnung an Dierich et al., 2020, S. 24)

So kann die gegenseitige Relevanz des IKT- und Energiesektors für die Versorgungssicherheit veranschaulicht werden, in der die Verfügbarkeit einer kritischen Dienstleistung bei der elektrischen Energieübertragung und -verteilung von der Verfügbarkeit der IKT, explizit der Datenanbindung, abhängig ist, und umgekehrt.

Infolgedessen kann nun geschlussfolgert werden, dass derartige wechselseitige und multidimensionale Interdependenzen innerhalb der elektrischen Energieversorgung und dem IKT-Sektor in kritischen Fällen auch Kaskadeneffekte (lawinenartige Auswirkungen auf eigene aber auch auf andere nicht verwandte kritische Dienstleistungen und Infrastrukturen) auslösen. Das kann zu einem Blackout führen, insbesondere dann, wenn der Wirkungsgrad eines Ausfalls in einem anderen Sektor gravierendere Ausprägungen aufweist als der Wirkungsgrad des ursprünglichen Ausfalls (vgl. Dierich et al., 2020, S. 7-18 | Hellström, 2007, S. 415-430 | Haacke/Endreß, 2022, S. 62).

Allerdings ist die Sicherstellung der Verfügbarkeit des Internets und der Telekommunikationsnetze nicht die einzige Dienstleistung, welche dem IKT-Sektor zugeordnet werden kann. Der IKT-Sektor beinhaltet neben dem Betrieb von Telekommunikationsnetzen auch den Betrieb von Rechenzentren (Housing und Hosting), die Entwicklung, Integration und Implementierung von Software- und Hardwaretechnologien, die Betreuung dieser Technologien sowie unterstützende Dienstleistungen in Form von Beratungen. Um die IKT-Abhängigkeitsverhältnisse für die technischen Basisinfrastrukturen besser verstehen und interpretieren zu können, müssen zunächst die Reichweite und der Umfang dieser Abhängigkeiten in den kritischen Sektoren „Energie“ und „Wasser“ näherbetrachtet werden. Konkret soll nun der Frage nachgegangen werden, inwieweit die kritischen Dienstleistungen in der Energie- und Wasserwirtschaft von einer funktionierenden IKT abhängig sind. So wie bereits exemplarisch aufgeführt, bestehen die implementierten industriellen Erzeugungs- und Versorgungsanlagen in der Energie- und Wasserwirtschaft aus heterogenen und differierenden Komponenten und sind weitläufig über größere, räumliche Distanzen distribuiert, sodass eine große physische Entfernung zwischen den einzelnen zentralen und dezentralen technischen Instanzen zur Überwachung und Steuerung überbrückt werden muss. Die physische Überbrückung dieser Instanzen ist jedoch eine zeitliche, personelle und kostenintensive Aufgabe. Um dieser Ineffizienz ökonomisch und prozessual entgegenzuwirken, werden die dezentralen Instanzen mit Hilfe von informationstechnischen Komponenten an einem zentralen System zwecks Fernüberwachung und -steuerung angeschlossen. Das Zusammenwirken dieser dezentralen und zentralen Komponenten muss jedoch so konzipiert sein, dass eine quantitativ und qualitativ einwandfreie, unterbrechungsfreie und kosteneffiziente Versorgung mit Strom, Gas und Wasser sichergestellt ist.

Die Orchestrierung und das Zusammenwirken dieser Komponenten bedarf demzufolge eine wechselseitige, valide und sichere Datenerfassung und -auswertung über Systemzustände sowie ein feinjustiertes informationstechnisches Konzept. Dieses informationstechnische Konzept beinhaltet überwiegend die physische und logische Verschmelzung der elektrotechnischen Instanzen mit den informationstechnischen Systemkomponenten, welche in den zentralen SCADA-Systemen und in den dezentralen Netzkoppelpunkten, Trafo- und Unterstationen und Wasserwerken über DCS, SPS, Sensorik und Aktorik zusammengetragen werden. Derartige Systeme bestehen aus skalierbaren Systemeinheiten, welche von wenigen modularen Steuerungskomponenten bis hin zu größeren komplexeren und verteilten Steuerungsinstanzen mit einer Vielzahl an bi- und multidirektionalen Datenanbindungen über zentrale Systemknoten und dezentrale Peripheriestationen miteinander verbunden werden.

Durch den Einsatz von ICS lassen sich eine Vielzahl von elektrischen und physischen Parametern digitalisieren und über die Datenverbindungschnittstellen an das zentrale Prozess- und Leitsystem zwecks Analyse und Überwachung (Vergleich der Ist-Prozessgrößen mit den gewünschten Soll-Prozessgrößen) und Berechnung und Steuerung (Ableitung von Handlungsoptionen bzw. Schaltbefehle) weiterleiten (vgl. BSI, 2015b, S. 165-169).

Die implementierten Systeme bieten somit systemrelevante Funktionen an. Diese Funktionen zergliedern sich in der Regel in Grund- und Zusatzfunktionen. Die Grundfunktionen umfassen die übergeordnete Steuerung und Überwachung aller dezentralen Anlagen und Anlagenteile, welche sich bspw. in den einzelnen Trafo- und Unterstationen oder Wasserwerken befinden. Darüber hinaus beinhalten die Grundfunktionen die Fähigkeit zur Aufnahme und Registrierung von Systemmeldungen und Alarmierungen (z.B. Meldungen bei der Default- bzw. Grenzverletzung der vorangestellten Soll-Parameter) sowie die Fähigkeit zur synchronen und einheitlichen Datenübertragung. Die Zusatzfunktionen stellen ergänzende Funktionen dar. Hierunter zählen (vgl. DVGW, 2006, S. 6 ff.):

- Funktionen zur Systemüberwachung und die Fähigkeit zur Generierung von Schaltbefehlen und Handlungsempfehlungen, welche mithilfe von vordefinierten Parametern menschliche und technische Fehler vermeiden sollen
- Optimierungsrelevante Funktionen zur Verbesserung der Anlagenauslastung, der Lastverteilung, des Energieflusses etc.
- Funktionen zu Integritäts- und Plausibilitätsüberprüfungen und -kontrollen sowie Auswertungen von Systemzuständen
- Funktionen zur Dokumentation der Systemzustände sowie Schaltbefehle in den elektronischen Betriebstagebüchern
- Funktionen zur Planung und Überwachung von turnusmäßigen bzw. planmäßigen Wartungs- und Instandhaltungsprozessen der elektrotechnischen Instanzen
- Funktionen zur Prognostik bzgl. des Systemverhaltens und der Systemzustände und
- Funktionen zur Personaleinsatzplanung und -überwachung

Die Interaktion mit den Systemen findet grundsätzlich über die Mensch-Maschine-Schnittstelle (engl. Human-Machine-Interface (HMI)), über die Dialogrechner und Dialogfunktionen statt. Somit beinhalten die Dialogrechner Visualisierungseinheiten und Anzeigeelemente, welche dedizierte Prozessinformationen über Messwerte, Systemzustände und Anlagenwerte bis hin zu Vergleichswerten darstellen. Dazu gehören festgelegte Standardparameter zur Ermittlung von kritischen Systemzuständen anhand der Grenzwertüber- oder -unterschreitungen. Diese Informationen werden den Systemoperatoren über physische Ausgabeschnittstellen wie Projektionen und Monitoren sowie weiteren Visualisierungsinstrumenten mitgeteilt (vgl. DVGW, 2006, S. 7). Zusätzlich zu der visuellen Darstellung der System- und Prozessinformationen werden auch akustische und optische Signale eingesetzt, um die Wahrnehmung der Systemoperatoren und Bediener in kritischen Fällen unterstützen zu können. Neben den Ausgabeschnittstellen besitzen die Dialogrechner bzw. die implementierten Systemschnittstellen ebenfalls Bedienelemente als Eingabeschnittstellen, über die entsprechende Handlungsoptionen und Schaltbefehle in das System eingegeben und ausgeführt werden können. Diese erfolgen grundsätzlich durch das Eingeben von Schaltbefehlen und Anweisungen im DCS und SCADA-System (vgl. DVGW, 2006, S. 7).

Die Schaltbefehle und Anweisungen lassen sich sowohl über die dezentralen Bedienplätze (Vor-Ort-Steuerung) als auch über zentrale PC-Arbeitsplätze mit Monitoren, Tastaturen und modernen Touchscreen-Instrumenten realisieren (Überwachung und Steuerung in den zentralen Leitstellen) (vgl. DVGW, 2006, S. 7).

Die vertikale und horizontale Integration der oben aufgeführten informationstechnischen Systeme innerhalb der Wasser- und Energiewirtschaft erfolgt unter anderem nach dem hierarchischen Aufbauprinzip des „PERA Reference Models“ (Level 0 bis Level 4) oder nach der klassischen Automatisierungspyramide nach Siepmann (2016) (Level 0 bis Level 5). Die „funktionale Hierarchie“ des Deutschen Instituts für Normung e.V., Europäische Norm (DIN EN) 62264-1:2014, im Folgenden vereinfacht als DIN EN 62264-1 bezeichnet, definiert mit unter das funktionale Hierarchiemodell, welches auf Grundlage des „ISA-95 functional models“ (engl. International Society of Automation (ISA)) entwickelt wurde. Hierbei stellt die ISA-95 ein fünfstufiges Vernetzungsmodell (Level) dar, wie unternehmensrelevante operative und strategische IT-Systeme aus den Büronetzwerken mit den OT-Systemen aus den industriellen und produktiven Fertigungsanlagen vernetzt werden können (vgl. Bildstein/Seidelmann, 2014, S. 584). Die Zielsetzung der DIN EN 62264-Reihe ist die Erstellung eines Referenzmodells bzw. einer Referenzarchitektur, mit dessen Hilfe der effektive Informationsaustausch unabhängig des jeweiligen Automatisierungsgrades einer Organisation erfolgen kann. Für diese Darstellung greift die DIN EN 62264-1 auf die Purdue Enterprise Reference Architecture (PERA) bzw. auf das PERA Reference Model zu, das nachfolgend erläutert wird (vgl. DIN EN 62264-1, 2014, S. 14 ff. | BSI, 2013, S. 13-21):

Level 4 Management Level (Enterprise Resource Planning (ERP)): Strategische, herstellungsbezogene Geschäftsaktivitäten, welche sich in der Ebene der Unternehmensleitung einbetten und taktische Aktivitäten im Bereich der Grobplanung, Beschaffung, Logistik und des Verkaufs umfassen.

Level 3 Planning Level (Manufactoring Operation Management (MOM): Strategische Produktionsaktivitäten, welche sich mit der direkten Produktionsplanung, Wartung und Instandhaltung beschäftigen, um die Herstellung der erforderlichen Produkte und Teilprodukte sicherzustellen.

Level 2 Supervisory Level Control (SCADA Systems): Operative Produktionsaktivitäten zur manuellen und automatisierten Überwachung und Steuerung der Produktionsprozesse.

Level 1 Control Level (SPS): Produktionsnahe Aktivitäten zur Messung der physischen Prozesse auf der Ebene 0 über Sensoren und Aktoren.

Level 0 Field Level (Physical production process): Physische Produktionsprozesse

Neben dem PERA Reference Model wird auch das Modell nach Siepmann (2016, S. 49) in der Literatur oft genannt. Dieses stellt im Gegensatz zu dem PERA Reference Model auf Basis der DIN EN 62264 eine Automatisierungspyramide dar, die das PERA Reference Model um eine tiefergehende Schicht (Prozessebenen) erweitert (Bild 5) (vgl. Siepmann, 2016, S. 49).

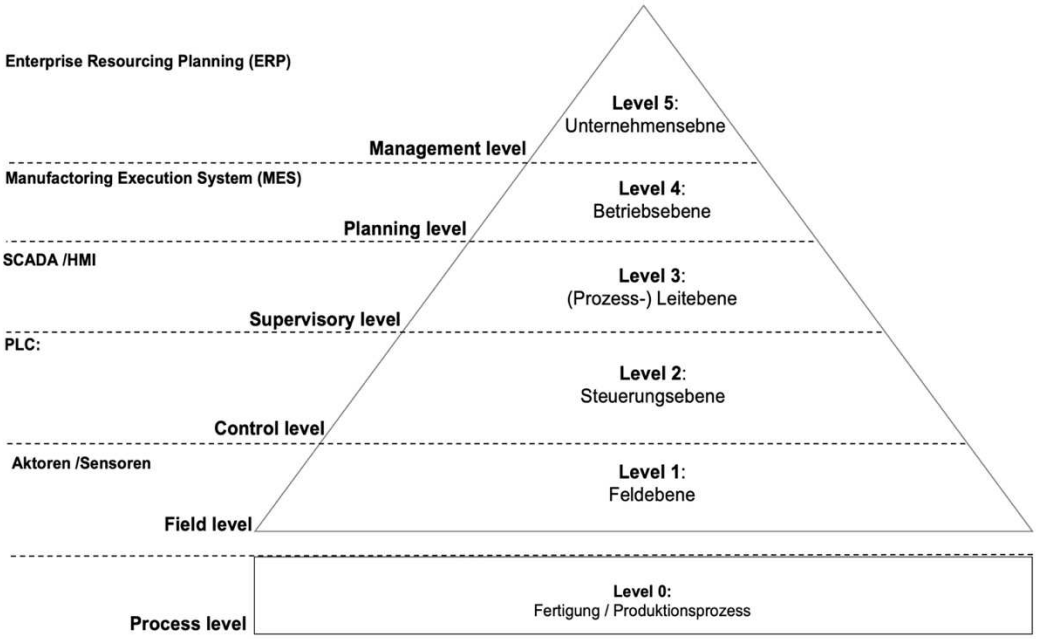


Bild 5: Automatisierungspyramide nach Siepmann (Quelle: In Anlehnung an Kiesel et al., 2020, S. 4 | Siepmann, 2016, S. 49)

So stellt die Nullebene (engl. Level 0 Process level: Physical Production Process) nach Siepmann (2016, S. 49) in der Automatisierungspyramide die unterste Ebene der hierarchischen Darstellung dar und besteht aus industriellen Anlagen, Aggregaten und Maschinen. Die Ebene 1, bzw. die Feldebene, (engl. Level 1 Field level: Sensing and controlling the production process) umfasst alle Automatisierungskomponenten, Sensoren (z.B. Lichtschranken, Temperaturfühler) und Aktoren (z. B. elektrische Regler und elektromagnetische Schalter wie Relais), welche die Interaktion zwischen den physischen Komponenten und den grundlegenderen Steuerungselementen wie DCS und SPS auf der zweiten Ebene sicherstellen. Die Aktivitäten auf der ersten Ebene beinhalten Tätigkeiten zur Konfiguration, Parametrierung und Messung der physischen Prozesse. Die Ebene 2 wird Steuerungsebene, auch Realtime-Ebene genannt (Control level). Diese ist für die Verarbeitung der SPS-Sensordaten sowie für die anschließende Weitergabe der Ergebnisdaten an die Feldebene (Level 1) verantwortlich. Die Steuerungsebene übernimmt so die Aufgaben zur dezentralen Vor-Ort-Steuerung der physischen Anlagen, Teilanlagen sowie der Aggregate. Die Ebene 3 (Supervisory level) wird als Industriehardware bzw. (Prozess-) Leitebene bezeichnet, auf der die Interaktion zwischen den übergeordneten zentralen SCADA-Systemen und den Prozessen auf der Steuerungsebene stattfindet. Auf der Ebene 4 (Planning level), der sogenannten Betriebsebene, werden die Fertigungsabläufe durch Manufacturing Execution Systems (MES) geplant und gesteuert. Bei dieser Planung wird grundsätzlich der Aufbau und Ablauf der Produktionsprozesse festgelegt. Auf der obersten Ebene (Management level), der Unternehmensebene, befinden sich die Enterprise-Resources-Planning (ERP)-Systeme. Diese verwalten das Inventar, die Rechnungsstellung, die Buchhaltung und die Logistik und werden in der Regel in das Büronetzwerk eingebettet (vgl. Siepmann, 2016, S. 49 | BSI, 2013, S. 13-21).

Bild 6 illustriert exemplarisch die Vernetzung eines industriellen SCADA-Netzwerkes mit einem Büro-Netzwerk (vgl. DIN EN 62264-1, 2014, S. 14 ff. | BSI, 2013, S. 13-21).

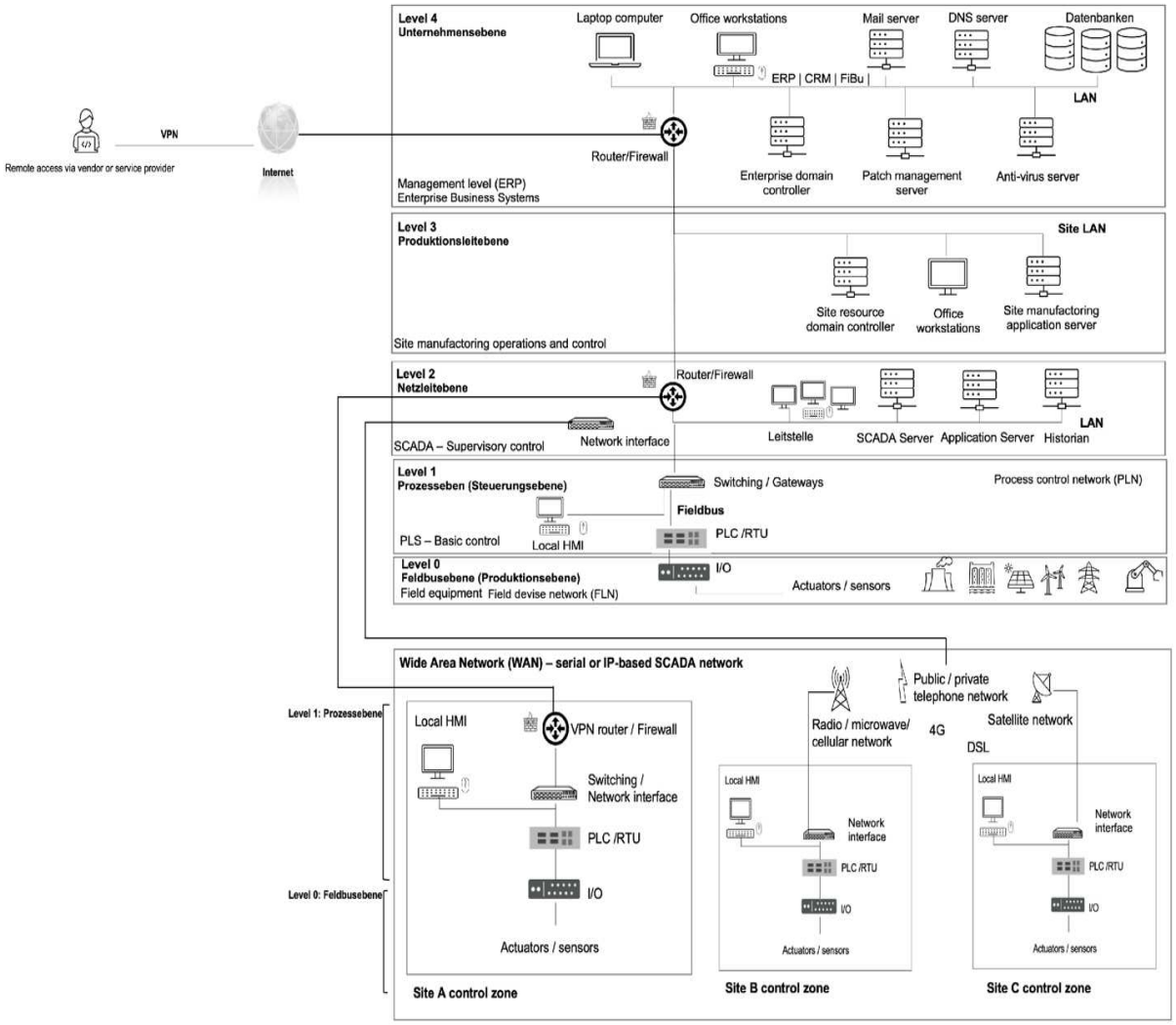


Bild 6: Exemplarische SCADA-Netzwerklandschaft (Quelle: In Anlehnung an DIN EN 62264-1, 2014, S. 17 | IEC 62443-2-1, 2010, S. 93 | IEC/TS 62443-1-1, 2009, S. 69-74 | BSI, 2013, S. 17)

Durch diese vertikale und horizontale Integration und Vernetzung der Informations- und Automatisierungstechnik können die ÜNB, VNB, WVU und ABU ihre versorgungstechnischen Prozesse nun effizienter durchführen. Beispielsweise können die anfallenden technischen System- und Netzstörungen in den dezentralen Instanzen durch die Echtzeitdatenerfassung und -überwachung frühzeitig entdeckt, lokalisiert und infolgedessen behandelt werden, wodurch die reaktive und die korrektive Fähigkeit im Sinne des Störungsmanagements erheblich optimiert werden kann. Zusätzlich hierzu lassen sich auch die systemkritischen Betriebszustände der einzelnen Instanzen auf der Feldebene und in den einzelnen Peripheriestationen durch Echtzeitüberwachung im Sinne der Prognostik (engl. State Estimation oder Forecasting) ermitteln und durch Warnfunktionen eskalieren, bevor diese zu einer Beeinträchtigung bzw. zu einem kritischen Systemzustand führen können (vgl. Dena, 2020, S. 79 | vgl. BSI, 2015b, S. 165-169).

Durch den Einsatz der OT-Systeme können zahlreiche Betriebs- und Prozessdaten in Echtzeit, bzw. minutengenau als Intervallergebnisse erfasst, gesammelt, überwacht und analysiert werden. Daraus können strategische Vorgehensweisen abgeleitet werden, die eine rationale Entscheidungsfindung im Sinne der Wirtschaftlichkeit ermöglichen. So lassen sich bspw. über die zentrale Datenerfassung die Verbrauchsmengen der einzelnen Anlagen exakter bestimmen, sodass sich anhand der gewonnenen Daten die Betriebsabläufe, Fahrpläne, Lastverteilung und der Anlagenbetrieb ebenfalls optimieren lassen. Durch diese Optimierung können nun auch die anfallenden Energie-, Betriebs- und Personalkosten reduziert werden. Hierdurch entstehen Einsparungspotentiale bezüglich der Personal- und Betriebskosten (vgl. BSI, 2015b, S. 163-169). In der gesamtheitlichen Betrachtung dient der Einsatz der Informations- und Automatisierungstechnik in der Energie- und Wasserwirtschaft zur Erfüllung folgender Anforderungen:

- Kontinuierliche Überwachung und Kontrolle zur Sicherstellung und Optimierung der Dienstleistungs- und Versorgungsgüte, welche innerhalb der Energie- und Wasserwirtschaft anhand bestimmter gesetzlicher Anforderungen gemäß dem Energiewirtschaftsgesetz (EnWG) und WHG bestimmt werden und zu erfüllen sind.
- Kontinuierliche Sicherstellung und Aufrechterhaltung der Betriebs- und Versorgungssicherheit mithilfe von Früherkennungs-, Warn- und Alarmierungssystemen zur vorzeitigen bzw. rechtzeitigen Identifizierung und Lokalisierung von elektrotechnischen und physikalischen Prozessanomalien, Störungen und Versorgungsengpässen.
- Qualitative und quantitative Optimierung der organisationalen und prozessualen Arbeitsvorgänge, welche zur Steuerung, Überwachung, Dokumentation, Berichterstattung und bereichsübergreifenden Daten- und Informationsakquise und -weiterleitung eingesetzt werden.

Bezugnehmend auf die Vielfalt und die Tiefe der wechselseitigen IKT-Abhängigkeiten wird die die Postulierung vorgenommen, dass die zu erbringenden Versorgungsleistungen in den beiden Sektoren Wasser und Energie aufgrund des progressiven Einsatzes der IKT von einer zuverlässigen und funktionierenden IKT abhängig sind. So trägt der Einsatz der IT durch die Vernetzung der industriellen Aggregate und Anlagen über OT-Systeme „unter anderem zur verlässlich hohen Trinkwasserqualität sowie -verfügbarkeit […] bei. Durch Einsatz von Informationstechnik können, die zur Trinkwasseraufbereitung benötigten biologischen oder chemischen Substanzen punktgenau und bedarfsgerecht hinzugefügt werden. Die damit erreichte Präzision ist bei manueller Interaktion nicht zu erreichen. Die IT-Unterstützung führt zudem zur Verbesserung ökonomischer Bilanzen. Dezentrale und zentrale Anlagen werden von immer weniger Leitstellen aus steuer- und überwachbar (Anbindung der einzelnen Systeme über das Internet), was zu einer Optimierung der Kosten- und Leistungsrechnung führt. Der zunehmende Einsatz von IT bedeutet jedoch gleichzeitig, dass eine Abhängigkeit von Informations- und Kommunikationstechnik entsteht und weiter steigen wird“ (BSI, 2015a, S. 18). Diese äquivalente Abhängigkeit von IKT ist auch für die Akteure in der Energiewirtschaft zu notieren (vgl. BNetzA, 2018, S. 3 | BSI, 2015b, S. 163-169).

Gleichwohl wächst jedoch auch die Diversität der implementierten Hardware- und Softwarekomponenten, die von unterschiedlichen Herstellern betrieben werden und auf verschiedene Entwicklungsmethoden, Softwaretechniken, Programmiersprachen, Betriebssysteme und Datenbankmodellierungen sowie Schnittstellenprogrammierungen zurückgreifen. Als Resultat steht zwangsläufig eine neue Abhängigkeit zu den OT-Systemherstellern, Dienstleistern und Lieferanten sowie Integratoren, die dem BSI zur Folge als „größte externe Abhängigkeit“ zu definieren sind (BSI, 2015b, S. 163). Bei der weiteren Betrachtung der Abhängigkeitsverhältnisse muss also auch die Frage zur Sicherheit der OT-Systeme der externen Soft- und Hardwarehersteller gestellt werden. Sind die eingesetzten OT-Komponenten sicher? Kann die Sicherheit der eingesetzten, bzw. erworbenen Hard- und Software auch von den Betreibern in der Energie- und Wasserwirtschaft eigen sichergestellt und aufrechterhalten werden? Die Frage zur „Beherrschbarkeit“ der OT-Systeme innerhalb der industriellen Produktions- und Versorgungsumgebung ist auch eine Frage der Heterogenität, Komplexität und Fragilität dieser OT-Systeme, die gleichwohl mit den fachlichen, personellen und finanziellen Ressourcen der Betreiber technischer Basisinfrastrukturen korreliert und in direktem Zusammenhang steht.

2.3 Folgen der IKT-Abhängigkeit für die technischen Basisinfrastrukturen

Die in Kapitel 2.2 dargestellte Ausführung weist daraufhin, dass die Funktionstüchtigkeit und die Gewährleistung einer unterbrechungsfreien Energie- und Wasserversorgung in hohem Maße von einer funktionierenden und sicheren IKT abhängig ist. So existieren bereits viele heterogene Komponenten wie Mikrochips, eingebettete Geräte, Betriebssysteme, Softwarebibliotheken, Standardanwendungen, Netzwerkkomponenten und mobile Geräte, welche unabhängig voneinander entwickelt und bereits in die industriellen Umgebungen der technischen Basisinfrastrukturen implementiert wurden. Diese Diversität bezugnehmend auf die entwickelten und implementieren Soft- und Hardwarekomponenten, Entwicklungsmethoden, involvierten Dienstleister, Hersteller und Lieferanten macht es den einzelnen Betreibern schwer, diese hohe Anzahl an variierenden und komplexen Systemen selbst zu beherrschen. Kommt es bspw. in der Energiewirtschaft zu „Sicherheitsproblemen bei diesen Partnern […], können Störungen und Ausfälle im Umfeld der Kritischen Infrastrukturen die Folge sein. Speziell in der Branche Elektrizität sind einige IKT-Dienstleistungen oder (Teile der) IKT-Infrastrukturen bei einzelnen Betreibern an Dienstleister ausgelagert, daher ist diese Branche besonders betroffen. Gleiches gilt auch bei der Einführung neuer IKT-Komponenten. Es bestehen nicht nur Abhängigkeiten zwischen Hersteller und Betreiber, sondern häufig zwischen Hersteller (teils auch noch Händler), Integrator und Betreiber“ (BSI, 2015b, S. 162).

In der Analogie zur Energiewirtschaft besteht auch in der Wasserwirtschaft diese externe Abhängigkeit, da die Sicherheit der Steuerungs- und Prozesstechnik in weiten Teilen von den Systemherstellern und Systementwicklern abhängig ist. „Schwachstellen, die bereits in der Entwicklung der Hard- und Software beim Hersteller oder in der fehlenden Implementierung von Sicherheitsfunktionalitäten begründet liegen, können durch die Betreiber selbst im Nachhinein nur schwer erkannt, geschweige denn behoben werden. Die Betreiber besitzen nicht genug Ressourcen, um eigene Sicherheitsanalysen der Systeme vorzunehmen“ (BSI, 2015a, S. 108).

In dieser Konstellation fehlen Versorgungsunternehmen innerhalb der Energie- und Wasserwirtschaft das hierfür erforderliche informationstechnische Wissen und personelle Kapazitäten, um derartige Vulnerabilitäten selbst detektieren und beseitigen zu können (vgl. BSI, 2015a, S. 108 | BSI, 2015b, S. 162-165). Dieser Umstand wird durch die Integration weiterer moderner Systeme, wie bspw. Virtuellen Kraftwerken zur Bündelung der distribuierten Energieerzeugungsanlagen auf Basis erneuerbarer Energien, weiter verschärft (vgl. Koza/Öztürk, 2021, S. 49-69 | BSI, 2015b, S. 29-31 und 165).

So fußt eine der wesentlichen Effekte aus dieser komplexen und heterogenen IKT-Abhängigkeit auf der Existenz von vorhandenen Sicherheitslücken in den Soft- und Hardwarekomponenten und den daraus resultierenden Gefährdungen für technische Basisinfrastrukturen. Wie lässt sich diese Schlussfolgerung im Detail erklären? In ihrem Ursprung hatten ICS marginale Ähnlichkeiten mit den klassischen IT-Systemen. Durch die Nutzung von spezieller proprietärer Hard- und Software sowie Steuerungsprotokollen ließen sich die ICS in einem isolierten Netzwerk nahezu vollständig autark und ohne externe Anbindung nach außen betreiben. Somit befanden sich viele ICS-Komponenten in physisch und logisch gesicherten Bereichen, in denen die Komponenten nicht mit IP-basierten Netzwerken und -Systemen in einer interaktiven Konnektivität standen. Durch die Standardisierungs- und Harmonisierungsverfahren der Kommunikationsprotokolle können die Hardware- und Softwarekomponenten unterschiedlicher Hersteller nun miteinander kompatibel betrieben werden. So kann der Informations- und Datenaustausch der ICS einheitlich auf der Grundlage von Transmission Control Protocol /Internetprotokoll (TCP/IP-) basierter Techniken erfolgen, was zur steigenden Interoperabilität der Systeme führt. Dadurch kann die Nutzung von teuren proprietären Systemen vermieden und gleichzeitig kostengünstigere und kompatiblere Komponenten beschafft werden (vgl. Baur et al., 2019, S. 723-730). So werden die Daten- und Informationsschnittstellen zwischen den dezentralen Peripheriestationen und den zentralen Systemen heute über Virtual Private Network (VPN)-Technologien, Multiprotocol Label Switching, Mobilfunktechnologien (z. B. 4G und Digital Subscriber Line), Funktechnologien sowie über eigene Standleitungen (Standleitungsmodem und kabelgebundene Übertragung mit Modbus und Feldbus und Single-Pair High-Speed Digital Subscriber Line-Standleitungsmodem und Lichtwellenleiter) realisiert (vgl. Koza et al., 2021, S. 175 | BSI, 2015b, S. 162). Dadurch können moderne, kostengünstige IP-fähige Komponenten die klassischen Infrastrukturen ersetzen. Mit der Verwendung und Integration von standarisierten Industriestandardcomputern, Betriebssystemen und Netzwerkprotokollen innerhalb der industriellen Umgebung beginnen diese OT-Systeme jedoch sich in der logischen Schlussfolgerung den klassischen IT-Systemen aus den Büronetzwerken immer mehr zu ähneln (vgl. Kiesel et al., 2020, S. 6).

In der Folge kann eine deutlich geringere Isolierung der ICS in Relation zu den Vorgängersystemen vorgenommen werden, sodass eine größere Notwendigkeit zur Sicherung dieser Systeme gegenüber externen Einflüssen erforderlich ist. Der vermehrte Einsatz von drahtlosen und Ethernet-basierten Systemen und Netzwerken stellt nun ein zunehmend größeres Risiko für ICS-Implementierungen dar. Betreiber technischer Basisinfrastrukturen nutzen eine Vielzahl von standardisierten und interoperablen OT-Komponenten, die direkt über ihre OT-Netzwerke oder indirekt über Büronetzwerke an das Medium Internet angeschlossen sind (vgl. BSI, 2019a, S. 6).

So deklariert das BSI in seinen BSI-Veröffentlichungen zur Cyber-Sicherheit „Industrial Control System Security – Top 10 der Bedrohungen und Gegenmaßnahmen“, dass für die ICS-Komponenten im Grunde täglich neue Schwachstellen entdeckt und publiziert werden, welche die Cyberkriminellen für eine Kompromittierung der OT-Netzwerke mit Schadsoftware missbrauchen können (vgl. BSI, 2019a, S. 6). Hierbei wird die Cyberbedrohung „Infektion mit Schadsoftware über Internet und Intranet“ als zweitgrößte Cybergefahr definiert (BSI, 2019a, S. 6). In Bild 7 werden diese 10 Bedrohungen aufgelistet.

Top 10 der Cyberbedrohungen für Industrial Control Systems (ICS)	Trendentwicklung seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	⇧
Infektion mit Schadsoftware über Internet und Intranet	⇧
Menschliches Fehlverhalten und Sabotage	⇧
Kompromittierung von Extranet und Cloud-Komponenten	⇧
Social Engineering mit Phishing	⇩
(D)DoS – Angriffe	⇧
Internet – verbundene Steuerungskomponente	⇨
Einbruch über Fernwartungszugänge	⇨
Technisches Fehlverhalten und höhere Gewalt	⇩
Kompromittierung von Smartphones im Produktionsumfeld	⇨

⇧ steigend ⇨ gleichbleibend ⇩ sinkend

Bild 7: TOP 10 der Bedrohungen für ICS (Quelle: In Anlehnung an BSI, 2019a, S. 2 | Kiesel et al., 2020, S. 7)

Die vorhandenen Schwachstellen können direkt über die Prozessnetze, z. B. über nicht rechtzeitig beseitigte Sicherheitslücken oder über nicht ausreichend gesicherte VPN-Schnittstellen, über sogenannte Remote-Zugriffschnittstellen zur Fernwartung (vgl. BSI, 2019a, S. 6), aber „[…] auch durch infizierte Wechseldatenträger direkt im Intranet […], ausgenutzt werden. Die Sicherheit wird zudem von der zunehmenden Verbreitung Ethernet-basierter Netze und Protokolle im ICS-Umfeld und deren Verbindung mit Systemen im Unternehmensnetz (Fileserver, ERP-, MES-Systeme, etc.) erschwert. Gelingt es einem Angreifer, in das Office-Netz einzudringen oder befindet er sich bereits im Intranet, kann er sich häufig direkt oder mit einem Folgeangriff in das ICS-Netz vorarbeiten“ (BSI, 2019a, S. 6). Insgesamt definiert das BSI fünf mögliche Angriffsvektoren (vgl. BSI, 2019a, S. 6):

- Infiltrierung eines Netzwerkes über sogenannte Schwachstellen sowie Zero-Day-Exploits, für die zum Zeitpunkt des Angriffs keine Detektionsmöglichkeiten sowie offizielle Abhilfemaßnahmen bekannt sind,
- Infiltrierung durch das Manipulieren von externen Webseiten, wie bspw. durch das Ausführen von Drive-by-Download, um das Opfersystem ohne Eingreifen des Nutzers durch einfaches Aufrufen der Webseite zu kompromittieren,
- Infiltrierung der Unternehmenswebseiten durch Structured Query Language-Injection oder Cross Site Scripting,
- Infiltrierung durch willkürliche Schadsoftware durch das Medium Internet, und
- Infiltrierung durch infizierte Hardwarekomponenten, wie bspw. infizierte USB-Komponenten der Mitarbeitenden durch den Einsatz von Bring Your Own Devices

In der logischen Schlussfolgerung lassen sich vier grundlegende und kohärente Tatsachen aus der Vielfalt der IKT-Abhängigkeiten und der daraus resultierenden Folgen ableiten, die eine potenzielle und weitreichende Gefährdung für die Betreiber technischer Basisinfrastrukturen darstellen.

Schlussfolgerung 1: Gefahren für die IKT-Sicherheit sind auch Gefahren für die Versorgungssicherheit.

Schlussfolgerung 2: Zunahme der Systemkomplexität und der Systemheterogenität durch Integration einer Vielzahl variierender OT-Systeme und OT-Applikationen verschiedener Hersteller mit unterschiedlichen Sicherheitsniveaus.

Schlussfolgerung 3: Praktisch täglich neue entdeckte Schwachstellen in OT-Systemen, die über das Medium „Internet“ jederzeit an jedem Ort ausgenutzt werden können.

Schlussfolgerung 4: Fehlende personelle und fachliche Ressourcen zur rechtzeitigen Detektion und Beseitigung von entdeckten Schwachstellen.

2.4 Quintessenz aus dem IKT-Einsatz und den Gefahren für KRITIS

Aufgrund des Vorhandenseins von Schwachstellen und Sicherheitslücken müssen daher detektierende und korrigierende Sicherheitsmechanismen zwingend eingeführt werden, um die bestehenden Schwachstellen und Sicherheitslücken in den Soft- und Hardware-Komponenten im Sinne des VM rechtzeitig vor der Ausnutzung durch Cyberkriminelle zu entdecken und zu eliminieren, um somit zur Erhöhung der Resilienz der Systeme beitragen zu können. Werden die bestehenden Schwachstellen frühzeitig entdeckt, so können die Systemhersteller bspw. durch die Bereitstellung von Sicherheitsupdates zur Eliminierung und Verbesserung der jeweiligen Schwachstellen in den Systemen beitragen. Da viele KRITIS nicht in der Lage sind diese Aufgabenstellung autark und effizient durchzuführen, müssen sie auf intelligente, schlanke und ressourcenschonende Lösungsansätze zurückgreifen, um ihre Prozess- bzw. ICS-Netzwerke vor einer derartigen Gefahrenlage sachdienlich und nachhaltig schützen zu können.

In der 2021 vom Verfasser durchgeführten empirischen Datenerhebung wurde unter anderem Bezug zu der Frage genommen, welche kritischen Hemmnisse und Erfolgsfaktoren eine relevante Rolle für ein nachhaltiges und effizientes Informationssicherheitsniveau bei Betreibern KRITIS, darunter auch Akteure aus der Energie- und Wasserwirtschaft, spielen. Zweck dieser empirischen Untersuchung war es, die bereits 2015 definierten Ausprägungen aus den BSI-Sektorstudien „Energie“, „Ernährung und Wasser“, „Gesundheitswesen“ und „IKT“ zu überprüfen und damit den Versuch zu unternehmen, die in den Sektorstudien festgehaltenen Deklarationen hinsichtlich der Hemmnisse, Erfolgsfaktoren und Herausforderungen für die Informationssicherheit zu reproduzieren oder diese ggf. anhand der empirischen Faktenlage zu widerlegen. Hierfür wurden insgesamt 86 Unternehmen, bzw. Hauptverantwortliche zum Thema Informationssicherheit befragt (vgl. Koza, 2021, S. 819-831).

So haben insgesamt 25 Unternehmen aus dem Bereich der Energieversorgung, 14 aus der IKT, 14 aus dem Gesundheitswesen, 25 aus der Wasserversorgung und Abwasserbeseitigung und 10 aus der Energie- und Wasserversorgung als Verbundunternehmen an der Studie teilgenommen. Die empirisch erworbenen Ergebnisse wurden innerhalb dieser Studie durch semantische Methoden zur Strukturanalyse in ein Modell überführt. Hierdurch wurden die korrelativen Zusammenhänge zwischen den einzelnen Hemmnissen und Erfolgsfaktoren in einem Gesamtbild visualisiert und interpretiert (vgl. Koza, 2021, S. 828).

In weiten Teilen können die getroffenen Deklarationen aus dem Jahr 2015 in den BSI-Sektorstudien bestätigt, bzw. erweitert werden. Insgesamt gaben 76 Unternehmen (88 %) an, dass die hohe zeitliche und personelle Belastung als das größte Hemmnis für ein effizientes und nachhaltiges Informationssicherheitsniveau zu betrachten ist (vgl. Koza, 2021, S. 823). Die Gründe für diese Deklaration sind vielfältiger Natur. Das IT-Sicherheitsgesetz 1.0 (IT-SiG 1.0 und 2.0) verändert als Artikelgesetz bestehende Gesetze wie u. a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und das EnWG. Bezüglich der im BSIG definierten Anforderungen werden KRITIS aufgefordert, „[…] angemessene technische und organisatorische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen […]“ (§ 8a Absatz 1 Satz 1 BSIG). Zur Erfüllung dieser verbindlichen Anforderung können die Akteure aus der Wasserwirtschaft auf den von den Wasserbranchenfachverbänden entwickelten Branchenspezifischen Sicherheitsstandard (B3S) zurückgreifen. Das B3S-Verfahren der beiden Fachverbände, die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. (DWA) und der Deutsche Verein des Gas- und Wasserfaches e.V. (DVGW), bietet auf Grundlage des BSI IT-Grundschutzes und BSI IT-Grundschutz-Kompendiums den WVU und ABU einen methodischen Ansatz, um die sicherheitstechnischen und sicherheitsorganisatorischen Anforderungen an ihren ICS-Netzwerken gerecht zu werden. Hinsichtlich der Modifikationen des EnWG durch das IT-SiG 1.0 werden ebenfalls gesetzliche Anforderungen explizit für Strom- und Gasnetzbetreiber sowie Anlagenbetreiber beschrieben, um die Resilienz ihrer kritischen Systeme zu erhöhen (vgl. Koza, 2021, S. 820 | Koza/Öztürk, 2022a, S. 92). Die Anforderungen werden in § 11 Absatz 1 (a) EnWG für die Netzbetreiber und § 11 Absatz 1 (b) EnWG für die Anlagenbetreiber konkretisiert. Demzufolge müssen die Netzbetreiber und Anlagenbetreiber, die im IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) (2015, S. 10) dargestellten Anforderungen umsetzen und ein ISMS gemäß DIN EN ISO/IEC 27019, DIN EN ISO/IEC 27001 und DIN EN ISO/IEC 27002 einführen und zertifizieren lassen (vgl. Koza, 2021, S. 820). Die Erfüllung dieser Anforderungen bedeutet jedoch im Kern, dass die Akteure in der Energie- und Wasserwirtschaft dazu verpflichtet werden, ihre bereits ausgelasteten personellen, fachlichen und finanziellen Ressourcen noch intensiver in Anspruch zu nehmen. Im Detail müssen die Betreiber ein breites Spektrum an technischen und organisatorischen Anforderungen erfüllen, welche die drei interaktiven Themengebiete der IT-Sicherheit, der Organisationssicherheit und der individuellen Sicherheit (des menschlichen Faktors (engl. Human Factors)) innerhalb der Informationssicherheit adressieren, deren sachdienliche und kontinuierliche Erfüllung viel Zeit und fundiertes Wissen in Anspruch nimmt (vgl. Koza, 2021, S. 819-831).

Diese Sichtweise impliziert die Tatsache, dass es sich bei der Informationssicherheit in der Analogie zur Digitalisierung um einen fortlaufenden Prozess handelt, dessen Zielsetzung jedoch in der kontinuierlichen und sukzessiven Optimierung des Informationssicherheitsniveaus liegt und lediglich mit einem hohen und adäquaten Ressourceneinsatz zu bewältigen ist (vgl. Koza, 2021, S. 819-831).

Ein weiterer Grund zur erhöhten personellen und zeitlichen Ressourcenanbindung und -auslastung liegt in der steigenden Komplexität der zu schützenden OT-Systeme. So definieren 74 Unternehmen (86 %) die steigende Komplexität und Heterogenität der OT-Systeme als zweitgrößtes Hemmnis für ein adäquates Informationssicherheitsniveau. Als Gegenkraft zu den zwei vorgestellten Hemmnissen definierten 83 Unternehmen (97 %) das Vorhandensein von informationstechnischem Wissen als den größten kritischen Erfolgsfaktor, um der Komplexität der OT-Systeme effizient und nachhaltig entgegenwirken zu können. Hierbei ist es von signifikanter Bedeutung die Beziehungen zwischen den einzelnen Faktoren in ihrer Gesamtheit zu verstehen. Informationstechnisches Wissen korreliert unmittelbar mit der Existenz von ausreichenden personellen und fachlichen Kapazitäten, um zum einen die vielfältigen Aufgabenfelder der Informationssicherheit und zum anderen die steigende Komplexität der OT-Systeme beherrschen zu können. So definieren 77 Unternehmen (90 %) ausreichende personelle Ressourcen als zweitgrößten kritischen Erfolgsfaktor. Die Betrachtung der innerhalb der Versorgungslandschaft agierenden kleinen und mittleren Unternehmen (KMU) verdeutlicht, dass diese mittlerweile unter einer verstärkten Überlastung leiden. Diese Überlastung lässt sich aber auch insgesamt durch die Fülle an regulatorischen Anforderungen erklären, die die Versorgungsunternehmen im Allgemeinen aber auch in dedizierten Bereichen wie dem Umweltmanagement, Energieeffizienzmanagement, technisches Sicherheitsmanagement, Qualitätsmanagement und ISMS freiwillig oder auch zwangsweise durch gesetzliche Verbindlichkeiten zu erfüllen haben (vgl. Koza, 2021, S. 823 f.).

Zur weiteren Verifikation wurde zudem auch die Rolle des Gesetzgebers als Initiator und als Impulsgeber zum Thema Informationssicherheit analysiert. Der Schwerpunkt im Untersuchungsbereich der Studie zielte auf die Prämisse, dass eine Vielzahl an KRITIS möglicherweise ohne die gesetzliche und verbindliche Deklaration (Erlass des IT-SiG 1.0 im Jahre 2015) keine intrinsischen Motive entwickelt hätten, um aus eigener Kraft und eigenem Willen personelle und finanzielle Bemühungen im Bereich der Informationssicherheit zu tätigen.

Neben dieser Prämisse sollte aber auch auf Basis der empirischen Daten ermittelt werden, welche Rolle der Gesetzgeber (z. B. als Enabler) in diesem Zusammenhang aufnimmt. Hierzu monieren 74 % der beteiligten Unternehmen die im IT-SiG 1.0 vorhandene Lücke, dass keine Vorgaben an die IT-Entwicklungsprozesse der Hersteller gestellt werden. Weitere 97 % bemängeln sogar die fachliche Lücke in der Lieferkette der KRITIS, da im IT-SiG 1.0 lediglich Anforderungen an die Informationssicherheit der Betreiber Kritischen Infrastrukturen, aber nicht an die Informationssicherheit der Lieferkette in der Hard- und Softwaretechnologien adressiert werden (vgl. Koza, 2021, S. 824 f.).

Die Betrachtung der beiden aufgeführten Argumente „ist von großer Bedeutung, da Organisationen unabhängig ihrer Sektorzugehörigkeit in der Regel mit externen IT-Dienstleistern im Bereich der Software- und Hardwaretechnologien arbeiten und somit auf Produkte und Dienstleistungen zurückgreifen müssen, die möglicherweise keine sicherheitstechnischen Merkmale aufweisen. Dabei muss konstatiert werden, dass mögliche Sicherheitslücken in den Hardware- und Software-Komponenten […] aufgrund fehlender Kapazitäten sowie fehlendem Wissen nicht autark analysiert und beseitigt werden können. Vielmehr müssen sich die Organisationen auf die Sicherheitsanalysen, Entwicklungsverfahren und Testverfahren der IT-Dienstleister verlassen, wobei deren Produkthaftungen in der Regel keine sicherheitstechnischen Defizite beinhalten. Innerhalb dieser Betrachtung fehlt die Übertragung der IT-Sicherheit auf Komponentenebene. Bereits bei der Entwicklungsphase sollte darauf geachtet werden, dass die Smartness der Software- und Hardware-Komponenten nicht isoliert für Produktivitätsvorteile eingesetzt wird, sondern auch als Früherkennungseinheiten und zur Detektion und Korrektion von Cyber-Angriffen genutzt werden. In der Summe muss die IT-Sicherheit in die Konzeption, Planung und Herstellung der IT-Komponenten […] einbezogen werden. Additional hierzu beeinflussen das Fehlen von geeigneten Methoden und Werkzeugen (H- Faktor: 30 Prozent sowie das Fehlen von intelligenten Softwarelösungen zu Sicherheitsanalysen (H-Faktor: 40 Prozent die personellen Ressourcenanbindungen […]. Als Gegenkraft hierzu wirken das Vorhandensein von effizienten Werkzeugen und intelligentere Lösungen zur Sicherheitsanalyse (E-Faktor: 66 Prozent), Best Practices sowie Verfahrensharmonisierungen (E-Faktor: 35 Prozent und -Synchronisationen (E-Faktor: 86 Prozent zur Generierung von Synergien“ (Koza, 2021, S. 829).

In Anbetracht der erreichten empirischen Ergebnisse aus der oben aufgeführten Studie lassen sich die bereits getroffenen Aussagen aus den BSI-Sektorstudien reproduzieren und damit der Wahrheitsgehalt der definierten Schlussfolgerungen bestätigen. Die technischen Basisinfrastrukturen stehen nach wie vor großen fachlichen und personellen Herausforderungen. Eine dieser Herausforderungen ist es die OT-Netzwerke mit geeigneten ressourcenschonenden und effizienten Mitteln gegenüber den vorhandenen Schwachstellen in den bereits eingesetzten Soft- und Hardwaretechnologien zu schützen und somit effektiv zur Resilienz-Erhöhung ihrer Systeme beitragen zu können.

Dieser Umstand wird aber auch durch die steigende Cyberkriminalität und den vermehrten Angriffsversuchen auf KRITIS als lukrative Zielscheibe weiterhin dramatisiert (z. B. die Ransomware-Attacke auf die Colonial Pipeline, die Lieferkette von Kaseya in der Lebensmittelindustrie sowie die Ransomware-Attacke auf das Universitätsklinikum Düsseldorf). Bereits seit 2014 beobachten das BSI und das Bundeskriminalamt in der Abteilung „Cybercrime“ eine zunehmende Professionalisierung und Separierung in den cyberkriminalistischen Strukturen.

Bereits in den vergangenen sechs Jahren verzeichnete das BSI insgesamt über 1,175 Milliarden Schadprogrammvarianten (2017: > 600 Mio., 2018: > 800 Mio., 2019: 914 Mio. (+ von 114 Mio. Zunahme zu 2018), 2020: 1,031 Mrd. (+ von 117,4 Mio. zu 2019), 2021: 1,175,4 Mrd. (+ von 144 Mio. zu 2020)), welche durch das Medium Internet im Umlauf sind und die OT-Netzwerke der KRITIS sowohl gezielt als auch willkürlich gefährden und infiltrieren können (vgl. BSI, 2017a, S. 22 | BSI, 2018, S. 91 | BSI, 2019b, S. 75 | BSI, 2020a, S. 36 | BSI, 2021a, S. 9).

Die Summe der bereits aufgeführten argumentativen Kette und Schlussfolgerungen verweist auf ein industrielles Sicherheits- und Forschungsproblem (zu viele Systemschwachstellen versus zu wenige Ressourcen), welches im Sinne der Informations- und Sicherheitstechnik, nach einer pragmatischen und effizienten Antwort verlangt, dessen Hauptfokus im Bereich der Vulnerabilität- und Resilienz-Forschung verankert ist. Diese beiden Schwerpunkte umfassen im Kern die dedizierten sicherheitstechnischen Themengebiete des VM, Risikomanagements, IRM sowie der methodischen Ansätze zur Konzeptualisierung und Operationalisierung von gestaltungsorientierten Modellen und Artefakten.

3. Forschungsdefizit

In den nachfolgenden Abschnitten werden relevante Standards, Empfehlungen, Normen und Forschungsarbeiten vorgestellt, die dedizierte Themengebiete der Informationssicherheit behandeln. Ableitend erfolgt die Darstellung des Forschungsdefizits.

3.1 Untersuchungsergebnisse der nationalen und internationalen Standards

Für ein besseres Verständnis und zur Reduzierung der Komplexität dieser Betrachtungsfelder wird in den nächsten Kapitelabschnitten der Versuch unternommen, zunächst den zu betrachtenden Forschungsbereich durch die Ermittlung von aktuellen theoretischen und praktischen Lösungsansätzen zu konkretisieren und die daraus gewonnen Erkenntnisse auf die ermittelte Quintessenz zu reflektieren, um hieraus die Möglichkeit zur Definition einer Forschungshypothese und konkreten deskriptiven Forschungsleitlinien zu erhalten.

3.1.1 Methodik zur qualitativen Dokumenten- und Inhaltsanalyse

Die Kehrseite der zunehmenden Digitalisierung im Sinne der sicherheitstechnischen Betrachtung ist die steigende Komplexität und Heterogenität der zu schützenden OT-Systeme. Bestehen diese Systeme aus mehreren vernetzten Haupt- und Subsystemen, die in einer komplexen Umgebung miteinander vernetzt sind, so kann eine lokale Sicherheitslücke weitreichende negative Auswirkungen auslösen. Diese Betrachtung ergibt sich aus der Tatsache heraus, dass die existierenden Sicherheitslücken und die daraus resultierenden Ausfallfolgen und Gefahren in der industriellen Umgebung der KRITIS eine direkte Auswirkung auf die physische Welt haben. Während bspw. die Ausnutzung einer Sicherheitslücke in klassischen IT-Systemen eines Versicherungsunternehmens zum Datenabfluss oder Datenverlust führt, kann eine Sicherheitslücke in der industriellen Umgebung eines ÜNBs unmittelbar zu einer Beeinträchtigung der Versorgungskontinuität führen und infolgedessen einen Blackout provozieren.

So kann eine Verletzung der Verfügbarkeit oder Integrität der OT-Systeme in der Energie- und Wasserwirtschaft zu erheblichen Risiken für die Gesundheit und Sicherheit von Menschen führen und schwere Umweltschäden, schwerwiegende finanzielle Probleme wie Produktionsausfälle sowie negative Auswirkungen auf die Wirtschaft eines Landes und der unautorisierten Offenlegung geschützter Informationen haben.

ICS-Netzwerke haben einzigartige Leistungs- und Zuverlässigkeitsanforderungen und verwenden oft Betriebssysteme und Anwendungen, die für das typische IT-Personal als unkonventionell gelten.

Die jüngste Zunahme der Cyberkriminalität und die damit verbundene steigende Anzahl von Ransomware-Angriffen, welche zum großen Teil durch die Ausnutzung der Sicherheitslücken verursacht werden (z.B. Ransomware-Angriff auf das Uniklinikum Düsseldorf durch die Ausnutzung der Sicherheitslücke in der Citrix-Umgebung), tragen dazu bei, dass die technischen Basisinfrastrukturen dem Umgang mit Sicherheitslücken mehr Aufmerksamkeit schenken, um ihre Organisationsstrukturen und kritischen Dienstleistungen besser schützen zu können.

Die steigende Komplexität und der steigende Grad der Vernetzung dieser Systeme in den OT-Netzwerken macht die Beherrschbarkeit dieser Systeme allerdings nicht einfach. Hierbei gilt der Grundsatz, je komplexer und heterogener eine Systemumgebung konzipiert ist, umso schwieriger und zeitaufwendiger ist der Prozess zur Schwachstellenerkennung und -bewertung. Diese Deklaration hat weitestgehend mit der konzipierten organisatorischen und informationstechnischen Struktur der ICS-Netzwerke zu tun.

Einfache Systemumgebungen bestehen meist aus wenigen und überschaubaren IT-Komponenten. Ein kommunales WVU setzt bspw. eine kleine Anzahl an IT-Komponenten in einem homogenen ICS-Netzwerk ein und besitzt daher eine einfache und zentralisierte Organisationstruktur. Durch die überschaubare Anzahl der eingesetzten Soft- und Hardwarekomponenten muss lediglich eine geringe Anzahl an Systemen laufend detektiert und überwacht werden. Der Aufwand zur Sicherstellung der Sicherheit der ICS-Systeme wächst mit der steigenden Anzahl der zu betreuenden Systeme und Subsysteme, die je nach Systemarchitektur über mehrere Standorte unterschiedlich miteinander vernetzt sind.

Mit jedem dazugekommenen Systemknoten wächst auch gleichzeitig die Anzahl der implementierten Schnittstellen und infolgedessen auch die Angriffsflächen, die Reichweite und die Folgen eines Angriffes. Um die existierenden Sicherheitslücken frühzeitig detektieren und behandeln zu können, greifen Sicherheits- und Netzwerkanalytiker auf die methodischen Ansätze zum VM zurück. VM umfasst Methoden zur Schwachstellenerkennung, -bewertung und -behandlung und korreliert unmittelbar mit dem Themengebiet des IRM, um anhand definierter Abläufe und Prozesse eine Reaktion „Response“ zur rechtzeitigen Beseitigung der entdeckten Schwachstellen zu ermöglichen. So können die Themenfelder des VM und IRM als Schlüsselthemen zur Verteidigung von industriellen IT-Systemen im Sinne der ersten Verteidigungslinie (engl. First Line of Defense) definiert werden, welche als integraler Bestandteil des ganzheitlichen Ansatzes der Informationssicherheit zur Resilienz-Erhöhung der IT-Systeme eingesetzt werden.

Dazu werden gezielte technische und organisatorische Mechanismen und Methoden eingesetzt, um mögliche Bedrohungen, Sicherheitslücken sowie Schwachstellen zu identifizieren, um diese im Sinne eines proaktiven Verteidigungsverhaltens vor der tatsächlichen Ausnutzung zu schließen.

Eine effiziente Bewertung und Beseitigung von Schwachstellen ist jedoch auch eine Frage der Entscheidungspräzision und Reaktionsgeschwindigkeit. Bezugnehmend auf eine komplexe und heterogene ICS-Umgebung existiert also eine Vielzahl an Sicherheitslücken, die nicht alle unmittelbar zu einem Systemausfall oder zu einer Verletzung der Versorgungssicherheit führen würden.

Wird diese Tatsache mit der endlichen Anzahl an personellen und zeitlichen Ressourcen von KRITIS in Verbindung gesetzt, so müssen die System- und Netzwerkanalytiker die Folgen einer Vielzahl an Sicherheitslücken bestimmen und diese schließlich gegeneinander abwägen. Diese Abwägung dient der Priorisierung einer Bewertung. Wird die Entscheidung zur Beseitigung einer Sicherheitslücke mit einem mäßigen Schadensausmaß getroffen, während eine andere Sicherheitslücke mit gravierenden und kritischen Schadensausmaß fälschlicherweise nicht mehr weiterbetrachtet oder anders priorisiert wird, entsteht die Gefahr, dass die endlichen Ressourcen ineffizient eingesetzt werden. Durch die Ausnutzung der offen gebliebenen und nicht behandelten Schwachstellen kann somit ein Systemausfall entstehen. So spielen Priorisierungsmethoden und Entscheidungsunterstützungsmodelle im Rahmen des VM eine wesentliche Rolle. Allerdings werden die Prinzipien zum VM und IRM in unterschiedlichen Ansätzen und mit unterschiedlicher Detailtiefe adressiert (vgl. Wang et al., 2018, S. 8599-8609 | Alperin et al., 2020, S. 30-39 | Cullen/Armitage, 2018, S. 1-2 | Ahmad et al., 2021, o. S., | Doynikova/Kotenko, 2018, S. 346-353 | Skopik et al., 2015, S. 1-8 | Tianfield, 2016, S. 782-787).

Um einen adäquaten Überblick über die einschlägigen Lösungsansätze zu erhalten, werden im ersten Untersuchungsschritt die nationalen und internationalen Normen, Standards, Handreichungen und Empfehlungen ermittelt, welche eine wesentliche Rolle zur Sicherstellung und Aufrechterhaltung der Informationssicherheit für ICS darstellen. Zu diesem Zweck wird eine qualitative Dokumenten- und Inhaltsanalyse konzeptualisiert, indem nach den methodischen Ansätzen nach Döring und Bortz (2016), systematisch nach geeigneten nationalen und internationalen Werken gesucht wird. Die Analyse dient als Orientierung zum Thema Informationssicherheit, VM und IRM für ICS. Nach Döring und Bortz (2016, S. 540) wird eine qualitative Dokumentenanalyse bei einem Problem aus der Forschung angewendet, „das[s] sich als offene Forschungsfrage darstellt und somit eine explorative oder theoriebildende Funktion hat.“

In diesem Kontext wird die qualitative Dokumenten- und Inhaltsanalyse anhand des definierten Forschungsproblems aus Kap. 2.4 zur Ermittlung von Bedeutungsgehalten der nationalen und internationalen Standards und Normen eingesetzt (vgl. Döring/Bortz, 2016, S. 540-542).

Hierbei geht es um die Existenz von zusammengehörigen und objektiven Entscheidungskriterien, welche quantifizierbar in ein dynamisches Entscheidungsmodell eingebettet sind, um die Bewertung der anfallenden Sicherheitslücken und daraus folgenden Handlungsoptionen nach der Kritikalität der Zeit und Ausfallfolgen zu bestimmen. Die Ermittlung der vorhandenen einschlägigen Standards und Normen gibt einen Überblick über den Stand der Technik (engl. State of the Art). Zudem ermöglicht es die Generierung von qualitativ beschriebenen Kategorien, welche mindestens eine Verifikation bzw. Falsifikation eines noch zu ermittelnden Forschungsdesiderates erlauben.

Bild 8 illustriert die einzelnen Schritte:

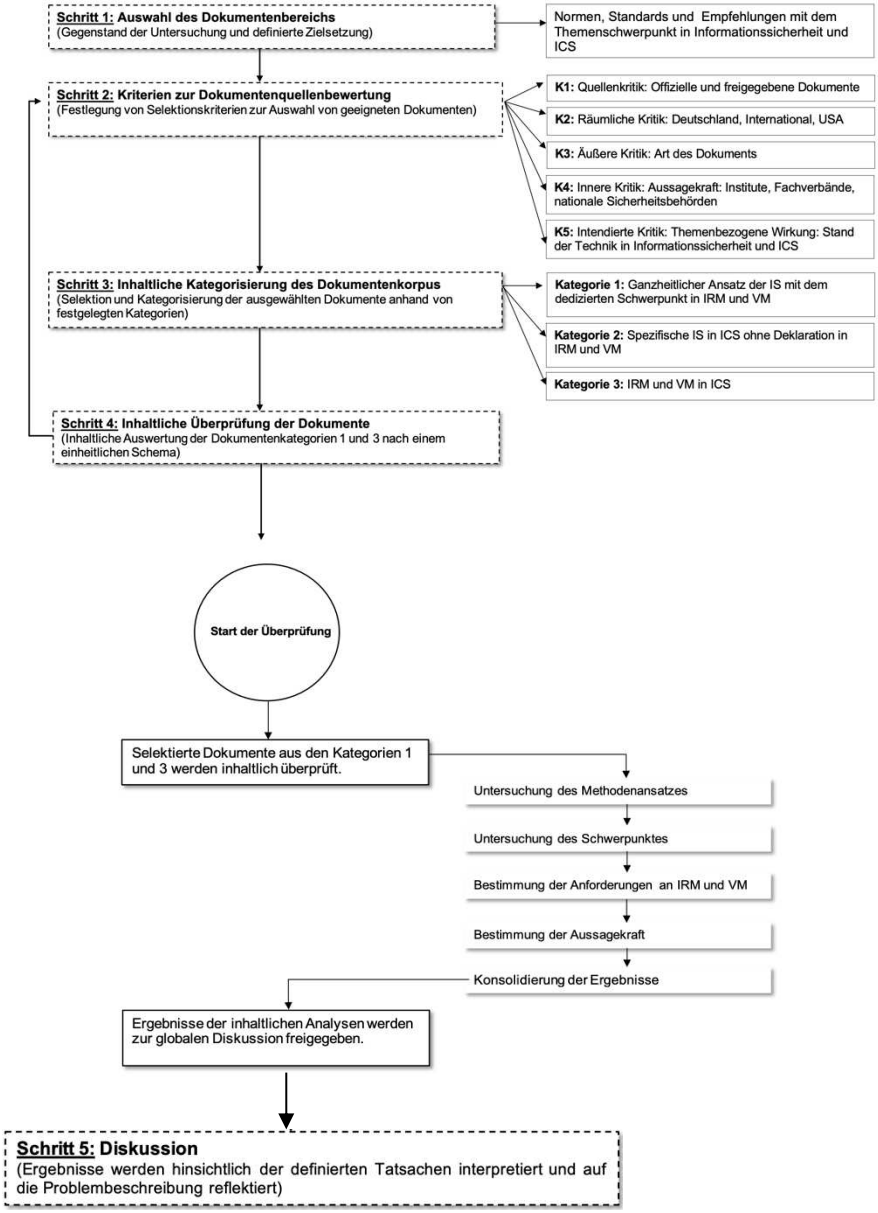


Bild 8: Systematische qualitative Dokumenten- und Inhaltsanalyse (Quelle: In Anlehnung an Kuckartz, 2016, S. 25 | Döring/Bortz, 2016, S. 533-552)

Insgesamt existiert eine Fülle von Standards, Normen, Handreichungen und Empfehlungen, die es System- und Netzwerkanalytikern in ICS-Netzwerken ermöglicht, ihre organisatorischen und technischen Prozesse im Sinne des VM und IRM zu konzipieren.

In der Summe wurden 61 Dokumente identifiziert und in die qualitative Dokumenten- und Inhaltsanalyse integriert (Tabelle 1).

Tabelle 1: Auflistung relevanter Standards, Normen und Empfehlungen für ICS- Netzwerke (Quelle: Eigene Darstellung)

ID	Kennung	Schwerpunkt
I-01	*ISO/IEC 27001: 2017*	*Information security management systems – Requirements*
I-02	*ISO/IEC 27002: 2017*	*Code of practice of information security controls*
I-03	*ISO/IEC 27019: 2020*	*Information security controls for the energy utility industry*
I-04	*ISO/IEC 27035 – 1: 2016*	*Information security incident management – Part 1: Principles of incident management*
I-05	*ISO/IEC 27035 – 2: 2016*	*Information security incident management – Part 2: Guidelines to plan and prepare for incident response*
I-06	*IEC TS 62443-1-1*	*Network and system security in ICS: Terminology, concepts, and models*
I-07	*IEC 62443-1-2*	*Master glossary of terms and abbreviations*
I-08	*IEC 62443-1-3*	*System security compliance metrics*
I-09	*IEC 62443-2-1*	*Establishing an ICS security program*
I-10	*IEC 62443-2-3*	*Patch management in the ICS environment*
I-11	*IEC 62443-2-4*	*Security program requirements for ICS service providers*
I-12	*IEC 62443-3-1*	*Security technologies for ICS*
I-13	*IEC 62443-3-2*	*Security risk assessment for system design*
I-14	*IEC 62443-3-3*	*System security requirements and security levels*
I-15	*IEC 62443-4-1*	*Secure product development lifecycle requirements*
I-16	*IEC 62443-4-2*	*Technical security requirements for ICS components*
I-17	*IEC 62351-1*	*Data and communications security – Part 1: Introduction to security issues*
I-18	*IEC 62351-2*	*Data and communications security – Part 2: Glossary of terms*
I-19	*IEC 62351-3*	*Data and communications security – Part 3: Profiles including TCP/IP*
I-20	*IEC 62351-4*	*Data and communications security – Part 4: Profiles including MMS and derivatives*
I-21	*IEC 62351-5*	*Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*
I-22	*IEC 62351-6*	*Data and communications security – Part 6: Security for IEC 61850*
I-23	*IEC 62351-7*	*Data and communications security – Part 7: Network and System Management (NSM) data object models*
I-24	*IEC 62351-8*	*Data and communications security – Part 8: Role-based access control for power system management*
I-25	*IEC 62351-9*	*Data and communications security – Part 9: Cyber security key management for power system equipment*
I-26	*IEC 62351-10*	*Data and communications security – Part 10: Security architecture guidelines*
I-27	*NERC CIP*	*North American Electric Reliability Corporation Critical Infrastructure Protection*
I-28	*NIST CSF*	*NIST Cybersecurity Framework*
I-29	*NIST SP 800-53*	*Security and Privacy Controls for Information Systems and Organizations*
I-30	*NIST SP 800-61*	*Computer Security Incident Handling Guide*
I-31	*NIST SP 800-82*	*Guide to ICS Security*

I-32	*NISTIR 7628*	*Guidelines for Smart Grid Cybersecurity*
I-33	*DHS CPLS*	*Department of Homeland Security: Cyber Security Procurement Language for Control Systems*
I-34	*N/A*	*Cyber Security Assessments of ICS*
I-35	*N/A*	*Recommended Practice: Improving ICS Cybersecurity with Defense-In-Depth-Strategies*
I-36	*N/A*	*Recommended Practice for Patch Management of Control Systems*
I-37	*N/A*	*Configuring and Managing Remote Access for ICS*
I-38	*N/A*	*Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments*
I-39	*N/A*	*Recommended Practices: Developing an ICS Cybersecurity Incident Response Capability*
I-40	*N/A*	*Catalog of Control Systems Security: Recommendation for Standards*
I-41	*N/A*	*Using Operational Security OPSEC to Support a Cyber Security Culture in Control Systems Environments*
I-42	*N/A*	*Personnel Security Guidelines*
I-43	*N/A*	*Good Practice Guide – Process Control and SCADA Security*
I-44	*N/A*	*Good Practice Guide – Firewall Deployment for SCADA and Process Control Network*
I-45	*IEEE 1686-2007*	*IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
I-46	*DIN SPEC 27009*	*Sector-specific application of ISO/IEC 27001 – Requirements*
I-47	*VDI/VDE-2182 Blatt 1.*	*Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell*
I-48	*VDI/VDE-2182 Blatt 2.1*	*Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomaten für Hersteller - Speicherprogrammierbare (SPS)*
I-49	*VDI/VDE-2182 Blatt 2.2*	*Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomaten für Maschinen - und Anlagenbauer - Umformpresse*
I-50	*VDI/VDE-2182 Blatt 3.1*	*Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller - Prozessleitsystem einer LDPE - Anlage*
I-51	*VDI/VDE-2182 Blatt 3.2*	*Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren - LDPE - Reaktor*
I-52	*VDI/VDE-2182 Blatt 3.3*	*Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber - LDPE - Anlage*
I-53	*NAMUR NA 115*	*IT-Sicherheit für Systeme der Automatisierungstechnik*
I-54	*BDEW – Whitepaper*	*Anforderungen an sichere Steuerungs- und Telekommunikationssysteme*
I-55	*VGB Richtlinie R175*	*IT-Sicherheit für Erzeugungsanlagen*
I-56	*BSI-Standard 200-1*	*Managementsysteme für Informationssicherheit (ISMS)*
I-57	*BSI-Standard 200-2*	*IT-Grundschutzmethodik*
I-58	*BSI-Standard 200-3*	*Risikoanalyse auf der Basis von IT-Grundschutz*
I-59	*BSI-Standard 100-4*	*Notfallmanagement (200-4: Business Continuity Management)*
I-60	*ICS Security Kompendium*	*BSI ICS Security Kompendium*
I-61	*IT-Grundschutz Kompendium*	*BSI IT-Grundschutz Kompendium*

In einem zweiten Prozessschritt (PS) wurden die 61 identifizierten Dokumente anhand der definierten Kriterien aus Bild 8 (Vorselektionskriterien: K1, K2, K3, K4 und K5) mit den Codierungsschlüsseln aus der Tabelle 2 in drei Kategorien unterteilt.

Tabelle 2: Auflistung der Codierungsschlüssel zur Kategorisierung der selektierten Dokumente (Quelle: Eigene Darstellung)

Kriterien	Ausprägung	Schlüssel
***K1**: Quellenkritik*	*Offiziell (freigegeben)*	***O***
	Inoffiziell	***IO***
***K2**: Räumliche Kritik*	*Deutschland*	***D***
	USA	***U***
	International	***I***
***K3**: Äußere Kritik*	*Standard*	***S***
	Handreichung	***H***
	Empfehlung	***E***
***K4:** Innere Kritik*	*Institute*	***In***
	Fachverbände	***F***
	Nationale Sicherheitsbehörde	***N***
***K5**: Intendierte Kritik*	*Informationssicherheit und Incident Response Management*	***ISIRM***
	Incident Response Management und Industrial control systems	***ICSIRM***
	Informationssicherheit und Industrial control systems	***ISICS***

Hierfür wurden die einzelnen Dokumente auf ihren thematischen Schwerpunkt, ihre Zielsetzung und Ausrichtung geprüft. Nach der Kategorisierung der selektierten Dokumente in die drei Kategorien wurden die Dokumenteneinheiten in der Kategorie 1 und 3 in die qualitative Inhaltsanalyse eingebettet und einer semantischen Inhaltsanalyse unterzogen. Insgesamt wurden 13 Dokumenteneinheiten, neun aus der Kategorie 1 und vier aus der Kategorie 3, ausgewählt, welche im Detail sowohl den holistischen Ansatz der Informationssicherheit als auch dedizierte Bereiche der ICS, IRM und VM adressieren und somit in der Lage sind, methodische und systematische Ansätze zu Identifizierungs-, Bewertungs- und Priorisierungsprozessen zu definieren, die eine Vorgehensweise zum Umgang mit Sicherheitslücken, Vorfällen und Ad-hoc-Risiken darstellen. Dem Kategorisierungsschema zur Folge existieren 12 Standards und eine Empfehlung, die organisatorische Strukturen, wie z.B. die Deklaration einer besonderen Aufbauorganisation (BAO) sowie prozessuale Anforderungen zur Erkennung, Bewertung, Behandlung und Beseitigung von Schwachstellen definieren (Tabelle 3).

Tabelle 3: Kategorisierung der selektierten Dokumente für die Dokumenten- und Inhaltsanalyse (Quelle: Eigene Darstellung)

ID	Kennung	K1	K2	K3	K4	K5	Kategorie-Zuordnung
I-01	***ISO/IEC 27001: 2017***	***O***	***I***	***S***	***In***	***ISIRM***	***Kategorie1***
I-02	***ISO/IEC 27002: 2017***	***O***	***I***	***S***	***In***	***ISIRM***	***Kategorie1***
I-03	***ISO/IEC 27019: 2017***	***O***	***I***	***S***	***In***	***ISIRM***	***Kategorie1***
I-04	***ISO/IEC 27035 – 1: 2016***	***O***	***I***	***S***	***In***	***ISIRM***	***Kategorie1***
I-05	***ISO/IEC 27035 – 2: 2016***	***O***	***I***	***S***	***In***	***ISIRM***	***Kategorie1***
I-06	*IEC 62443 - 1 - 1*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-07	*IEC 62443 - 1 - 2*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-08	*IEC 62443 - 1 - 3*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-09	*IEC 62443 - 2 - 1*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-10	*IEC 62443 - 2 - 3*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-11	*IEC 62443 - 2 - 4*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*

I-12	*IEC 62443 - 3 - 1*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-13	*IEC 62443 - 3 - 2*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-14	*IEC 62443 - 3 - 3*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-15	*IEC 62443 - 4 - 1*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-16	*IEC 62443 - 4 - 2*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-17	*IEC 62351 - 1*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-18	*IEC 62351 - 2*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-19	*IEC 62351 - 3*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-20	*IEC 62351 - 4*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-21	*IEC 62351 - 5*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-22	*IEC 62351 - 6*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-23	*IEC 62351 - 7*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-24	*IEC 62351 - 8*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-25	*IEC 62351 - 9*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-26	*IEC 62351 - 10*	*O*	*I*	*S*	*In*	*ISICS*	*Kategorie2*
I-27	***NERC CIP***	***O***	***U***	***S***	***In***	***ICSIRM***	***Kategorie3***
I-28	***NIST CSF***	***O***	***U***	***S***	***N***	***ISIRM***	***Kategorie1***
I-29	***NIST SP 800-53***	***O***	***U***	***S***	***N***	***ISIRM***	***Kategorie1***
I-30	***NIST SP 800-61***	***O***	***U***	***S***	***N***	***ISIRM***	***Kategorie1***
I-31	***NIST SP 800-82***	***O***	***U***	***S***	***N***	***ICSIRM***	***Kategorie3***
I-32	*NIST IR 7628*	*O*	*U*	*S*	*N*	*ISICS*	*Kategorie2*
I-33	*DHS CPLS*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-34	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-35	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-36	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-37	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-38	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-39	***N/A***	***O***	***U***	***H***	***N***	***ICSIRM***	***Kategorie3***
I-40	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-41	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-42	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-43	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-44	*N/A*	*O*	*U*	*H*	*N*	*ISICS*	*Kategorie2*
I-45	*IEEE 1686 - 2007*	*O*	*I*	*H*	*In*	*ISICS*	*Kategorie2*
I-46	*DIN SPEC 27009*	*O*	*D*	*S*	*In*	*ISICS*	*Kategorie2*
I-47	*VDI/VDE - 2182 Blatt 1.*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-48	*VDI/VDE - 2182 Blatt 2.1*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-49	*VDI/VDE - 2182 Blatt 2.2*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-50	*VDI/VDE - 2182 Blatt 3.1*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-51	*VDI/VDE - 2182 Blatt 3.2*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-52	*VDI/VDE - 2182 Blatt 3.3*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-53	*NAMUR NA 115*	*O*	*I*	*H*	*F*	*ISICS*	*Kategorie2*
I-54	*BDEW – Whitepaper*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-55	*VGB Richtlinie R175*	*O*	*D*	*H*	*F*	*ISICS*	*Kategorie2*
I-56	*BSI-Standard 200-1*	*O*	*D*	*S*	*N*	*N/A*	*N/A*
I-57	*BSI-Standard 200-2*	*O*	*D*	*S*	*N*	*N/A*	*N/A*
I-58	*BSI-Standard 200-3*	*O*	*D*	*S*	*N*	*N/A*	*N/A*
I-59	*BSI-Standard 100-4 (200-4)*	*O*	*D*	*S*	*N*	*N/A*	*N/A*
I-60	***BSI ICS Security Kompendium***	***O***	***D***	***S***	***N***	***ICSIRM***	***Kategorie3***
I-61	***BSI IT-Grundschutz Kompendium***	***O***	***D***	***S***	***N***	***ISIRM***	***Kategorie1***

Im vorletzten Schritt werden die 13 ausgewählten Dokumente nach dem vorgegebenen Schema aus Bild 8 „Schritt 4: Semantische Inhaltsanalyse“ qualitativ analysiert. In diesem Zusammenhang folgt die semantische Inhaltsanalyse einem vorgegebenen Schema. Die Definition des Schemas soll im weiteren Verlauf auch dazu dienen, die Ergebnisse aus der Analyse miteinander vergleichbar zu machen.

Zu diesem Zweck werden die Hauptmethodik, der Schwerpunkt und die Aussagekraft der relevanten Dokumente festgehalten und dokumentiert. Anhand der herauskristallisierten Ergebnisse werden mögliche Schlussfolgerungen gezogen, inwieweit die definierten Anforderungen und Methoden die Dynamik und Interaktivität der ICS-Umgebung berücksichtigen und zu einer effizienten Bewertung, Priorisierung und Behandlung von Sicherheitslücken und Schwachstellen beitragen. Bild 9 illustriert die Übersicht und die Aufteilung der ausgewählten Dokumententypen.

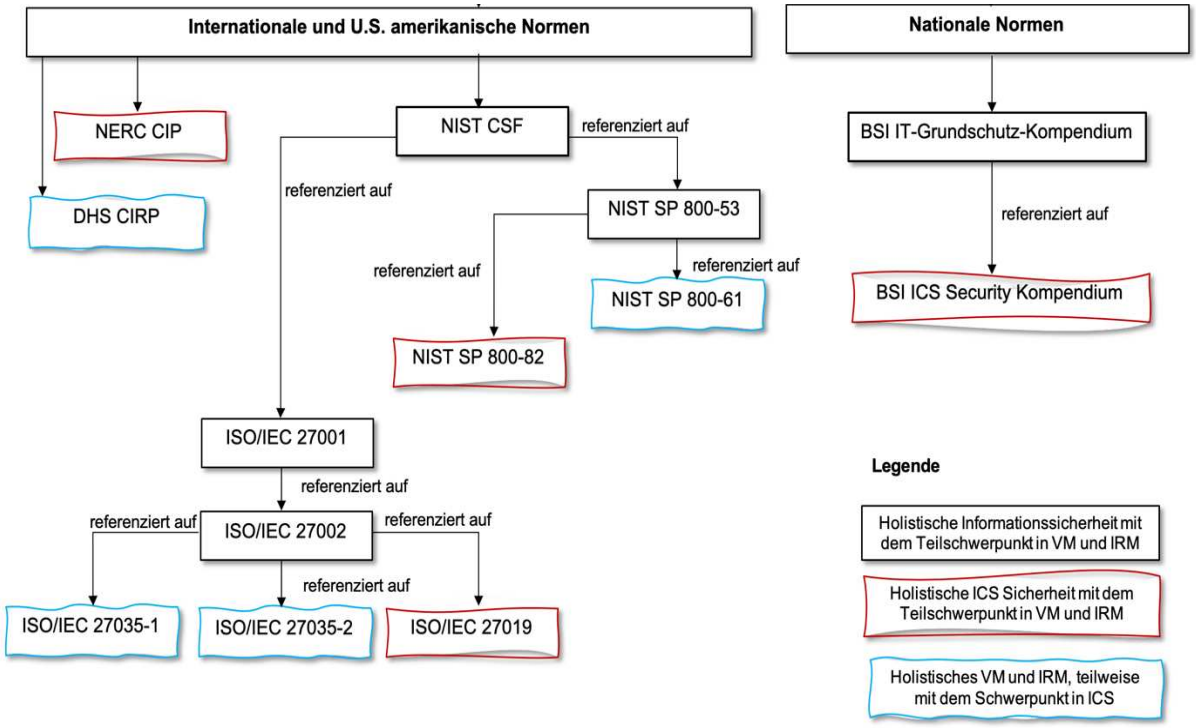


Bild 9: Übersicht der zur qualitativen Inhaltsanalyse selektierten Standards und Normen (Quelle: Eigene Darstellung)

In der gesamtheitlichen Betrachtung existiert derzeit eine Vielzahl an relevanten ICS-spezifischen Standards und Empfehlungen wie bspw. die IEC 62443 Normenreihe, die zwecks sicheren Betriebs von ICS-Netzwerken konkrete Anforderungen an die Informationssicherheit stellt. Allerdings greifen diese jeweils auf ein bestimmtes Sicherheitsgebiet zurück und deklarieren zielgerichtete Anforderungen für ICS und Industrial Automation Control Systems. Bei der IEC 62443 Normenreihe werden grundsätzliche, funktionale Anforderungen an Automatisierungskomponenten sowie Betriebs-, Implementierungs- und Integrations- und Produktionsentwicklungsmodellen definiert, welche sich sowohl an Systemhersteller und Integratoren als auch an Betreiber richten. Die IEC 62351 Normenreihe definiert spezielle Sicherheitsmaßnahmen, die zur Absicherung von industriellen Kommunikationsprotokollen und -Standards in der Energietechnik eingesetzt werden. Neben dieser internationalen Normenreihe existiert auch eine Reihe von Empfehlungen, die im Wesentlichen auf die Arbeit des US-Heimatschutzministeriums (US Department of Homeland Security (DHS)) im Rahmen des Control Systems Security Programs zurückgeführt werden kann.

So werden Anforderungen zur Beschaffungs- und Systemsicherheit der ICS-Komponenten-Hersteller, zur informationssicherheitstechnischen Risikobewertung der ICS, zur Integration des Sicherheitsparadigmas „Defense-In-Depth“ in den ICS-Entwicklungsprozessen und zum Patch-Management der ICS-Netzwerke insbesondere für die Automatisierungs- und Steuerungstechnik definiert. Außerdem werden Empfehlungen zur Analyse von Modem-Verbindungen, Absicherung von Fernzugängen, zur sicheren Installation und zum Betrieb von Funknetzen, zur Deklaration von branchenunabhängigen und allgemeingültigen Sicherheitsmaßnahmen für ICS-Netzwerke, operationellen Sicherheit sowie zur Schulung und Sensibilisierung von ICS-Mitarbeitenden erläutert und in Form von Empfehlungen veröffentlicht.

Zusätzlich zu den internationalen und US-amerikanischen Instituten deklarieren auch die nationalen Fach- und Branchenverbände, darunter der Verein Deutscher Ingenieure e. V. (VDI), Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE), Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DKE), Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW), DVGW, die DWA und Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der Chemischen Industrie (NAMUR) eine Reihe von Handreichungen und Richtlinien, die im Kern dedizierte Themen aus der Informationssicherheit im Kontext der ICS-Netzwerken verfeinern und spezifizieren. Hierunter zählt die VDI/VDE Richtlinie 2182 „Informationssicherheit in der industriellen Automatisierung“ mit den jeweils dazugehörigen Blättern, in denen mit Hilfe eines prozessorientierten und iterativen Ansatzes die grundlegenden sicherheitstechnischen Anforderungen an Hersteller, Integratoren und Betreiber definiert werden.

Zusätzlich hierzu werden auch von NAMUR im Arbeitsblatt NAMUR NA 115 „IT-Sicherheit für Systeme der Automatisierungstechnik“ Sicherheitsanforderungen an die Hersteller der ICS-Komponenten und von der BDEW im BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ zur Absicherung der ICS-Netzwerke in der Energiewirtschaft mit Bezug zur DIN EN ISO/IEC 27002:2017, im Folgenden vereinfacht DIN EN ISO/IEC 27002 definiert.

Die aufgeführten Standards, Normen und Empfehlungen umfassen jeweils einen speziellen Themenschwerpunkt zur Absicherung der ICS und lassen sich der Kategorie 2 zuordnen und werden somit nicht mehr in die qualitative Inhaltsanalyse integriert. Fünf der ausgewählten Dokumente: DIN EN ISO/IEC 27001:2017, im Folgenden DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27002, NIST SP 800-53, National Institute of Standards Cyber Security Framework (NIST CSF) und das BSI IT-Grundschutz-Kompendium stellen jedoch einen holistischen und branchenübergreifenden Ansatz der Informationssicherheit in den Vordergrund der Betrachtung und zeigen eine gemeinsame Schnittmenge, da diese die interaktiven Themengebiete der IT-Sicherheit, der Organisationssicherheit und der individuellen Sicherheitspraktiken des menschlichen Faktors, darunter auch IRM-Prozesse in einem systematischen Vorgehen adressieren.

Diese stellen in diesem Zusammenhang einen systematischen Ansatz zur Implementierung und zum Betrieb eines ganzheitlichen ISMS dar und haben das Ziel ein kontinuierlich angemessenes Niveau der Informationssicherheit zu gewährleisten.

Acht weitere Dokumente stellen eine Verbindung zwischen der Informationssicherheit, ICS und IRM her, deren Zielsetzung mitunter auch in der Bestimmung organisatorischer und technischer IRM-Prozesse innerhalb der ICS-Netzwerke liegt. Um dieses Ziel zu erreichen, greifen diese Normen auf unterschiedliche methodische Ansätze zurück, auf die in den nächsten Kapitelabschnitten konzis eingegangen wird.

3.1.2 NIST Cyber Security Framework (NIST CSF)

Im Gegensatz zu der DIN EN ISO/IEC 27001 und NIST SP 800-53 stellt das NIST mit dem CSF einen risikoorientierten Ansatz dar, dessen Ziel die unternehmensindividuelle Identifikation und Bewertung und Priorisierung von prozessbezogenen Sicherheitsaktivitäten ist (vgl. NIST, 2018, S. 20). Das NIST befasste sich mit der Entwicklung eines flexiblen, kosteneffizienten und leistungsbasierten Ansatzes, um Maßnahmen und Kontrollmechanismen zur Identifizierung, Bewertung und Verwaltung von Sicherheitsaktivitäten zu definieren. Dabei greift das NIST CSF auf eine modulare Struktur aus drei übergeordneten Rahmenwerken: „Framework Core“, „Framework Tiers“ und „Framework Profiles“ zurück.

Das Framework Core besteht aus vier Referenzierungsebenen, in denen insgesamt fünf Funktionen (engl. Functions) auf acht Kategorien (engl. Categories) verweisen, welche wiederum in 108 Unterkategorien (engl. Subcategories) und sechs informative Referenzen, darunter COBIT 5, Center for Internet Security Critical Security Controls (CIS CSC), NIST SP 800-53, DIN EN ISO/IEC 27001, IEC 62443-2-1:2010 und IEC 62443-3-3:2013, im Folgenden IEC 62443-2-1 und IEC 62443-3-3 unterteilt werden. Die fünf Funktionen stellen die höchste Ebene im Framework Core dar (vgl. NIST, 2018, S. 24, zitiert nach Koza, 2022c, S. 34). Das Framework Core besteht aus den folgenden Funktionen (Bild 10): Identifizieren (engl. Identify), Schützen (engl. Protect), Erkennen (engl. Detect), Reagieren (engl. Respond) und Wiederherstellen (engl. Recover) (vgl. NIST, o. J. a, zitiert nach Koza, 2022c, S. 34).

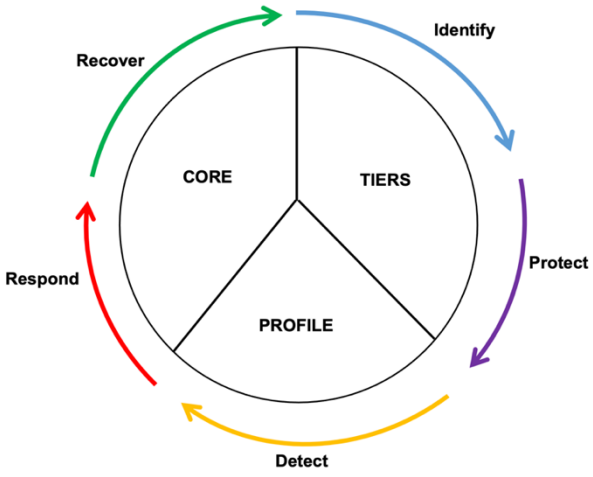


Bild 10: Framework und die Funktionen im NIST CSF (Quelle: In Anlehnung an NIST, o. J. a)

Die Identify-Funktion bietet die Basis für einen ganzheitlichen Verständnisses im Informationssicherheitsmanagement. Es hilft den Anwendern, sich auf ihre Hauptsicherheitsaktivitäten zu fokussieren. Dabei lassen sich die Sicherheitsaktivitäten bedarfsgerecht in Abhängigkeit vom Geschäftskontext, von Ressourcen und der Bedrohungslage sowie in Übereinstimmung mit der Risikomanagementstrategie der Organisation bestimmen (vgl. NIST, 2018, S. 7 f., zitiert nach Koza, 2022c, S. 35). „Die Protect-Funktion umfasst in erster Linie präventive Schutzmechanismen, die dazu dienen, die Geschäftskontinuität der kritischen Dienste und Geschäftsprozesse in der vorgesehenen Qualität und Quantität sicherzustellen“ (Koza, 2022c, S. 35 (eigene Übersetzung)).

Die Detect-Funktion konkretisiert Handlungen, die als Warn- und Früherkennungssysteme eingesetzt werden, um Systemanomalien rechtzeitig zu erkennen. Dazu zählen Handlungen zur Erkennung von Anomalien, die laufende Überwachung von Informationssicherheitsereignissen sowie die Wirksamkeitsüberprüfung von Maßnahmen (vgl. NIST, 2018, S. 7 f., zitiert nach Koza, 2022c, S. 35).

„Die Respond-Funktion umfasst Korrekturmaßnahmen, die im Rahmen des IRM eingesetzt werden, um die Auswirkungen eines potenziellen Informationssicherheitsvorfalls einzudämmen. Sie fasst insbesondere Sicherheitsaktivitäten innerhalb der Reaktionsplanungsprozesse zusammen, die während und nach einem Vorfall zum Einsatz kommen. Diese Prozesse sind sowohl organisatorischer Natur (z.B. die Definition eines Reaktionsteams sowie deren Kommunikationsstruktur) als auch technischer Natur (z.B. digitale forensische Analyse). Darüber hinaus können die gewonnenen Erkenntnisse als Lessons Learned aus aktuellen und früheren Erkennungs- und Reaktionsmaßnahmen als Präventivmaßnahmen zur Vermeidung einer Wiederholung des Informationssicherheitsvorfalls standardisiert und in die bisherigen organisatorischen und technischen Prozesse im Sinne einer kontinuierlichen Verbesserung implementiert werden“ (Koza, 2022c, S. 35 (eigene Übersetzung))

„Die Recover-Funktion umfasst die reaktiven und korrektiven Aktivitäten, die im Krisen-, Notfall- und Katastrophenmanagement eingesetzt werden, um die Dienste und Systeme schnellstmöglich in der erforderlichen Qualität und Quantität wiederherzustellen, die durch ein Schadensereignis beeinträchtigt wurden. So werden diese Aktivitäten in die Notfallvorbereitung (z.B. die Erstellung von Wiederherstellungsplänen, Durchführung von Notfallübungen, Erhöhung der Reaktionsgeschwindigkeit und Validierung definierter Wiederherstellungspläne und -verfahren) und die Koordinierung der internen und externen Kommunikation während und nach der Wiederherstellung eines Schadensereignisses unterteilt“ (Koza, 2022c, S. 35 (eigene Übersetzung)).

Zur Etablierung des NIST CSF, u.a. auch für KRITIS, wird ein sieben-stufiges iteratives Implementierungsmodell vorgeschlagen, in dem die erforderlichen Schritte zur Nutzung des NIST CSF operationalisiert werden können (Bild 11) (vgl. Koza, 2022c, S. 36).

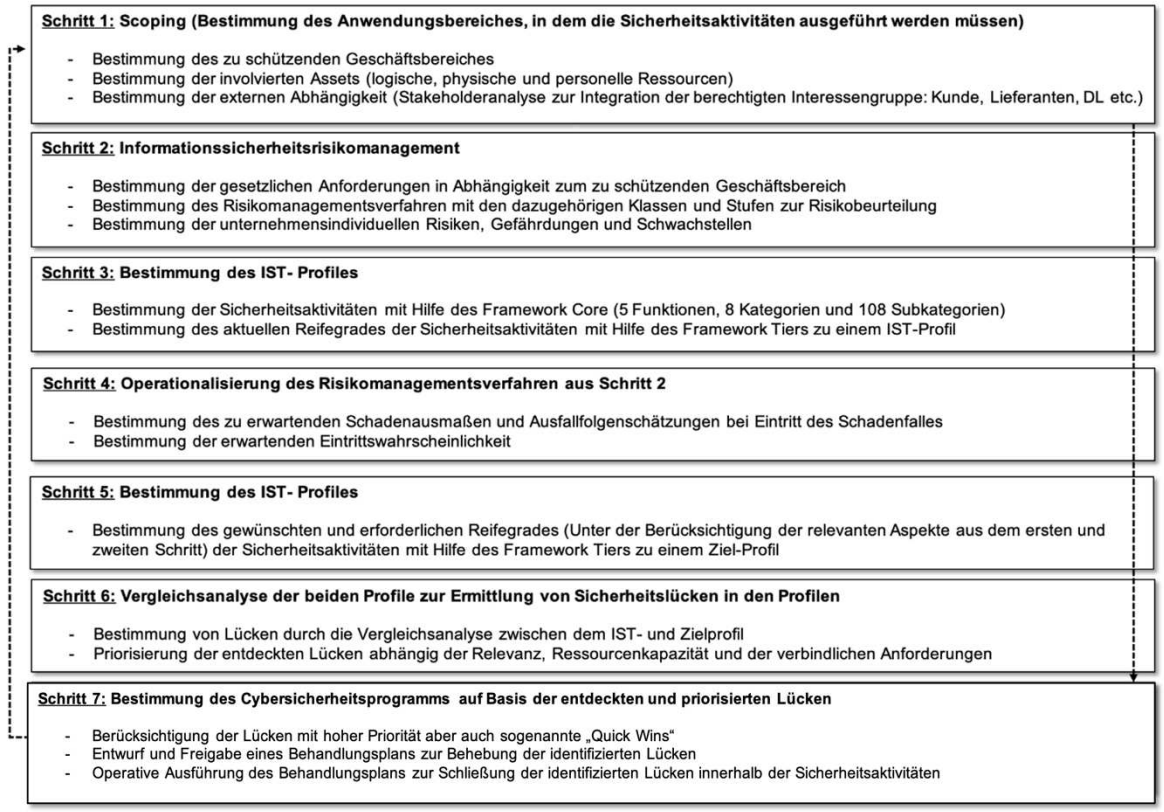


Bild 11: Implementierungs- und Betriebsmodell des NIST CSF (Quelle: In Anlehnung an NIST, 2018, S. 14 f. (eigene Übersetzung))

Zur Operationalisierung des NIST CSF wird im ersten Schritt zunächst der schützenswerte Geschäftsbereich ermittelt. Ausgehend vom zu schützenden Geschäftsbereich erfolgt im zweiten Schritt die Bestimmung der gesetzlichen, regulativen und vertraglichen Anforderungen und der unternehmensrealitätsnahen Gefährdungen und Risiken. Innerhalb des zweiten Implementierungsschrittes erfolgt auch die Bestimmung der globalen Risikomanagementstrategie der Organisation. Im dritten Schritt werden durch Funktionen, Kategorien und Subkategorien des Framework Core die Sicherheitsaktivitäten bestimmt und in ein IST-Profil (engl. Current Profile) nach dem Klassifizierungsschema des Framework Tiers eingebettet und nach dem aktuellen Umsetzungsgrad klassifiziert. Diese Klassifizierungsstufen des Framework Tiers beschreiben einen zunehmenden Reifegrad, den Grad an Strenge und Ausgereiftheit der selektierten Funktionen und Kategorien (vgl. NIST, 2018, S. 14 f., zitiert nach Koza, 2022c, S. 36 f.).

Bevor das IST-Profil mit dem sogenannten Ziel-Profil (engl. Target Profile) verglichen werden kann, wird im vierten Schritt die Bewertung der identifizierten Risiken und Gefährdungen im Rahmen eines Risk-Assessments anhand der zwei Bestimmungsgrößen „Eintrittswahrscheinlichkeit“ „Schadensausmaß“ vorgenommen.

Unter der Berücksichtigung der aktuellen Gefährdungslage und Risiken wird im fünften Prozessschritt das Ziel-Profil bestimmt, in dem die selektierten Sicherheitsaktivitäten des IST-Profils nun mit dem gewünschten und erforderlichen Reifegrad bestimmt werden (vgl. NIST, 2018, S. 14 f., zitiert nach Koza, 2022c, S. 36 f.).

Im sechsten Schritt wird das Ziel-Profil mit dem IST-Profil verglichen, um die möglichen sicherheitsrelevanten und sicherheitsorganisatorischen Abweichungen und Lücken zu identifizieren. Dies ermöglicht der Organisation, je nach Ressourcen und Kapazitäten eine individuelle Entscheidung im letzten Prozessschritt zu treffen, um die identifizierten Lücken unternehmensabhängig zu priorisieren und mit Hilfe eines Behandlungsplans laufend zu optimieren. So wird im siebten Verfahrensschritt ein Aktionsplan bzw. Behandlungsplan definiert, um die herauskristallisierten Lücken zu schließen. Die häufige Wiederholung des NIST CSF Implementierungs- und Betriebsmodells führt zu einer kontinuierlichen Verbesserung des Informationssicherheitsniveaus der Organisation. Das NST CSF ist allerdings eine branchenübergreifende Methode, die sich im Wesentlichen mit der Steuerung und Überwachung von Informationssicherheitsaktivitäten befasst. Aufgrund der etablierten modularen Aufbaustruktur lässt sich das NIST CSF inhaltlich bedarfsgerecht bestimmen. Hierfür spielen die informativen Referenzschichten des NIST CSF eine wesentliche Rolle. Mit Hilfe der informativen Referenzen kann das NIST CSF sowohl mit der DIN EN ISO/IEC 27001, NIST SP 800-53 und CIS CSC als auch mit den ICS-spezifischen Ansätzen wie IEC 62443-2-1 und IEC 62443-3-3 operationalisiert und betrieben werden (vgl. NIST, 2018, S. 14 f., zitiert nach Koza, 2022c, S. 36 f.).

3.1.3 ISO/IEC 27000er-Familie

Ein ISMS ist ein branchenübergreifender, systematischer und prozessorientierter Ansatz zur Einführung, Planung, Umsetzung, Überwachung, Überprüfung und kontinuierlichen Verbesserung der Informationssicherheitsziele einer Organisation. Es umfasst eine große Bandbreite an organisatorischen und sicherheitstechnischen Prozessen, die im Kern zur Sicherstellung und Aufrechterhaltung der Grundwerte der Informationssicherheit „Vertraulichkeit“, „Integrität“ und „Vertraulichkeit“ beitragen.

Dabei wird der Begriff der Informationssicherheit sowohl auf die Gewährleistung der Sicherheit der Informationswerte in Form von digitalen und non-digitalen Informationen als auch auf die Systemsicherheit im Sinne der technischen Sicherheit übertragen. In der Analogie zum NIST CSF wird ein ISMS zur Sicherstellung der Geschäftsziele einer Organisation und somit abhängig vom Geschäftskontext, den Ressourcenkapazitäten und gesetzlichen und vertraglichen Anforderungen operationalisiert. Dabei kann ein ISMS auf unterschiedliche inhaltliche Grundlagen zurückgreifen wie bspw. auf Basis der internationalen Norm der DIN EN ISO/IEC 27001 oder gemäß des BSI IT-Grundschutzes (vgl. DIN EN ISO/IEC 27001, 2017, S. 5 | BSI, 2017b, S. 7). Die DIN EN ISO/IEC 27001 ist ein integraler Bestandteil der 27000er Normenreihe (DIN EN ISO/IEC 27000, 2020) und wurde in Zusammenarbeit zwischen der International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC) entwickelt und veröffentlicht. Der Kerninhalt der DIN EN ISO/IEC 27001 basiert auf der früheren Arbeit des British Standard 7799 der British Standards Institution (BS 7799 Part 2).

Die 27000er Normenreihe greift zur Reduzierung der thematischen Komplexität auf ein fünfstufiges Referenzierungsmodell, indem die einzelnen Themengebiete in einem Top-down-Schema definiert werden.

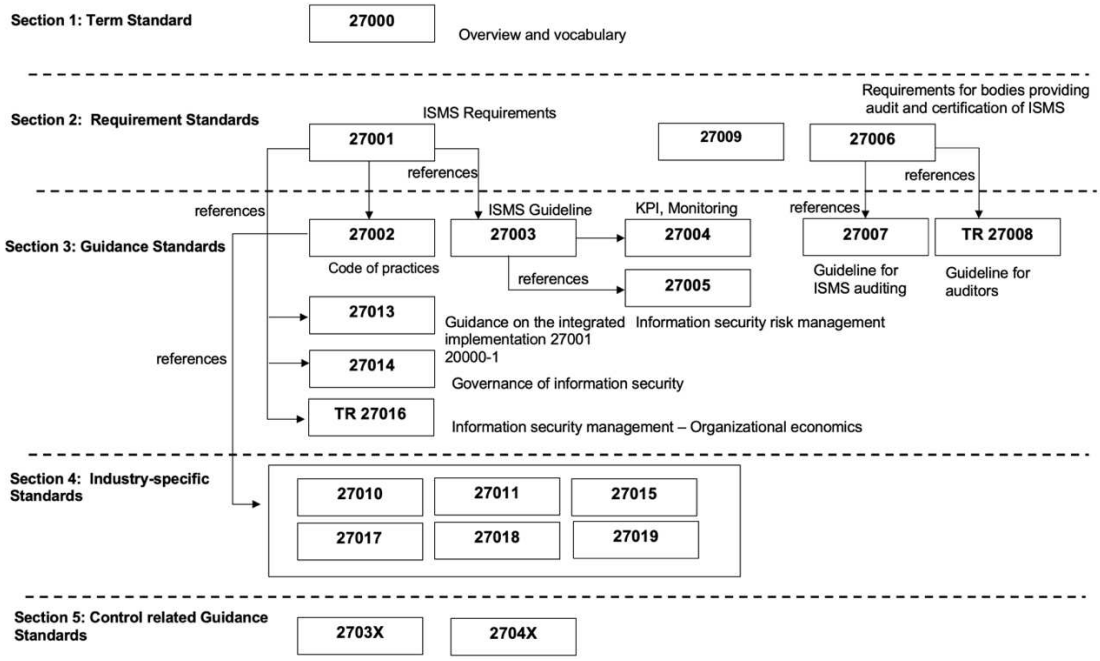


Bild 12: Referenzierungsstruktur der ISO/IEC 27000er Familie (Quelle: Koza, 2022c, S. 29)

Innerhalb dieser Betrachtung besitzen die einzelnen Normen unterschiedliche inhaltliche und formelle Charaktereigenschaften und lassen sich im Detail in normative und informative Standards unterteilen. Unabhängig des jeweiligen Inhalts und der Art der Deklaration stehen die Normen in einer Beziehung zueinander (Bild 12). Hierdurch lassen sich die einzelnen Themengebiete der 27000er Familie in unterschiedliche Sektionen mit verschiedenen Schwerpunkten unterteilen. Die erste Sektion beginnt mit der konzeptionellen Norm der ISO/IEC 27000, die zur Sicherstellung einer gemeinsamen terminologischen Grundlage zwischen den Systemanwendern dient. Die DIN EN ISO/IEC 27000 enthält eine umfassende Begriffserklärung, die in Form eines Glossars aufgelistet wird und als gemeinsame Sprache zu weiterer Nutzung der 27000er Familie angewendet werden kann. Die zweite Sektion enthält insgesamt drei normative Grundlagen: DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27006:2021 und DIN ISO/IEC 27009:2016. Die DIN EN ISO/IEC 27001 teilt sich als normative Grundlage in zwei Bereiche auf und stellt verbindliche Anforderungen an ein ISMS. Im ersten Teilbereich, Kap. 4 „Kontext der Organisation“ bis Kap. 10 „Verbesserung“, werden die wesentlichen Anforderungen aufgeführt, die für den Betrieb eines ISMS bedeutsam sind. Diese Anforderungen adressieren strukturelle, organisatorische und unterstützende Prozesse (vgl. DIN EN ISO/IEC 27001, 2017, S. 6-16):

- zur Bestimmung des ISMS-Anwendungsbereiches (Plan-Phase)
- zur strategischen Definition und Verwendung sachdienlicher Informationssicherheitspolitik,
- zur strategischen Planung der ISMS-Sicherheitsaktivitäten (Plan-Phase),
- zum operativen Betrieb der ISMS-Sicherheitsaktivitäten (Do-Phase),
- zur Integration von finanziellen und personellen Ressourcen (Do-Phase)
- zur laufenden Überwachung der Informationssicherheitsaktivitäten (Check-Phase),
- zur Überprüfung der ISMS-Wirksamkeit (Check-Phase) und
- zur Durchführung von kontinuierlichen Verbesserungsprozessen (Act-Phase).

Diese Anforderungen spiegeln die vier Phasen eines Plans, Do, Check, Act (PDCA)-Zyklus (Demingkreis) wider und dienen als übergreifende und übergeordnete Anforderungen zur grundsätzlichen Etablierung eines effizienten Managementsystems. Der zweite Teilbereich wird im Anhang A der DIN EN ISO/IEC 27001 aufgeführt, indem insgesamt 114 Controls, welche derzeit in 14 Themenbereiche unterteilt sind, aufgelistet werden. Die 14 deklarierten Themengebiete definieren branchenübergreifende holistische Anforderungen an die Informationssicherheit, die im Wesentlichen sowohl Anforderungen an die technische Sicherheit der IT-Systeme wie Netzwerk-, Applikations-, Konfigurationssicherheit als auch an die Querschnittsthemen wie Gebäudesicherheit, Perimeterschutz, Betriebssicherheit, Personalsicherheit, Beschaffungssicherheit, Notfallmanagement und Business Continuity Management und Schulung und Sensibilisierung der Mitarbeitenden definieren (vgl. DIN EN ISO/IEC 27001, 2017, S. 17-31). Die expliziten Anforderungen an die Prozesse des IRM sind im Control A.16 definiert (vgl. DIN EN ISO/IEC 27001, 2017, S. 28 f.):

- A.16.1: Handhabung von Informationssicherheitsvorfällen und -verbesserungen:
  - A 16.1.1: Verantwortlichkeiten und Verfahren,
  - A 16.1.2: Meldung von Informationssicherheitsereignissen,
  - A. 16.1.3: Meldung von Schwächen in der Informationssicherheit,
  - A. 16.1.4: Beurteilung von Entscheidung über Informationssicherheitsereignisse,
  - A. 16.1.5: Reaktion auf Informationssicherheitsvorfälle,
  - A. 16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen und
  - A. 16.1.7: Sammeln von Beweisen,

Insgesamt werden sieben Controls genannt, die die wesentlichen Anforderungen an organisatorische und technische Prozesse des IRM spezifizieren. Um eine adäquate Umsetzung und Erfüllung der Anforderungen zu gewährleisten, verweist die DIN EN ISO/IEC 27001 auf die informativen Grundlagen der DIN EN ISO/IEC 27002 in der dritten Sektion, um die einzelnen Anforderungen aus der DIN EN ISO/IEC 27001 anhand der definierten Implementierungshinweise zu operationalisieren. Die dritte Sektion der 27000er Familie enthält somit eine Reihe von informativen Normen und Leitfäden, die einzelne Themengebiete aus der DIN EN ISO/IEC 27001 aufgreifen und durch explizite methodische Ansätze, definierten Vorgehensweisen und zielgerichteten Umsetzungshinweisen spezifizieren. Zwecks Integration branchenspezifischer Merkmale verweist die DIN EN ISO/IEC 27002 auf die DIN EN ISO/IEC 27019:2020, im Folgenden nur noch DIN EN ISO/IEC 27019, in der vierten Sektion, um die allgemeinen und branchenübergreifenden Umsetzungshinweise um spezifische Zusatzanforderungen und -hinweise für die Akteure in der Energiewirtschaft zu erweitern.

Durch die Integration der vierten Sektion lassen sich im Wesentlichen die industrie-spezifischen bzw. sektorspezifischen Umsetzungshinweise und Leitfäden als Nachtrag zur DIN EN ISO/IEC 27002 definieren. So lassen sich bspw. in der DIN EN ISO/IEC 27019 weitere Umsetzungshinweise zu industriellen Netzwerkprotokollen, der Sicherung von Technikräumen und Leitstellen und weitere ICS-spezifische Merkmale für die Akteure in der Energiewirtschaft deklarieren (vgl. DIN EN ISO/IEC 27019, 2020, S. 27). Für eine genauere Umsetzung der aufgeführten Controls aus A. 16 verweist die DIN EN ISO/IEC 27002 (2017, S. 94) auf die ISO/IEC 27035-Reihe die als maßnahmenbezogenen Leitfadennormen in der letzten Sektion, detaillierte informative und weiterführende Anleitungen zum IRM bereitstellen (vgl. ISO/IEC 27035-1, 2016, S. 1-21, | ISO/IEC 27035-2, 2016, S. 1-57 | ISO/IEC 27035-3, 2020, S. 1-31).

3.1.4 NIST SP 800-53

Die NIST Special Publication (SP) 800-53 (2020) wurde von der U.S. amerikanischen Bundesbehörde NIST für den präventiven, reaktiven und detektierenden Schutz von informationstechnischen Systemen der US-Behörden entwickelt. Das Risk Management Framework (RMF) der NIST SP 800-53 verwendet ein äquivalentes iteratives und inkrementelles Verfahren zum Demingkreis, das in sechs Schritten zur kontinuierlichen Verbesserung ausgeführt wird. Die NIST SP 800-53 greift ebenfalls auf eine modular aufgebaute Aufbaustruktur, in der die einzelnen Anforderungen auf weitere dedizierte Referenzen, Normen und Umsetzungshinweise verweisen. In der Analogie zur DIN EN ISO/IEC 27001 definiert auch die NIST SP 800-53 insgesamt über 900 Anforderungen in 18 „Familien“ (vgl. NIST, 2020, S. 9). Die expliziten Anforderungen an das IRM sind in der „Incident Response“ Familie definiert. Es werden insgesamt 10 Controls beschrieben, die die wesentlichen Anforderungen an das IRM deklarieren (vgl. NIST, 2020, S. F-103-F-110):

- Incident Response: IR-Family:
  - IR-1: Incident Response Policy and Procedures
  - IR-2: Incident Response Training
  - IR-3: Incident Response Testing
  - IR-4: Incident Handling
  - IR-5: Incident Monitoring
  - IR-6: Incident Reporting
  - IR-7: Incident Response Assistance
  - IR-8: Incident Response Plan
  - IR-9: Information Spillage Response
  - IR-10: Integrated Information Security Analysis Team

Zur adäquaten Umsetzung und Erfüllung der Anforderungen verweist die NIST SP 800-53 auf das NIST SP 800-61 „*Computer Security Incident Handling Guide*“. Ähnlich wie die DIN EN ISO/IEC 27001 stellt auch die NIST SP 800-53 (2020, S. xv) einen übergeordneten holistischen Ansatz dar, der keine expliziten branchenspezifischen Anforderungen an die ICS definiert. In derselben Analogie greift auch die NIST SP 800-53 auf ihre Referenzierungsstruktur und verweist auf die NIST SP 800-82 „Guide to Industrial Control Systems (ICS) Security“, um sogenannte Best Practices zur Implementierung und zum Betrieb von Schutzmechanismen für einen sicheren Betrieb von ICS-Netzwerken zu formulieren (vgl. NIST, 2020, S. 16).

3.1.5 BSI IT-Grundschutz-Kompendium Edition 2021

Das IT-Grundschutz-Kompendium (BSI, 2021b) ist das Ergebnis des BSI-IT-Grundschutz-Modernisierungsverfahrens des BSI aus dem Jahr 2018 und dient als branchenübergreifendes Kompendium zur Implementierung von holistischen Anforderungen für die Informationssicherheit, indem die Anforderungen in verschiedene themenspezifische Segmente unterteilt werden. Das IT-Grundschutz-Kompendium greift zur Spezifikation seiner sicherheitstechnischen Anforderungen auf Bausteine zu, die sich in die zwei übergeordneten Bereiche „Prozessbausteine“ und „Systembausteine“ unterteilen lassen (siehe Bilder 13 und 14). Die zwei übergeordneten Bausteine lassen sich in weitere dedizierte unterteilen.

Die Prozessbausteine (Bild 13) werden insgesamt in weitere fünf Bausteine „ISMS (Sicherheitsmanagement)“, „ORP (Organisation und Personal)“, „CON (Konzepte und Vorgehensweisen)“, „OPS (Betrieb)“ und „DER (Detektion und Reaktion)“ ausdifferenzieren (vgl. BSI, 2021b, S. 2 f.). Der IRM-Prozessbaustein „DER (Detektion und Reaktion)“ zergliedert sich wiederum in vier weitere Bausteine (vgl. BSI, 2021b, S. 3):

- *DER 1: Detektion von sicherheitsrelevanten Ereignissen,*
- *DER 2: Security Incident Management,*
- *DER 3: Sicherheitsprüfungen und*
- *DER 4: Notfallmanagement.*

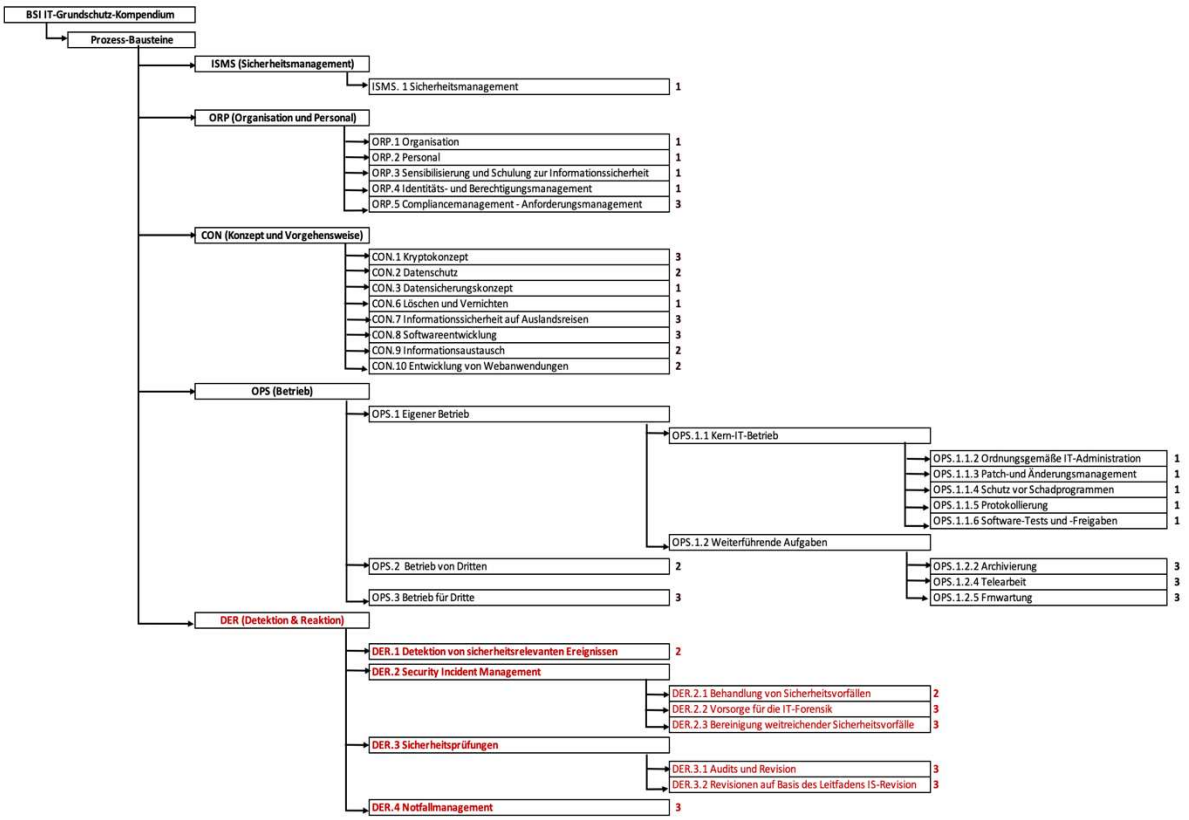


Bild 13: Übersicht der Prozessbausteine des BSI IT-Grundschutz-Kompendiums 2021 (Quelle: In Anlehnung an BSI, 2021b, S. 1-4)

Die Systembausteine (Bild 14) lassen sich insgesamt in fünf Bausteine „APP (Anwendungen)“, „SYS (IT-Systeme)“, „IND (industrielle IT)“, „NET (Netze und Kommunikation)“ und „INF (Infrastruktur)“ unterteilen. Der Systembaustein „IND (industrielle IT)“ spezifiziert die ICS-Sicherheitsanforderungen und teilt sich wiederum in die zwei Bausteine: „IND.1: Prozessleit- und Automatisierungstechnik“ und „IND.2: ICS-Komponenten“ (vgl. BSI, 2021b, S. 1-4)

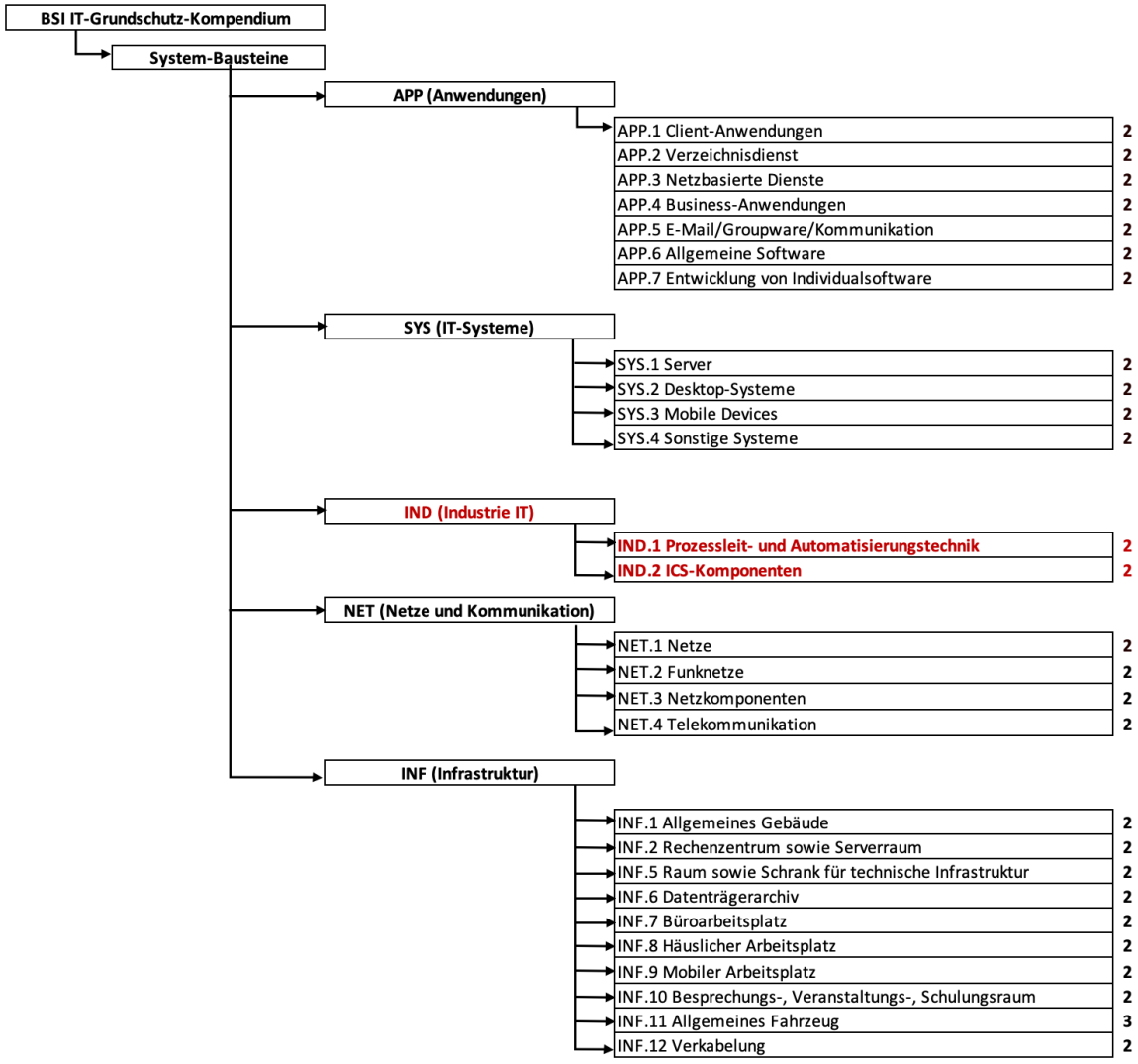


Bild 14: Übersicht der Systembausteine des BSI IT-Grundschutz-Kompendiums 2021 (Quelle: In Anlehnung an BSI, 2021b, S. 3 f.)

Zur Operationalisierung des Kompendiums werden die einzelnen Bausteine abhängig des jeweiligen Geschäftskontexts ausgewählt. Dem Kompendium zugrunde liegenden methodischen Ansatz nach, sollten die einzelnen Bausteine in einer bestimmten zeitlichen Reihenfolge implementiert werden. Der Beginn der Implementierung erfolgt durch die Umsetzung der Basisanforderungen, die in Bild 13 mit „1“ gekennzeichnet sind. Die Umsetzung dieser Bausteine sollte primär erfolgen, da sie grundlegend für einen effektiven Informationssicherheitsprozess sind.

Die Umsetzung der Bausteine mit „2“ stellt die Standardanforderungen dar und sollte anschließend erfolgen. Die Standardanforderungen beschreiben eine Erweiterung des Schutzniveaus und sind für ein nachhaltiges Informationssicherheitsniveau und zur Erreichung des Stands der Technik erforderlich. Die letzte Gruppe umfasst die Anforderungen bei erhöhtem Schutzbedarf und sollte in der zeitlichen Reihenfolge als letztes umgesetzt werden. Dieser hierarchische Aufbau kann als eine Art Implementierungspyramide verstanden werden, die sowohl die zeitliche Reihenfolge als auch das zu erreichende Niveau transparent darstellt (vgl. BSI, 2021b, S. 6).

3.1.6 ICS-Spezifische Standards im Bereich der Informationssicherheit und IRM

Insgesamt existieren derzeit vier relevante ICS-spezifische Standards bzw. Empfehlungen, welche sowohl den holistischen Ansatz der Informationssicherheit als auch das spezifische Themengebiet des IRM miteinander kombinieren und im Grundsatz als Zusatzdokument zur spezifischen Operationalisierung der NIST CSF, NIST SP 800-53, NIST SP 800-61, BSI IT-Grundschutz-Kompendiums oder DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27002 und die ISO/IEC 27035-Reihe im Kontext der ICS-Netzwerke eingesetzt werden können:

- NIST SP 800-82 „Guide to Industrial Control System (ICS) Security,
- BSI ICS Security Kompendium,
- DIN EN ISO/IEC 27019 auf Basis der DIN EN ISO/IEC 27002
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), Cyber Security Standard Critical Infrastructure Protection

Alle vier Dokumente bieten eine Anleitung zur Absicherung von ICS, einschließlich SCADA-Systemen, DCS und anderen Kontrollsystemkonfigurationen und berücksichtigen dabei deren besondere Leistungs-, Zuverlässigkeits- und Sicherheitsanforderungen. Diese zeigen eine individuelle Weiterführung und Spezifikation der branchenübergreifenden Standards und zeigen Best Practices auf, mit deren Hilfe die typischen Bedrohungen und Schwachstellen der ICS-Systeme wirksam bekämpft werden können. Hierbei werden auch die Themengebiete innerhalb des IRM aufgegriffen und um die spezifischen Anforderungen aus dem ICS-Netzwerk erweitert. So greift das NERC CIP auf seine vom Federal Energy Regulatory Commission freigegebene Standardreihe CIP-001 bis CIP-009 zurück und formuliert verbindliche Sicherheitsmaßnahmen zum präventiven, reaktiven und detektierenden Schutz der KRITIS innerhalb der elektrischen Stromversorgung in den USA, Kanada und Mexiko. Das NERC CIP legt in CIP-008 „Incident Reporting and Response Planning” und CIP-009 „Recovery Plans for Critical Cyber Assets” Anforderungen an IRM-Prozesse fest (vgl. NERC CIP, 2019, S. 1 | NERC CIP, 2006, S. 1).

In der Analogie zum NERC CIP bestimmen auch die NIST SP 800-82 (2015, S. 5-25) und das BSI im ICS-Security-Kompendium (2013, S. 49) spezifischere Anforderungen an Detektions-, Response- und Recoveryprozesse, ohne auf eine praxisnahe Umsetzung einzugehen und beschreiben nicht, wie die Schwachstellen objektiv, faktenbasiert, reproduzierbar und effizient bewertet und priorisiert werden können.

3.1.7 DHS, NIST SP 800-61, ISO/IEC 27035-1 und ISO/IEC 27035-2

„Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability" ist eine Empfehlung des US-Heimatschutzministeriums aus dem Jahr 2009, die zur Vorbereitung, Bewertung, Analyse und Reaktion von Sicherheitsvorfällen in ICS-Netzwerken entsprechende Anweisungen deklariert (vgl. DHS, 2009). Dabei gliedert sich die Empfehlung in Planungsaufgaben, Prävention, Management und Post-Incident Aktivitäten wie forensische Analysen. Inhaltlich verweist das DHS größtenteils auf die thematische Darstellung der NIST SP 800-61 (2012) (vgl. DHS, 2009, S. 31).

Im Rahmen der qualitativen Inhaltsanalyse ist ersichtlich geworden, dass die untersuchten Dokumente größtenteils zur Verfeinerung der definierten IRM-Prozesse auf die inhaltliche Darstellung, Anforderungen und Hinweise der beiden speziellen Normen im IRM-Bereich der ISO/IEC 27035 und NIST SP 800-61 verweisen. Sowohl die ISO/IEC 27035-1:2016, ISO/IEC 27035-2:2016, nachfolgend nur noch ISO/IEC 27035-1 und ISO/IEC 27035-2, als auch NIST SP 800-61 beschreiben grundlegende Konzepte und Phasen und zeigen einen strukturierten Ansatz für die Erkennung von Vorfällen, Bewertung und Reaktion sowie die Anwendung der gewonnenen Erkenntnisse, welche in einem modularen 5-Phasen- (ISO/IEC 27035-1) bzw. 4-Phasen-(NIST SP 800-61) Modell abgebildet werden (Bild 15).

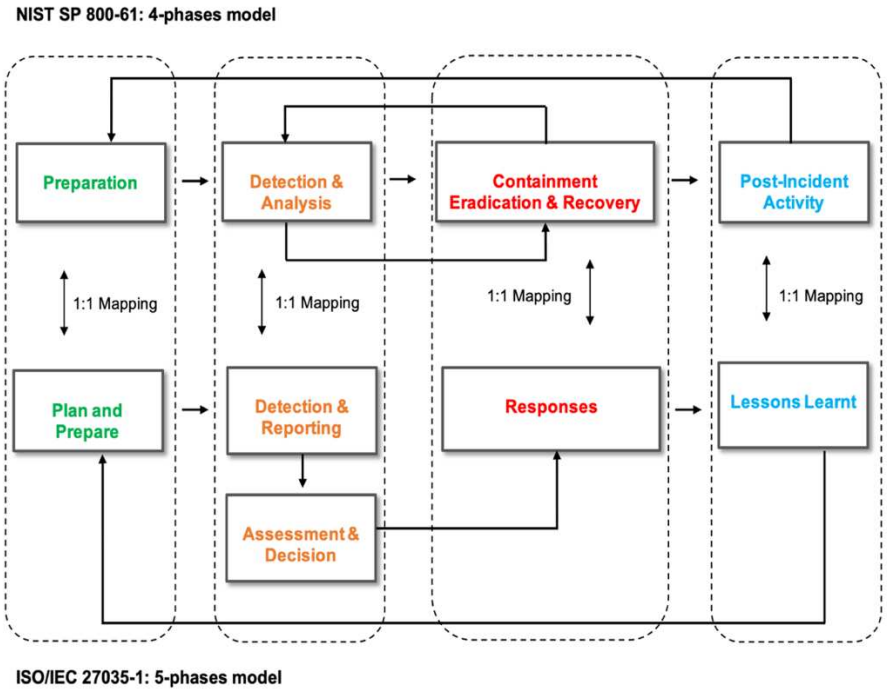


Bild 15: IRM-Phasenmodell nach NIST 800-61 und ISO/IEC 27035-1 (Quelle: In Anlehnung an NIST, 2012, S. 21 und ISO/IEC 27035-1, 2016, S. 7)

Die Gestaltungsprinzipien der beiden Standards sind als branchenübergreifende gültige Prinzipien zu verstehen, die von Organisationen sektorübergreifend implementiert und ausgeführt werden können.

Um die Effektivität der Planung in der Praxis sicherstellen zu können, müssen neben der Integration eines übergreifenden IRM-Leitfadens auch geeignete technische und organisatorische Prozesse in die ersten Phasen der beiden Modelle implementiert werden. Dabei geht es in erster Linie um die Etablierung einer geeigneten technischen und betrieblichen Kommunikationsstruktur zur Integration der internen und externen Schnittstellen, um den Umfang, die Quantität und die Qualität der Informationsbeschaffungsprozesse zur Detektion von Schwachstellen und Sicherheitslücken zu bestimmen. Sekundär liegt der Fokus auf der Einrichtung eines Incident Response Teams (IRT) mit den dazugehörigen Verantwortlichkeiten und Rollen sowie der notwendigen Ausstattung, die zur Überwachung, Bewertung und Durchführung von Erkennungs-, Korrektur- und Reaktionsmaßnahmen eingesetzt werden.

Die ISO/IEC 27035-2 (2016, S. 15) definiert insgesamt drei BAO mit dem „Single type of IRT“ (zentrales IRT mit direkter Verbindung zu den technischen Einheiten am selben Standort), „Hierarchical type of IRT“ (zentrales IRT mit Verbindung zu weiteren IRTs am selben Standort) und „Remote type of IRT“ (zentrales IRT mit direkter Verbindung zu den technischen Einheiten am und außerhalb eines Standortes). So existieren derzeit drei grundlegende Organisationsstrukturen, die je nach spezifischen Ressourcengegebenheiten und ICS-Netzwerkarchitekturen einer Organisation, ausgewählt und operationalisiert werden können. Die zweite Phase, die „Erkennung", befasst sich mit den wichtigsten Aktivitäten zur laufenden technischen und organisatorischen Überwachung interner und externer Netzwerkknoten und Netzwerkaktivitäten sowie zur Erkennung von Anomalien, Schwachstellen und Vorfällen. Auch hier haben die beiden spezifischen Verfahren ISO/IEC 27035-1 (2016, S. 17 f.) und NIST SP 800-61 (2012, S. 10) die gleiche thematische Struktur. Die Analyse von Vorfällen wird hier sowohl manuell über den „Point of Contact“ als auch über automatisierte Erkennungsfunktionen initiiert. Die Sammlung von Situationsinformationen bezieht sich auf Datenquellen aus lokalen Systemen und Netzwerkverkehrs- und Aktivitätsprotokollen wie Intrusion Detection Systemen (IDS) sowie auf extern angebundenen Informationsquellen wie Computer Emergency Response Teams (CERT) und auf Hinweise der nationalen Sicherheitsbehörden (vgl. Koza/Öztürk, 2022b, S. 203-217).

Das Ziel hierbei ist es, ein ganzheitliches 360-Grad-Monitoring zu generieren, das sowohl interne und individuelle Systemeigenschaften und -bedingungen als auch externe Bedingungen wie Vorfalltrends, Angriffsvektoren, aktuelle Angriffsindikatoren und Angriffsstrategien sowie mögliche Handlungsoptionen berücksichtigt. Im Vordergrund dieser Betrachtung stehen die Aspekte des Lagebewusstseins, die als operatives Konstrukt zur Bestimmung der relevanten Sicherheitsparameter zur Ermittlung von Sicherheits- und Gefährdungslage verstanden werden können. Dies ermöglicht einen Zustand, in dem das IRT nicht nur interne Gegebenheiten und Einflussfaktoren, sondern auch die externen Wechselwirkungen und Einflüsse von Systemen bei der Bewertung von Verwundbarkeiten oder Vorfällen berücksichtigen kann. Zu diesem Zweck spezifizieren beide Verfahren die Art der zu erfassenden Informationen, indem sie die notwendigen Informationen, die Art der Quelle, den Umfang der Informationen, die Quantität und Qualität des Informationssicherheitsmeldeverfahrens für Ereignisse, Bedrohungen und Vorfälle und weitere einzubeziehenden Informationen entsprechend benennen.

Auf diese Weise stellen beide Verfahren sicher, dass die Informationen in der gewünschten Qualität und Quantität vorliegen, um sie effizient und ergebnisorientiert auswerten zu können.

Für die Erkennung von globalen Sicherheitsvorfällen werden automatisierte Lösungsansätze wie bspw. der Anschluss an CERT-Meldestrukturen und Computer Incident Response Centers wie Structured Warning Information Format der britischen Regierung vorgeschlagen. Der wesentliche verfahrenstechnische Unterschied zwischen der ISO/IEC 27035-1 und NIST SP 800-61 besteht in der Trennung eines Zwischenschritts zur Bewertung der erfassten Vorfälle, der in beiden Fällen unterschiedlich ausgeführt wird. Während die NIST SP 800-61 den Prozess zur Klassifizierung von Vorfällen in die zweite Phase integriert, wird dieser Prozess in der ISO/IEC 27035-1 in einer separaten Phase „Assessment and Decision“ aufgeführt. Die inhaltlichen Darstellungen sind jedoch identisch (vgl. NIST, 2012, S. 21 | ISO/IEC 27035-1, 2016, S. 10).

Die in den vorangegangenen Phasen bzw. Prozessschritten gesammelten Informationen werden nun im nächsten Schritt ausgewertet. Dabei werden die gesammelten internen und externen Informationen konsolidiert, um die Auswirkungen eines Vorfalls klassifizieren zu können. Darüber hinaus sollten alle Informationen über einen Vorfall, eine Schwachstelle oder ein Ereignis protokolliert und in einer vom IRT verwalteten Datenbank für die weitere Kontextanalyse gespeichert werden. In diesem Zusammenhang liefert die ISO/IEC 27035-2 weitere Informationen, die zur Klassifizierung und Kategorisierung von Vorfällen verwendet werden können. Dabei wird lediglich eine Fülle von Parametern und Bewertungsvektoren aufgezeigt, wie ein Incident bewertet werden kann. Der Deklarationscharakter der definierten Parameter und Vektoren beinhaltet folgende Merkmale (vgl. ISO/IEC 27035-2, 2016, S. 31):

- Bewertung des Incident-Einflusses auf Daten und Informationen,
- Bewertung des Incident-Einflusses auf IT-Systeme,
- Bewertung des Incident-Einflusses auf weitere vor- und nachgelagerte IT-Systeme und Dienste,
- Bewertung des Incident-Einflusses auf den Grundwert „Verfügbarkeit“,
- Bewertung des Incident-Einflusses auf den Grundwert „Integrität“ und
- Bewertung des Incident-Einflusses auf den Grundwert „Vertraulichkeit“.

Wie diese Bewertung in ICS-Umgebungen zu erfolgen hat, wird in den vier ICS-spezifischen Dokumenten nicht erläutert. Hierbei wird lediglich der Hinweis aufgeführt, dass eine Bewertung und Bestimmung der Auswirkungen eines Informationssicherheitsvorfalls bzw. einer Schwachstelle ebenfalls den Einfluss auf die physische Umgebung, mögliche Schäden für die menschliche Sicherheit, die natürliche Umwelt und andere KRITIS mitberücksichtigen sollte. Die Auswirkungen auf die menschliche Sicherheit sollten danach bewertet werden, ob durch eine Fehlfunktion des ICS-Netzwerkes Verletzungen, Krankheiten und somit Gefahr für Leib und Leben möglich sind. Dabei sollten alle zuvor von der Organisation durchgeführten Sicherheitsfolgenabschätzungen für Mitarbeitende und die externen Stakeholder berücksichtigt werden. Auch die Auswirkungen auf die Umwelt sollten unter Umständen berücksichtigt werden. Auf die Frage, wie diese Einschätzung erfolgen soll, wird nicht weiter Bezug genommen.

Nach der Bewertung eines Informationssicherheitsvorfalls bzw. einer Sicherheitslücke muss nun die Entscheidung getroffen werden, wie auf den Vorfall reagiert werden kann. So umfasst die vierte Phase der beiden IRM-Verfahren die Reaktion auf den Vorfall, die gemäß den in der Beurteilungs- und Entscheidungsphase festgelegten Maßnahmen durchgeführt wird. Je nach festgelegter Behandlungsstrategie (gemäß dem Bewertungs- und dem zugehörigen Behandlungsschema) kann die Reaktion in Echtzeit oder mit Verzögerung erfolgen. In diesem Zusammenhang wird ein Reaktionsplan für den Vorfall erstellt, in dem Maßnahmen festgelegt und umgesetzt werden. Sobald die Sicherheitslücke oder der Vorfall abgeschlossen ist, folgt die fünfte Phase der beiden Verfahren. In dieser Phase steht der Gedanke der kontinuierlichen Verbesserung im Vordergrund, wo Lehren aus dem Umgang mit dem Vorfall gezogen werden. In der fünften Phase „Lessons learned" oder „Post-Incident-Aktivität“ werden die identifizierten Behandlungsmaßnahmen überprüft und als qualitätssichernde Rückkopplung in die IT-Prozesse im Sinne der Prävention implementiert, um eine Wiederholung des Vorfalls zu vermeiden. Die nachfolgende erweiterten ereignisgesteuerten Prozesskette (eEPK)-Modellierung illustriert diese zuvor beschriebenen VM- und IRM-Phasen (Bild 16).

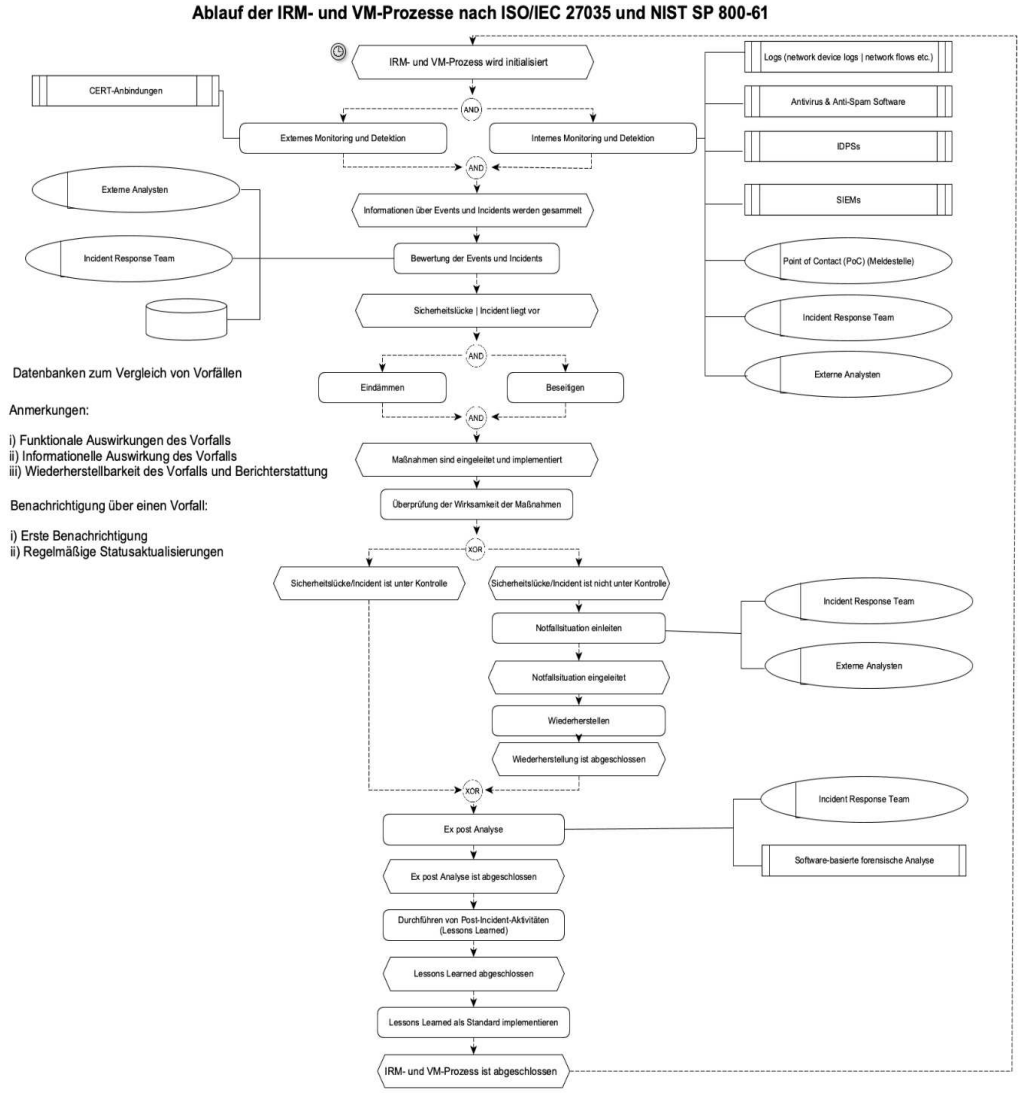


Bild 16: Ablauf der IRM-Prozesse nach NIST 800-61 und ISO/IEC 27035-1 (Quelle: In Anlehnung an NIST 800-61 und ISO/IEC 27035-1)

3.1.8 Zusammenführung der Analyseergebnisse

Aus der qualitativen Inhaltsanalyse lassen sich nun folgende Schlussfolgerungen ziehen: Alle fünf ausgewählten holistischen Ansätze lassen sich größtenteils auch ICS-spezifisch instanziieren und stellen somit Vorgehensweisen für IRM-Prozesse dar. Diese umfassen einen systematischen und vordefinierten Anforderungskatalog, um das IRM der Organisation effektiv und nachhaltig zu etablieren. Der metakonzeptionelle Charakter dieser Verfahren ermöglicht es Organisationen unabhängig der Sektorenzugehörigkeit, die Prozesse zum IRM zu operationalisieren und flexibel an ihre Strukturen anzupassen. Aufgrund der vorherrschenden Komplexität und Vielfalt der Themengebiete werden bei allen fünf dargestellten ganzheitlichen Methoden über eine Referenzmodellierung einzelne Themenbereiche definiert, die wiederum in ihre weiteren integralen Bestandteile zerlegt werden.

Dabei greifen die holistischen Ansätze auf weitere spezifische Normen zurück, um zum einen Umsetzungshinweise und detaillierte Leitfäden zu generieren und zum anderen die allgemeingültigen Anforderungen, um die branchespezifischen Merkmale zu erweitern. Dies dient zur Reduzierung der thematischen Vielfalt und Komplexität der Informationssicherheit. Als Resultat definieren die Normen primär „was zu tun ist“ und sekundär „wie das was umgesetzt werden kann“. Allerdings werden die Umsetzungshinweise zum Teil nicht in der erforderlichen Detailtiefe aufgeführt. Als Beispiel kann die folgende Fallbeschreibung herangezogen werden: Bei der Betrachtung einer Sicherheitslücke sollen alle möglichen Einflüsse auf die Datensicherheit und Systemsicherheit sowie die daraus resultierenden Gefahren für die Versorgungssicherheit zur Beurteilung dieser Sicherheitslücke herangezogen werden. Wie soll nun der Einfluss einer Sicherheitslücke faktenbasiert, objektiv und anhand von reproduzierbaren Entscheidungskriterien bestimmt werden? Die aufgelisteten holistischen Ansätze liefern keine Antwort auf diese Frage.

Im Gegensatz zu den ganzheitlichen Ansätzen geben die vier IRM-spezifischen Standards den Anwendern weitere Verfahrensanweisungen, wie ein strukturierter IRM-Ansatz geplant, operationalisiert und kontinuierlich optimiert werden kann. Dazu werden iterative und inkrementelle Phasenmodelle aufgezeigt, die dem Anwender einen leichten Einstieg erlauben. Dadurch ist es möglich, die einzelnen Phasen trotz der sequenziellen IRM-Prozessmodellierung zu parallelisieren, um bspw. die Reaktionsgeschwindigkeit der IRM-Prozesse zu beschleunigen.

So können die einzelnen Aufgaben exemplarisch für das Monitoring, Reporting, die Analyse, Bewertung, sowie Durchführung und Integration von Maßnahmen durch Aufgabentrennung den Rollen zugewiesen werden, die über spezielles Wissen verfügen.

Bei der Betrachtung der vorgestellten Phasenmodelle werden jedoch auch weitere grundsätzliche Defizite deutlich. Die definierten iterativen und inkrementellen Phasenmodelle erklären nicht, **wie** die Anwender ihre gewonnenen internen und externen Informationen zur Generierung von wertvollem Wissen kombinieren können. Es gibt kein geeignetes Schema, in dem aus Beobachtungen (Monitoring) und einer Abbildung dieser Beobachtungen (Analyse) proaktive Entscheidungen abgeleitet werden können.

Ferner wird auch nicht definiert, welche der weltweit definierten Methoden zur globalen externen Informationsgewinnung (siehe Kap. 3.2) am ehesten in Frage kommen. Hierbei wird lediglich die Anbindung an ein CERT vorgeschlagen.

Folglich fehlen in den vorgestellten spezifischen IRM-Standards Entscheidungsmodelle oder Strategien, wie die explizite Bewertung einer Schwachstelle anhand von objektiven Parametern erfolgen soll. Im Detail deklarieren die untersuchten Standards, unabhängig davon, ob diese ICS-spezifisch oder allgemeingültig deklariert sind, lediglich die organisatorischen und technischen Anforderungen, sodass hier nur die Effektivität der Anforderungen in den Vordergrund gestellt werden, gemäß dem Motto „das Richtige tun“. Allerdings bleibt die Frage offen, wie die Bewertung und Priorisierung von Schwachstellen, insbesondere personenunabhängig erfolgen soll.

Die Antwort auf diese Frage adressiert die Effizienz einer Anforderung, die nur dann erreicht werden kann, wenn sachdienliche und adäquate Lösungsansätze existieren, sodass die Anforderungen ressourcenschonend, zielführend und wirksam umgesetzt werden können. Die vorgestellten Phasenmodelle lassen auch die Tatsache unberücksichtigt, dass die Effizienz einer Entscheidung bzw. Bewertung nicht nur von der Geschwindigkeit der Bewertung, sondern auch von der Qualität der Entscheidung bzw. Bewertung einer Sicherheitslücke abhängig sind. In der Folge konzentrieren sich die vorgestellten Phasenmodelle auf die selektive und konstruktive Wahrnehmung, was einer subjektiven, nicht nach Faktenlage getroffenen Bewertung gleichkommt.

Die IRM-Anforderungen zeigen somit eine verstärkte Fokussierung auf die Geschwindigkeit. Dies mag an erster Stelle eine sinnvolle Vorgehensweise darstellen, um bspw. mit Hilfe von schnell ausführbaren und trainierten korrektiven Maßnahmen das Schadensausmaß eines Angriffes unverzüglich eindämmen zu können. Allerdings ist die Reaktionsgeschwindigkeit nur eine Komponente von vielen, die eine wesentliche Rolle zur Bewertung und Behandlung von Schwachstellen und Sicherheitslücken darstellt. Während also die Reaktionsgeschwindigkeit durch etablierte Trainingsstrukturen und regelmäßige Wiederholungen der Phasenmodelle sowie Notfallübungen sehr schnell optimiert werden kann, bleibt die Entscheidungsqualität ein subjektives und individuelles Merkmal, das in der Regel von der Verhaltensintention, der Salienz und damit vom Wissensfaktor des jeweiligen Entscheidungsträgers abhängig ist. Die Entscheidungsqualität kann aber auch durch den Einsatz von Entscheidungsunterstützungsmodellen und objektiven Berechnungsmodellen zur Analyse der Kausalkette (Ursache-Wirkungs-Analyse) und zur Ableitung von Handlungsoptionen optimiert werden. Dabei wird hier der Fokus auf die **Präzision** einer Entscheidung und damit auf die Korrektheit, Validität, und Objektivität einer Bewertung gelegt.

Bewertungen erfolgen weitestgehend personengebunden. So kann ein Sicherheitsvorfall oder eine Sicherheitslücke auf Basis der subjektiven Erfahrungswerte und des individuellen Sicherheitsbewusstseins des jeweiligen Bewerters erfolgen. Führt ein anderer Analyst die Bewertung derselben Sicherheitslücke durch, so kann das Ergebnis der Bewertung anders ausfallen, da es kein einheitliches und objektives Bewertungsmuster mit entsprechenden Regeln und Beziehungen gibt.

Das kann dazu führen, dass ein gravierender Vorfall auf Grund von Sturheit oder einem falschen und trügerischen Sicherheitsgefühl als False Negative (FN) deklariert wird und nicht mehr zur Behandlung freigegeben wird. Das kann u.a. zu katastrophalen Folgen und kritischen Systemzuständen führen.

Zurück zu dem ursprünglichen Forschungsproblem aus Kap. 2.4 muss nun in Ermangelung an effizienten praktischen Lösungsansätzen die Aussage getroffen werden, dass die derzeitigen allgemeingültigen und ICS-spezifischen Standards im Bereich der Informationssicherheit, IRM und VM keine kohärenten und objektiven Entscheidungskriterien definieren, welche quantifizierbar und instanziierbar in ein dynamisches Entscheidungsmodell eingebettet sind, um die Bewertung der anfallenden Sicherheitslücken und daraus folgenden Handlungsoptionen nach der Kritikalität von Zeit, der Ausfallfolgen und des Aufwands zu bestimmen. Damit erfüllt die qualitative Inhaltsanalyse den Zweck, indem zunächst die Verifikation des Forschungsdesiderates bestätigt wird.

Wie groß diese thematische und praktische Lücke ist, zeigen auch die aufgeführten industriellen Forschungs- und Lösungsansätze im Kapitelabschnitt 3.2, die aufgrund ihrer dynamischen Forschungseigenschaft bei der Fragestellung: „Wie können die Sicherheitslücken in Hard- und Software bestimmt, bewertet und behandelt werden?“ viel weiter sind als die klassischen und spezifischen Industriestandards. Demgemäß werden im nachfolgenden Abschnitt die aktuellen Forschungsergebnisse im Bereich des VM aufgezeigt und näherbeschrieben.

3.2 Untersuchung der aktuellen Forschungsarbeiten

Das VM umfasst ein breites Spektrum an differenzierten Forschungsbereichen, welche in die interdisziplinäre Forschung eingebettet sind. Es existieren mehrere technische und empirische Forschungsstränge, die sich im Sinne einer gestaltungsorientierten Forschung mit der Konzeption und Entwicklung von technischen Überwachungssystemen, intelligenten Algorithmen zur Datenanalyse und Methoden zur Schwachstellenerkennung und -analyse befassen. Eine der Forschungsschwerpunkte liegt hier vor allem auf der globalen Sammlung, Konsolidierung und Bewertung von Schwachstellen in den Computersystemen wie bspw. das Exploit Prediction Scoring System (EPSS)) und CVSS (vgl. Bolívar et al., 2019, S. 1-6 | (Vanamala et al., 2020, S. 1-5 | Kebande et al., 2018, S. 1-10 | Almukaynizi et al., 2017, S. 82-88).

So mündeten die Forschungsarbeiten des National Infrastructure Advisory Council (NIAC) im Februar 2005 zur Einführung von CVSS in Version 1 (CVSS v1) mit dem Ziel eine offene, universelle und standardisierte Schweregradbewertung von Soft- und Hardwareschwachstellen und Sicherheitslücken bereitzustellen. Im späteren Verlauf des Jahres 2005 wurde das Forum of Incident Response and Security Teams (FIRST) von NIAC als Betreuer zur weiteren Entwicklung der CVSS-Methodik beauftragt. Aktuell wird zur globalen Bewertung von Schwachstellen weltweit auf die von FIRST weiterentwickelte CVSS-Version 3.1 zurückgegriffen (vgl. FIRST, 2005, o. S. | NIAC, 2005, S. 8).

Das CVSS ist ein international anerkannter Industriestandard mit einem einheitlichen Informations- und Bewertungsschema zur Bewertung des Ausfallgrades im Sinne der Ausfallfolgenschätzung von Schwachstellen und Sicherheitslücken in Computersystemen.
Das CVSS bestimmt die wichtigsten technischen Aspekte von Schwachstellen in Soft-, Hard-, und Firmware (vgl. FIRST, o. J. a, S. 2 ff.).

Die Ergebnisse umfassen numerische Punktzahlen, die den Schweregrad einer Schwachstelle verglichen zu anderen Schwachstellen darstellen. CVSS besteht aus drei metrischen Gruppen (Bild 17): Base, Temporal und Environmental. Die Base-Metrics stellen den Schweregrad einer Schwachstelle gemäß ihren inhärenten Merkmalen dar, die im Laufe der Zeit gleichbleiben. Die Temporal Metrics passen die Base-Metrics einer Schwachstelle basierend auf volatilen und dynamischen Faktoren an, die sich mit der Zeit ändern, wie etwa das Vorhandensein von Exploit-Codes (praktisch ausführbarer Programmcode zur Ausnutzung definierter Schwachstellen) (vgl. FIRST, o. J. a, S. 2 ff.).

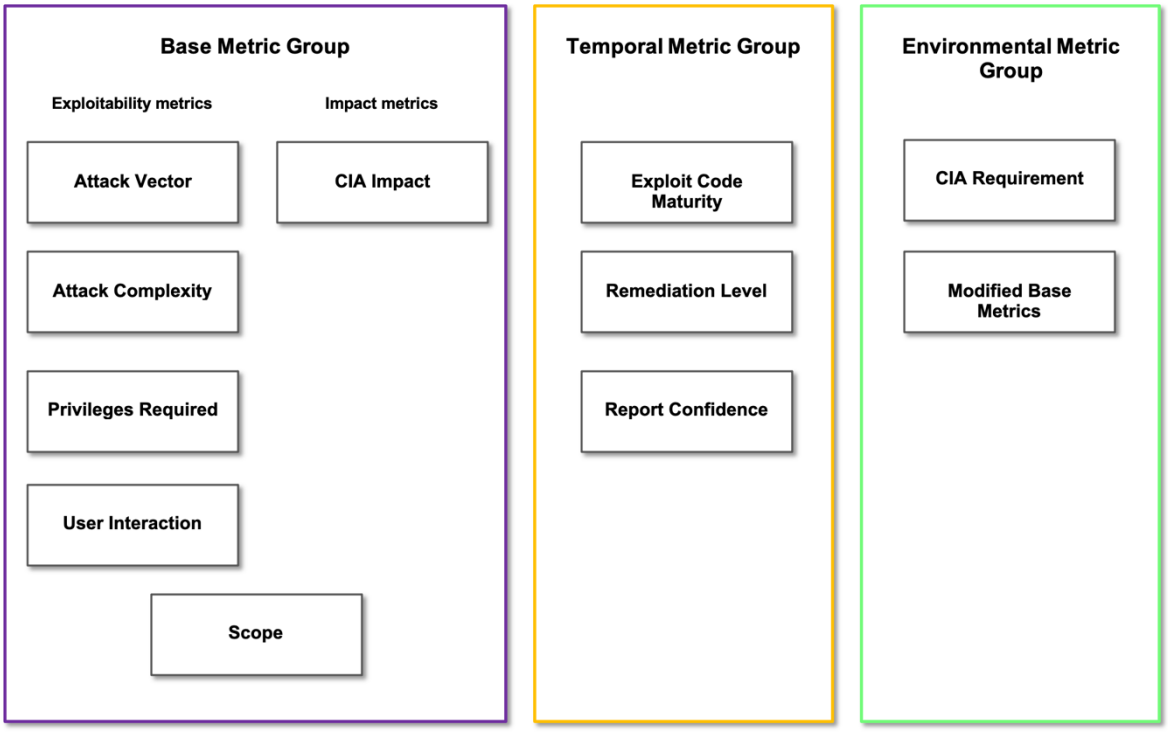


Bild 17: CVSS-v 3.1. Metriken (Quelle: First, o. J. a, S. 3)

Die Umgebungsmetriken passen die Base und Temporal Metrics an eine bestimmte Umgebung an. Diese berücksichtigen Aspekte wie die Verfügbarkeit von präventiven oder reaktiven Maßnahmen sowie individuelle Systemeigenschaften in den dedizierten Umgebungen. Die eigentliche individuelle Bewertung muss jedoch von der Organisation eigen erstellt werden, die das verwundbare bzw. betroffene Produkt verwaltet. In der Regel werden nur die Base Metrics publiziert, da diese sich nicht ändern und für alle Umgebungen entsprechend gleichbleiben.

CVSS-Anwender werden bspw. dazu aufgefordert, den vom CVSS definierten Basis-Score durch individuelle Temporal und Environmental Metrics zu ergänzen, um einen Ausfallgrad zu erhalten, der für ihre spezifische Unternehmensumgebung und Netzwerklandschaft zugeschnitten ist. So können CVSS-Informationen in Schwachstellenmanagementprozesse integriert werden, um Bedrohungen für Netzwerklandschaften unternehmensspezifisch einstufen zu können. Dadurch können fundierte und belastbare Entscheidungen zur Behebung von Schwachstellen getroffen werden (vgl. FIRST, o. J. a, S. 2 ff.).

„Solche Faktoren können sein: Anzahl der Kunden einer Produktlinie, monetäre Verluste aufgrund einer Sicherheitslücke, Bedrohung von Leben oder Eigentum oder die öffentliche Meinung zu öffentlichkeitswirksamen Sicherheitslücken. Diese Faktoren liegen außerhalb des Anwendungsbereichs von CVSS. Zu den Vorteilen von CVSS gehört die Bereitstellung einer standardisierten, hersteller- und plattformunabhängigen Methodik zur Bewertung von Schwachstellen. Es handelt sich um ein offenes Rahmenwerk, das Transparenz über die einzelnen Merkmale und die Methodik zur Ableitung einer Bewertung bietet“ (FIRST, o. J. a, S. 2 ff. (eigene Übersetzung)).

So wird der CVSS-Base-Score auf der Grundlage einer nummerischen Berechnungsformel aus den Base Metrics ausgearbeitet. Die Skala-Werte reichen von 0 bis 10, wobei 10 die kritischste Stufe darstellt. Um die Berechnungsmethodik der CVSS nutzen zu können, greift FIRST auf das CVE-System zurück (vgl. FIRST, o. J. a, S. 16). Das CVE-System bietet eine Referenzmethode für öffentlich bekannte Schwachstellen, Gefährdungen und Sicherheitslücken in Computernetzwerken. Das National Cybersecurity „Federally Funded Research and Development Centers“ der Vereinigten Staaten, das von der MITRE Corporation betrieben wird, unterhält das System mit finanzieller Unterstützung der US National Cyber Security Division des US DHS. Das CVE-System wurde im September 1999 der Öffentlichkeit offiziell zugänglich gemacht (vgl. Mann/Christey, 1999, o. S. | CVE, o. J. a).

Neben FIRST verwendet auch das Security Content Automation Protocol das CVE-System, um Schwachstellen weltweit einmalig und wiedererkennbar zu kennzeichnen und diese der sicherheitstechnischen Gemeinschaft global zur Verfügung zu stellen. Der praktische Grund für die Deklaration dieser Kennung liegt in der Tatsache, dass es im Allgemeinen schwierig ist, von einer bestimmten Sicherheitslücke zu sprechen, da viele Soft- und Hardwareprodukte existieren, die eine Vielzahl an Sicherheitslücken haben können. CVE-Kennungen geben daher jeder Sicherheitslücke eine einmalige und atomare ID, so dass man weltweit über bestimmte Sicherheitslücken transparent sprechen kann, indem die CVE-ID (zusammengesetzt aus CVE-Präfix-Jahr (YYYY)-beliebige Ziffer (NNNNN)) verwendet wird. Die Dokumentation der MITRE Corporation definiert CVE-Kennungen bzw. CVE als eindeutige, gemeinsame Kennungen für öffentlich bekannte Informationssicherheitsschwachstellen in bekannten Soft- und Hardwarewarepaketen. So werden CVE von einer CVE Numbering Authority zugewiesen. Die CVE werden in den beiden Datenbanken von MITRE und der US National Vulnerability Database (NVD) aufgeführt (vgl. NIST, o. J. b | CVE, o. J. b.).

Ferner greift auch das CERT der Deutschen Telekom (dCERT) auf die beiden CVE-Datenbanken zu und publiziert und bewertet diese im Rahmen des Vulnerability Advisory Services für alle Organisationen, welche sich an dieser Dienstleistung der Deutschen Telekom angeschlossen haben (vgl. CVE, o. J. c. | dCERT o. J.).

So stellen die CVSS-Methodik und das CVE-System ein globales Bewertungs- und Identifizierungsschema für Sicherheitslücken und Schwachstellen in den Hard- und Softwarekomponenten dar. Allerdings wird auch hier nicht erläutert, wie aus dieser globalen Bewertung eine unternehmensindividuelle Bewertung generiert werden kann. Es werden lediglich übergeordnete Parameter benannt, welche zwecks individueller Bewertung herangezogen werden können. Die eigentliche Frage zur Definition von objektiven und validen Entscheidungsparametern bleibt offen. Dennoch ist die CVSS-Methodik ein sinnvolles Instrument, sodass mit Hilfe des globalen CVSS-Base-Score und des CVE-Systems die Bewertungsprozesse erstmal initialisiert werden können. „Bei der Behebung von Schwachstellen gibt es einige grundlegende Wahrheiten. Erstens gibt es zu viele Schwachstellen, um sie alle sofort zu beheben. Frühere Untersuchungen haben gezeigt, dass Unternehmen in der Lage sind, zwischen 5 und 20 % der bekannten Schwachstellen pro Monat zu beheben. Zweitens wird nur eine kleine Teilmenge (2 bis 7 %) der veröffentlichten Schwachstellen jemals in freier Wildbahn ausgenutzt. Aus diesen Tatsachen ergibt sich sowohl die Notwendigkeit als auch die Rechtfertigung für gute Priorisierungstechniken, da Unternehmen nicht alles sofort beheben können und auch nicht müssen“ (FIRST, o. J. b (eigene Übersetzung)).

So kombiniert die EPSS-Methodik die Vulnerabilitätsinformationen aus der CVSS-Methodik. Das Sammeln dieser Informationen kann die Priorisierung von Schwachstellen verbessern, indem die Wahrscheinlichkeiten bewertet werden, die eine belastbare Aussage über „die tatsächliche Ausnutzung von Schwachstellen in freier Wildbahn [machen]“ (FIRST, o. J. b (eigene Übersetzung)). Das Berechnungsmodell gibt eine Zahl zwischen 0 und 1 (0 % und 100 %) (vgl. FIRST, o. J. b).

Wird der globale CVSS-Base-Score (Schweregrad des Ausfalls) mit dem dazugehörigen EPSS-Score (tatsächliche Eintrittswahrscheinlichkeit) kombiniert, so resultiert eine *globale* Bewertung, die die beiden klassischen Bewertungsparameter aus dem Risikomanagement berücksichtigt. Derzeit existiert jedoch kein adäquates Modell bzw. Werkzeug, das zur praktischen und individuellen Kombination dieser zwei globalen Parameter eingesetzt werden kann. Vielmehr müssen einzelne Informationen über verteilte Webanwendungen gesammelt und zusammengeführt werden.

Neben den bisher dargestellten Ansätzen existieren auch weitere Konzepte aus der Spieltheorie, die sich in erster Linie auf den menschlichen Faktor konzentrieren, um dessen Entscheidungsfindung effektiver zu gestalten (vgl. Jalali et al., 2017, S. 82-88 | Gianini et al., 2015, S. 88-91). Zhu et al. (2019, S. 657-661) definieren ebenfalls einen spielbasierten Ansatz, wobei das CVSS als Grundlage dient. Es gibt auch ontologische Ansätze, die die Beziehungen zwischen Schwachstellen analysieren und auf ein breites Spektrum an Wissen zurückgreifen, um Angriffe zu verstehen und vermeiden zu können (vgl. Babar et al., 2019, S. 54-63 | Faria et al., 2019, o. S.)

Mundie et al. (2014) beschreiben die Notwendigkeit, ein Verfahren oder eine Ontologie für IRM zu entwickeln. Es gibt auch Ansätze, die sich mit der ganzheitlichen Betrachtung von VM und IRM befassen und verschiedene Faktoren auflisten, die neben der technischen Betrachtung ebenfalls eine relevante Rolle spielen (Betriebsumgebung: Physischer Perimeterschutz, Anbieter von Hard- und Software, etc.). Außerdem wird ein ontologisches Konzept beschrieben, das verschiedene Standards wie CVSS, CVE, Common Attack Pattern Enumeration and Classification, Common Weakness Enumeration (CWE), Common Platform Enumeration beinhaltet (vgl. DiMasse et al., 2020, S. 1-8 | Wang et al., 2009, S. 159-168 | Koza, 2023, S. 96).

Eine der wenigen praktischen Möglichkeiten, CVE individuell, also unternehmensspezifisch und im Kontext der technischen Basisinfrastrukturen ICS-spezifisch zu evaluieren, sind webbasierte Anwendungsdienste. Darunter zählen z.B. Kalkulatoren, die den Analysten z.B. über die NIST NVD-Website zur Verfügung gestellt werden. Hier haben Analysten die Möglichkeit, die zeit- und umgebungsbezogenen Metriken einer CVE individuell zu bestimmen und zu bewerten. Die angewandten Rechner ändern den CVE-Wert auf der Grundlage der ausgewählten spezifischen Unternehmenswerte, um die CVE individuell zu bewerten. Dieser Auswahlprozess ist jedoch intuitiv und subjektiv.

Die einzelnen Bewertungsstufen sind global definiert und lassen sich in der Regel nicht ohne weiteres auf die lokale Sicht eines ICS-Netzwerks beziehen. Des Weiteren existieren hier auch keine objektiven Parameter, Klassifizierungsstufen oder einheitliche Definitionen, die zu einer reproduzierbaren und belastbaren Bewertung führen würden. In der Folge können die Bewertungen von Analytiker zu Analytiker stark variieren.

Es besteht also die Gefahr, dass hier eine beliebige und subjektive Bewertung vorgenommen wird, die mitunter zu einer Verfälschung des Ergebnisses führen kann. Daraus folgt eine Erhöhung der Ineffizienz, da ein CVE für die weitere Behandlung ausgewählt werden kann, der als „False Positive“ (FP) definiert wird und daher hätte niemals ausgewählt werden dürfen. Außerdem werden die CVE ausschließlich nach dem Grad ihrer Verwundbarkeit bewertet, so dass die wichtigste Determinante „Wahrscheinlichkeit des Auftretens" nicht in dieser webbasierten Bewertung berücksichtigt wird. Außerdem erlauben solche Ansätze keine Dokumentation, sodass die Validierung, Revision und Reproduzierbarkeit des Prozesses ineffizient werden. Darüber hinaus beschreiben Pham und Dang (2018, S. 1296-1301) ein interaktives System, das Cybersicherheitsbedrohungen visualisiert. Darauf aufbauend kann eine Berichterstattung und Alarmierung in einer Organisation erfolgen. Allerdings dient dieses System nur als Hilfsmittel für eine transparentere und bessere Erkennung von CVE. Es dient also nicht explizit als Entscheidungshilfe, sondern erleichtert dem Benutzer den Überblick über relevante CVE zu erhalten.

Somit stellen CVE zunächst einmal eine sinnvolle Möglichkeit dar, die weltweit generierten Sicherheitslücken und Schwachstellen zu erkennen und die individuelle Bewertung und Behandlung der entdeckten CVE unverzüglich zu initialisieren.

Hierdurch können die Netzwerkanalytiker auf Basis ihrer spezifischen ICS-Umgebung und der eingesetzten Software- und Hardware eine zielführende Vorselektion treffen, indem sie zunächst ihre eingesetzten Soft- und Hardware-Komponenten sorgfältig ermitteln und festlegen. Als nächstes können nur die Schwachstellen in das Bewertungs- und Behandlungsprogramm eingebettet werden, die genau auf diese ausgewählten Systeme und ICS-Komponenten zutreffen.

An dieser Stelle benötigen sie nun ein effizientes Bewertungsmuster sowie effiziente Werkzeuge, welche eine schnelle, objektive und präzise Bewertung und Priorisierung erlauben. Wie eine Bewertungs- und Priorisierungsmethode zur Effizienzsteigerung der VM- und IRM-Prozesse führen kann, wird im nächsten Kapitel anhand einer deskriptiven Forschungshypothese definiert und als Forschungsgegenstand dieser Niederschrift näherbeschrieben.

3.3 Formulierung des Forschungsdefizites

Das Forschungsdefizit besteht darin, dass bisher keine systematischen und objektiven Bewertungs- und Priorisierungsmodelle existieren, die die notwendigen Entscheidungskriterien für ICS-spezifische CVE-Bewertungen identifizieren und quantifizieren.

Infolgedessen adressiert die identifizierte Forschungslücke die Kernthematik dieser Dissertation: Welche objektiven Entscheidungskriterien sind besonders relevant für die ICS-spezifische CVE-Bewertung? Und wie können diese Kriterien systematisch erfasst und durch ein entsprechendes Modell quantifiziert werden? Die Beseitigung dieser Forschungslücke kann dazu beitragen, die Effektivität und Praktikabilität von objektiven Entscheidungskriterien und dynamischen Entscheidungsmodellen zur ICS-spezifischen CVE-Bewertung zu verbessern und somit einen Beitrag zur Sicherheit industrieller Steuerungssysteme zu leisten.

4. Forschungshypothese und Forschungsmethodik

Abgeleitet aus den bisherigen Ausführungen gibt es einige theoretische und praktische Konzepte und Standards, die detailliert beschreiben, **was** im Sinne der Informationssicherheit, VM und IRM zur Erhöhung der Resilienz der ICS-Systeme zu tun ist. Die aufgeführten Standards können über mehrere, interdisziplinäre Bereiche hinweg zusammengestellt werden. Was jedoch insbesondere bei der Bewertung und Priorisierung von Schwachstellen und Sicherheitslücken, explizit CVE in Bezug auf die eigene spezifische ICS-Netzwerklandschaft unvollständig ist, ist der Mangel an effizienten und intelligenten Lösungsansätzen, die aufzeigen, **wie** die Anforderungen der Standards im Bereich des VM und IRM zu erfüllen sind. Diese Betrachtung gewinnt insbesondere dann an Relevanz, wenn die Cybersicherheitsingenieure und Netzwerkanalytiker in den Prozess- bzw. ICS-Netzwerken vor der Entscheidung stehen, welche der anfallenden Sicherheitsmeldungen und identifizierten Schwachstellen sofort oder zeitnah behandelt werden müssen, um ihre begrenzten personellen und fachlichen Kapazitäten effizient einzusetzen.

Hierbei geht es primär um die Aufrechterhaltung und Sicherstellung der Betriebsfähigkeit der Prozesse, also um die Aspekte der Resilienz-Erhöhung, Business Continuity und dem Umgang mit den Schwachstellen. Um diese Entscheidung nach Faktenlage validierbar, nachvollziehbar und instanziierbar treffen zu können, müssen die Entscheidungskriterien, Zusammenhänge und Dependenzen der einzelnen Kriterien untereinander sowie deren wechselseitige Auswirkungen in ein Metamodell integriert werden, um hieraus ein adaptives Entscheidungsmodell für die Bewertung und Priorisierung der globalen CVE in ICS-Netzwerken entwickeln zu können. Die grundlegende Zielsetzung dieses adaptiven Entscheidungsmodells ist es, den Fachanwendern die wesentlichen objektiven und systembezogenen Kriterien zur Kategorisierung der CVE nach der Kritikalität von Zeit, der Ausfallfolgen und des Aufwands in einem quantifizierbaren Modell zur Verfügung zu stellen, mit dessen Hilfe sie die anfallenden Sicherheitsmeldungen individuell bewerten und zur operativen Umsetzung initiieren können.

Dabei geht es im Kern darum, verfügbare externe CVE-Informationen zu filtern, diese in einen individuellen ICS-Kontext umzuwandeln, um in der Lage zu sein, die optimale Entscheidung schnell zu treffen, wobei auch berücksichtigt werden muss, dass Änderungen vorgenommen werden können, wenn mehr externe CVE-Informationen verfügbar sind. Daher benötigen die Anwender in den ICS-Netzwerken einen lösungsorientierten Ansatz, um ein Entscheidungsmodell zu generieren und operationalisieren zu können. Diese Kernanforderung beschäftigt sich daher mit der Aufgabestellung, wie die optimale Priorisierungs- und Bewertungsstrategie für die individuelle Bewertung, Priorisierung und Behebung von CVE operationalisiert werden kann.

So können Bewertungen unabhängig vom Entscheidungsträger (Faktor Mensch) und nach Faktenlage auf Grundlage der technischen und spezifischen Netzwerk- und Systemarchitekturen generiert werden.

So erfolgt die Entscheidung wie eine CVE individuell zu bewerten und priorisieren gilt auf Basis der systembezogenen Eigenschaften und Parameter und nicht gemäß der subjektiven Wahrnehmung des Entscheiders. Entsprechend der obigen Ausführung lässt sich die nachfolgende Forschungshypothese definieren, welche sich aus der praktischen Relevanz heraus in die gestaltungsorientierte deskriptive Forschung integrieren lässt:

Deskriptive Forschungshypothese:

Objektive Entscheidungskriterien zur ICS-spezifischen Bewertung und Priorisierung von CVE, welche quantifizierbar und instanziierbar in ein dynamisches Entscheidungsmodell eingebettet sind, sorgen für wirksame und effiziente Handlungsoptionen nach der Kritikalität von Zeit, der Ausfallfolgen und des erforderlichen Aufwands.

In Ermangelung effizienter Werkzeuge zur individuellen Bewertungs- und Priorisierungstechniken von Schwachstellen besteht nun das Ziel, ein instanziierbares Kohärenzmodell zur Bewertung und Priorisierung von CVE zu konzipieren. Als organisatorisches Rahmenwerk wird auf die hierfür modifizierte OODA-Schleife zurückgegriffen, um die einzelnen Prozesse und Verfahrensschritte des Kohärenzmodells systematisch operationalisieren zu können. Die konzeptualisierte OODA-Schleife konzentriert sich auf die Dynamik und Vielfalt von Cyberangriffen und soll nicht nur eine schnelle, sondern auch eine effiziente Gestaltung der Prozesse zur Entscheidungsfindung ermöglichen. Die operative Durchführung der einzelnen Forschungsarbeitsschritte und Forschungsphasen orientiert sich grundsätzlich an dem in der Praxis erprobten Design Science Research Zyklus-Modell, welches als Basismodell zur Klärung der gestaltungsorientierten Forschungsfragen in den Ingenieurswissenschaften eingesetzt wird, um die wissenschaftliche Tragfähigkeit durch die Verbindung der Relevanzebene mit der Rigorositätsebene sicherzustellen. Auf Grund der vorhandenen Komplexität der Forschungshypothese wird eine methodenpluralistische Vorgehensweise ausgewählt, um einen zielgerichteten Einsatz von geeigneten Methoden zur den einzelnen Forschungsleitlinien (FL 1 und FL 2) zu ermöglichen.

In diesem Zusammenhang wird im Gesamtkontext der Forschungshypothese neben der Integration des Design Science Research Zyklus zur Entwicklung des Kohärenzmodells, das Prototyping zur Operationalisierung des Metamodells und die Erfolgsevaluierung als weitere Methode zur Überprüfung der Machbarkeit und der Korrektheit des Kohärenzmodells eingesetzt. Um den wissenschaftlichen Denkprozess, der für die oben aufgeführte Hypothese sowie für die Erstellung eines Lösungsmodells notwendig ist, nachvollziehbar und transparent darzustellen, muss in einem ersten Schritt die Komplexität des Themas reduziert werden. Aus der Forschungshypothese lassen sich folgende Forschungsleitlinien ableiten:

Forschungsleitlinie 1 (FL 1):

„Wie können objektive Entscheidungskriterien (quantifizierbar und instanziierbar) als Entscheidungsmodell definiert werden, um das Ausmaß der zu bewertenden CVE nach der Kritikalität von Zeit, der Ausfallfolgen und des erforderlichen Aufwands zu bestimmen?“ (Koza, 2023, S. 97 (eigene Übersetzung)):

Forschungsleitlinie 2 (FL 2):

„Wie können die Erkenntnisse aus der OODA-Schleife als dynamischer Rahmen in IRET umgewandelt werden, sodass die Entscheidungsträger und Analysten ein adäquates Werkzeug zur Registrierung, Analyse, Bewertung und Dokumentation der CVE erhalten?“ (Koza, 2023, S. 97 (eigene Übersetzung)):

Basierend auf den Forschungsleitlinien wird ein Kohärenzmodell als eine adaptive und integrative Metamethode zur Bewertung und Priorisierung von CVE und Schwachstellen in ICS-Netzwerken erstellt. Das Kohärenzmodell integriert interne und externe komplementäre Determinanten in das Tool IRET. IRET integriert zu diesem Zweck ein mathematisches Berechnungsmodell, mit dem die CVE schnell und faktenbasiert bewertet und priorisiert werden können. Der Grundgedanke ist es, system- und netzwerkorientierte Determinanten zu identifizieren, die eine faktenbasierte Bewertung ermöglichen. Dies soll ermöglichen, den Bewertungsprozess objektiv und unabhängig von (subjektiven) Entscheidungsträgern und Analytikern durchzuführen. Damit kann die Möglichkeit geschaffen werden, die CVE nach objektiven Merkmalen (system- und netzwerkabhängige Merkmale) zu bewerten und die Ergebnisse jederzeit reproduzierbar zu gestalten. Eines der grundlegenden Aspekte ist also die Instanziierbarkeit des Kohärenzmodells. Das Kohärenzmodell ist in seiner Gesamtheit als ein Metamodell zur Bestimmung von CVE-Bewertungskriterien zu verstehen, welches unabhängig vom Anwendungsbereich operationalisiert und verwendet werden kann. Die praktische Machbarkeit des Kohärenzmodells wurde ein Jahr an einer international operierenden KRITIS im Energiesektor mit Kohleförderung, Stromerzeugung aus konventionellen sowie erneuerbaren Energiequellen sowie Stromverteilung in öffentlichen Hoch- und Mittelspannungsnetzen getestet. Die Entwicklung und die Evaluierung des Kohärenzmodells erfolgte im Rahmen eines industriellen Forschungsprojekts, in dem ein V-Modell-ähnliches Vorgehen ausgeführt wurde.

In dieser systematischen Vorgehensweise wurden fünf Entwicklungsphasen definiert. Angefangen bei der theoretischen Entwicklung bis hin zum Protoyping wurden sequenzielle Prozessschritte mit Teilevaluationsphasen bestimmt (Bild 18).

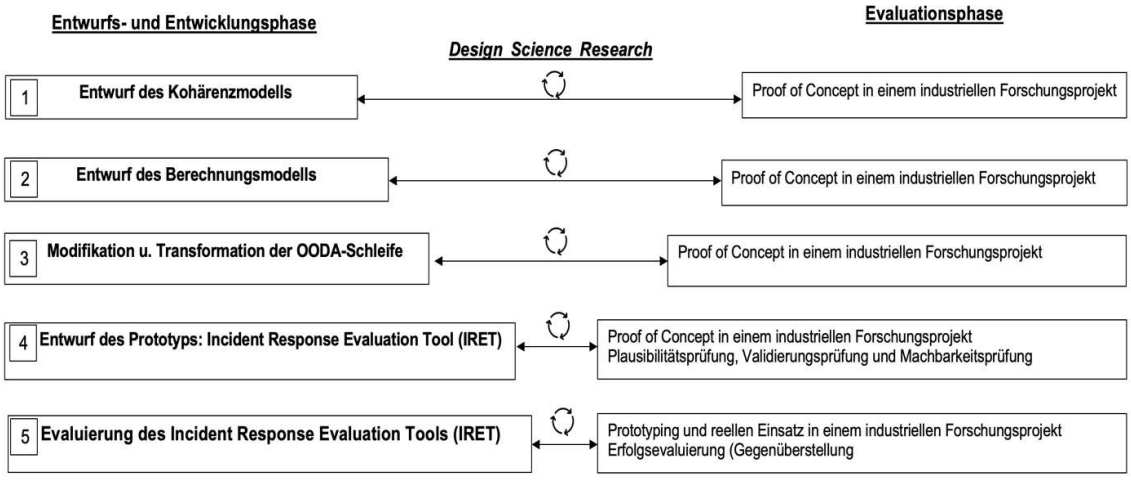


Bild 18: Forschungsphasen (Quelle: Eigene Darstellung)

Die Details zu den einzelnen Forschungsphasen kann anhand des nachfolgenden Bildes 19 „Forschungsdurchführungsplan“ illustriert werden. Darin wurden die einzelnen Forschungsphasen in insgesamt neun Iterationen unterteilt und operationalisiert.

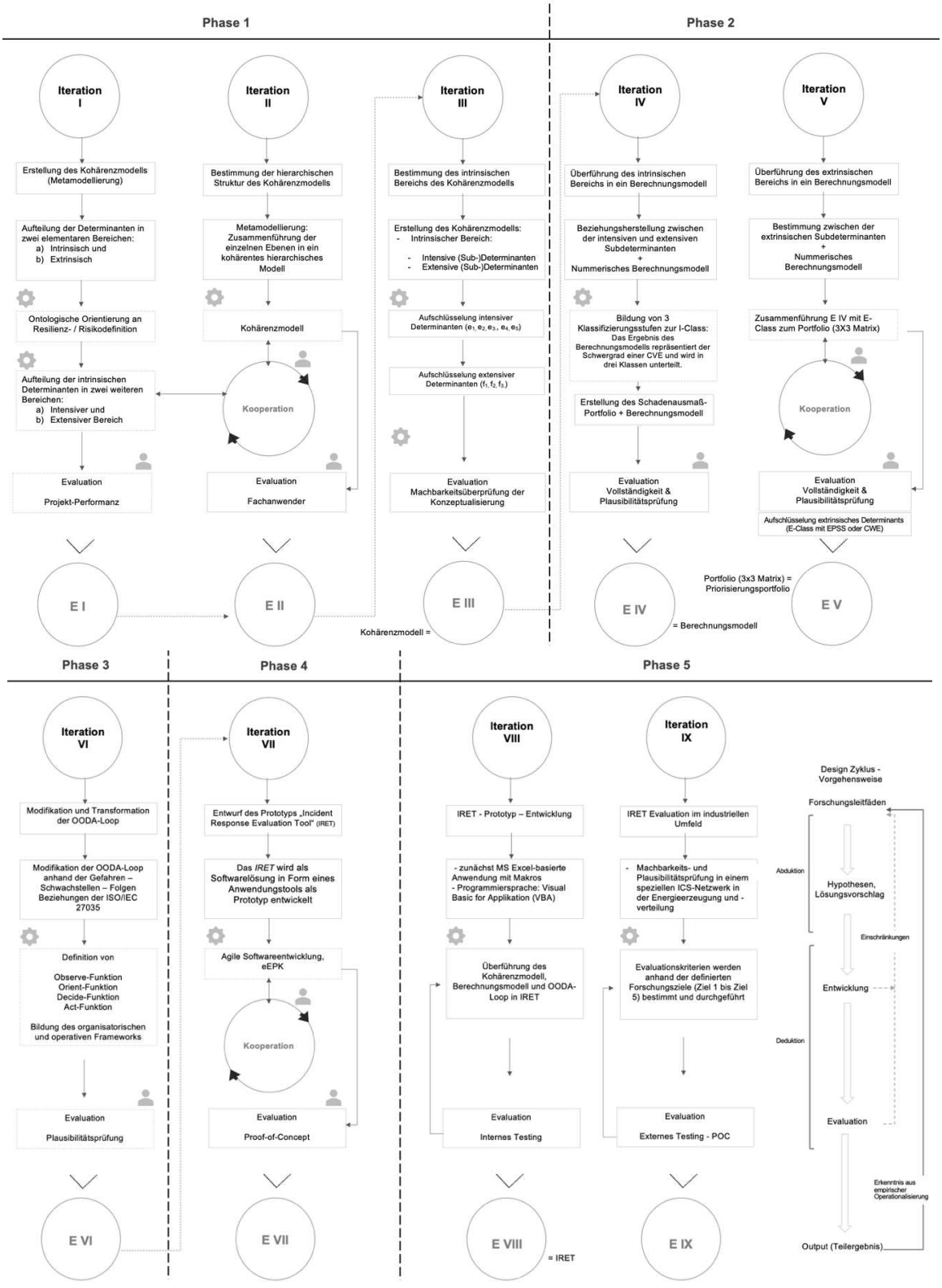


Bild 19: Forschungsdurchführungsplan (Quelle: Eigene Darstellung)

In der ersten Forschungsphase erfolgt mit jeweils drei Iterationen das grundsätzliche Design des Kohärenzmodells (Metamodell), indem die CVE-Bewertungsparameter anhand von übergeordneten Determinanten und den jeweiligen Subdeterminanten konzeptualisiert werden. In der zweiten Phase wird das Kohärenzmodell zwecks nummerischer Quantifizierung in ein Berechnungsmodell überführt, das später innerhalb der vierten Phase mithilfe eines software-basierten Lösungsansatzes auf Basis der Programmiersprache „Visual Basic for Application“ (VBA) realisiert wird. Um die Prozessschritte zur Registrierung, Analyse, Bewertung, Behandlung und Dokumentation einer CVE in das Kohärenzmodell einbinden zu können, werden die dynamischen Phasen der OODA-Schleife für diese Nutzung mit Hilfe der Beziehungstypen aus der ISO/IEC 27035-1 modifiziert und ebenfalls in die Softwarelösung als operatives und organisatorisches Rahmenwerk eingebettet. In der dritten Phase wird der Schwerpunkt der Forschung vom Konzept der OODA-Schleife auf eine konkrete Lösung verlagert, um einen dynamischen Rahmen vorzuschlagen. Zu diesem Zweck besteht der Kern der Forschung darin, zu untersuchen, inwieweit die OODA-Schleife für die dynamische Beobachtung von CVE, für proaktives Handeln und eine effiziente Handlungsgeschwindigkeit geeignet ist. In der vierten Phase wird der Prototyp entworfen. In der letzten Phase des Forschungsplans wird die konzipierte Softwarelösung „IRET“ entwickelt und zur industriellen Nutzung freigegeben. In dieser Phase erfolgt auch zugleich die Evaluation des Artefaktes, in dem die Plausibilität, Machbarkeit und Effizienz des Kohärenzmodells und IRET für die praktische Nutzung im industriellen Umfeld getestet wird. Hierfür werden insgesamt fünf Ziele festgelegt, welche im Forschungsverlauf zu evaluieren sind. IRET soll in der Gesamtheit als ein operationelles und effizientes Werkzeug verstanden werden, das die Arbeit von Cybersicherheitsingenieuren und Netzwerkanalysten zur Aufnahme, Dokumentation, Analyse, Bewertung, Behandlung und Berichten von CVE vereinfacht. So kann des Forschungsfeld innerhalb einer einfachen Modellierung zwischen der Aufnahme einer CVE (CVE-Eingang) und dem Schließen einer CVE (Dokumentation) visualisiert und definiert werden (Bild 20). Genau hier soll das Kohärenzmodell mit der dazugehörigen Softwarelösung „IRET“ zum Einsatz kommen und gemäß der Zieldefinitionen evaluiert werden.

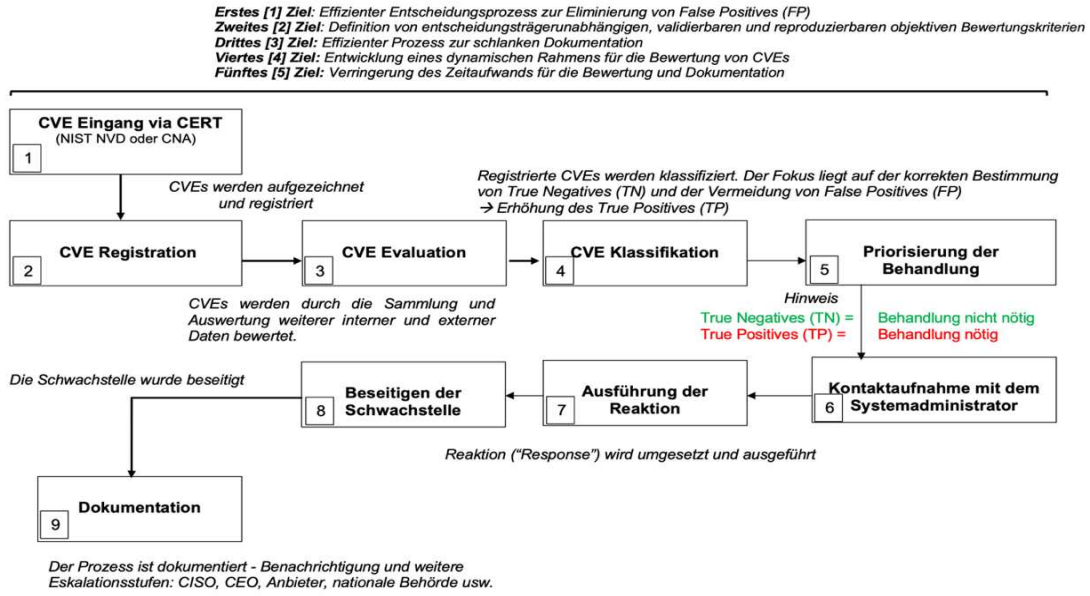


Bild 20: Forschungsfeld und die entsprechenden Detailziele (Quelle: Koza, 2023, S. 98 (eigene Übersetzung))

5. Forschungsergebnisse

Nachfolgend werden die Ergebnisse der einzelnen Forschungsphasen detailliert beschrieben. Die Darstellung der Forschungsergebnisse orientiert sich an den zuvor dargestellten Forschungsphasen.

5.1 Die Grundgedanken hinter dem Kohärenzmodell

ICS-Netzwerke beinhalten eine Vielzahl an unterschiedlichen Hard- und Softwaretechnologien, die bekanntermaßen zur Erhöhung der Effizienz und gleichzeitig aber auch der Fragilität führen können. Hierbei spielen Schwachstellen eine zentrale Rolle. Eine Schwachstelle repräsentiert einen sicherheitstechnischen Fehler in Soft- und Hardware-Komponenten. Ursächlich kann das Vorhandensein einer Schwachstelle in Hard- und Softwaretechnologien auf unterschiedliche Gründe zurückgeführt werden. So verweisen Anderson und Moore (2006, S. 6) in: „The Economics of Information Security“ auf marktwirtschaftliche Mechanismen, die im Wesentlichen mit der Monetarisierung der ICS-Produkte in Verbindung stehen. Sicherheitstechnische Implementierungs- und Prüfmechanismen in den Entwicklungs- und Testphasen der ICS-Produkte führen unmittelbar zu einer Verteuerung der ICS-Komponenten, wobei die Abnehmer auf der anderen Seite nicht dazu bereit sind diese höheren anfallenden Anschaffungskosten zu tragen. In der Schlussfolgerung ergibt sich also die Sichtweise, dass die Betreiber als Abnehmer erst gar nicht nach der Sicherheit der ICS-Produkte, sondern lediglich nach der korrekten Funktionalität der ICS-Produkte fragen. Dieses Dilemma spielte zu Beginn der Entwicklung und der Nutzung der ICS-Komponenten eine Rolle, allerdings zeigt sich nicht zuletzt durch die steigende Angriffsintensivität und den damit verbundenen hohen Ausfall- und Wiederherstellungskosten, dass die ICS-Hersteller vermehrt hohe Anfragen bezüglich der Sicherheit ihrer Komponenten seitens der Abnehmer erhalten. So müssen sich die Hersteller, Lieferanten und Integratoren, insbesondere im Umfeld der Kritischen Infrastrukturen, intensiver mit der Frage der Sicherheit ihrer ICS-Komponenten beschäftigen. Während Anderson und Moore (2006, S. 7) und Koza (2021, S. 827) die Ursache in der mangelhaften Zahlungsbereitschaft der Betreiber bzw. Abnehmer sehen, moniert Luiijf (2014, S. 23 f.) die fehlende Lernbereitschaft der ICS-Hersteller, die von den entdeckten Fehlern nicht lernen. Die ursächlichen Zusammenhänge, warum eine nahezu unendliche Anzahl an Schwachstellen derzeit existiert, kann nach Belieben fortgeführt werden, wobei diese Fortführung dann nicht zur Verbesserung des Sicherheitsniveaus, sondern vielmehr zu einer Art Lähmung und Lethargie führt, die auch unter anderem unter dem Begriff „Cycle of Blame“ zusammengefasst werden kann (vgl. Wendzel, 2021, S. 320 f.). Unabhängig der Ursachenforschung und dessen Resultate, müssen die Betreiber, Hersteller, Integratoren aber auch Sicherheitsexperten sich mit der Frage beschäftigen, wie diese diffizile Sachlage wirksam bekämpft werden kann. Bezugnehmend auf die Deklaration des Begriffes „Schwachstelle“ muss allerdings erstmal erläutert werden, was eine Schwachstelle ist und zu welchen prozessualen Ausfällen und monetären Schäden derartige Schwachstellen führen können. Im Allgemeinen wird unter der Terminologie „Schwachstelle“ auch „Verwundbarkeit“ verstanden. „Eine *Verwundbarkeit* (engl. *Vulnerability*) ist eine Schwachstelle, die durch einen Angreifer zu seinem Vorteil und zum Nachteil des zu schützenden Systems werden kann“ (Wendzel, 2021, S. 90).

In der Schlussfolgerung stellt eine Verwundbarkeit eine Bedrohung (engl. Threat) dar, wenn diese über einen bestimmten Angriffsvektor oder durch eine Angriffsmethode ausgenutzt werden kann. Eine Sicherheitslücke in einer ICS-Software, bedingt durch einen Fehler im Quellcode dieser Software, kann folglich ausgenutzt werden, in dem der Angreifer diese Verwundbarkeit gezielt über das Medium Internet mit einem hierfür entwickelten Code und entsprechenden Tools zu seinem Vorteil nutzt, um z.B. die Vertraulichkeit, Integrität oder die Verfügbarkeit der ICS-Software zu verletzen. Selbst wenn die ICS-Software in einer isolierten Umgebung ohne Zugang zum Internet aufgesetzt wird, so kann ein Innentäter weiterhin (engl. Insider Threat) die Ausnutzung dieser ICS-Software mit entsprechenden Mitteln hinter der eingesetzten Firewall vollziehen. In diesen Konstellationen existieren grundsätzlich zwei Arten von Angriffen: Die, die als netzwerkbasierter Angriffsvektor vor der Firewall über das Medium Internet ausgeführt werden und die, die als Insider Threats hinter der Firewall erfolgen können. Aufgrund der aufgeführten Logik werden in diesem Zusammenhang die beiden Begriffe „Schwachstelle“ und „Verwundbarkeit“ synonym verwendet. Die Betrachtung der Folgen einer Sicherheitslücke, in diesem und weiterem Kontext einer Schwachstelle, ist nicht abstrakt. Jede eingesetzte Soft- und Hardwarekomponente gehört aus Relevanzgründen zu den sogenannten Werten (engl. Asset) einer Organisation. Jedes Asset *(A*) innerhalb des sogenannten Informationsverbundes besitzt unausweichlich technische oder auch organisatorische Schwachstellen oder Verwundbarkeiten *(V*), die wiederum durch Bedrohungen *(B*) gefährdet werden, was in Folge zu einem Risiko (*R*) führt (Bild 21) (vgl. Wendzel, 2021, S. 90).

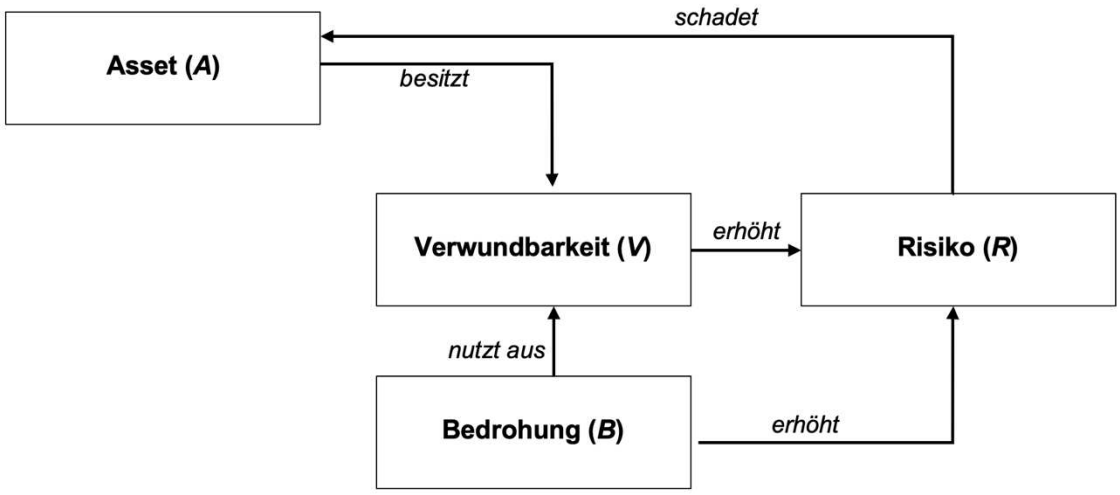


Bild 21: Beziehung zwischen Asset, Bedrohung, Verwundbarkeit und Risiko (Quelle: In Anlehnung an Wendzel, 2021, S. 90)

Durch diese Beziehung können einem Asset, die dazugehörige Verwundbarkeit und daraus resultierenden Bedrohungen und Werte zugeordnet werden, um den eigentlichen Wert des Risikos berechnen zu können. So definieren Shepherd et al. (2017, S. 7 f.) in „An Exploratory Analysis of the Security Risks of the Internet of Things in Finance“ eine nummerische Formel, um den zu ermittelten Risikowert in einem Skalasystem von 1-13 darstellen zu können.

$$R_{Wert} = A_{Wert} + V_{Wert} + B_{Wert} - 2$$

Der Risikobegriff wird aus der ingenieurwissenschaftlichen Perspektive wie folgt definiert: „Eine durch Risiko beschriebene Situation ist weder als gewiss noch als ungewiss einzuordnen bzw. besitzt sowohl gewisse als auch ungewisse Elemente. Mit dieser Positionierung als operationalisierte Wahrscheinlichkeit wird der Versuch unternommen, Risiko als ein objektives Maß zu sehen. Mit dem Element der Ungewissheit wird jedoch auch eine Unsicherheit (unsafety) impliziert, die der subjektiven Sicherheit (safety), ausgelöst durch gewisse Elemente, gegenübersteht. Dadurch kommt es zu einer situativen Einschätzung, die stark von emotionalen Komponenten geprägt ist. Ein subjektives Risiko wird projiziert“ (Ibers/Hey, 2005, S. 8). Die mathematische Erfassung eines Risikos soll daher weitestgehend aus der logisch-ingenieurwissenschaftlichen Erfahrung eines Tatbestandes oder Ereignisses abgeleitet werden, in der eine Reproduzierbarkeit und Nachprüfbarkeit der erreichten Bewertungen jederzeit möglich ist. Die Ergebnisse müssen demzufolge aus einer objektiven und vom Beobachter losgelösten Bewertung sowie aus einer bestimmten validen Methodik auf Basis empirischer Statistiken oder vergleichbaren Werten generiert werden (vgl. Mock, 2003, S. 167-172).

Abgeleitet aus der obigen Definition lässt sich ein Risiko nicht ausschließlich auf Grundlage der Schwere der zu erwartenden Ausfallfolgen, sondern auch auf Basis seiner Eintrittswahrscheinlichkeit, mit der das erwartete Risiko eintreten kann, bemessen. Dadurch ist die obige Quantifizierungsformel nicht vollständig, da diese dem Beobachter die Bestimmungsgröße zur Ermittlung der Eintrittswahrscheinlichkeit eines Risikos beraubt. Wird dieser Gedankengang nun weiterverfolgt, kommt man zu den beiden Risikobestimmungsgrößen, die sich aus der mathematischen Funktion der Häufigkeit (engl. Frequency) (*F)* eines Risikos und dessen Schadensausmaßes (engl. Consequence) (*C*) definieren lassen. So kann auch das Maß für ein Risiko (*R*) als das Produkt aus der Eintrittswahrscheinlichkeit und Schadenshöhe bestimmt werden (vgl. Mock, 2003, S. 167):

$$R = f(F, C) \rightarrow R = F \times C.$$

Bei dieser Auslegung spielt der Faktor „Ungewissheit“ eine wichtige Rolle. Während die Schadenshöhe, bzw. die möglichen Ausfallfolgen eines Risikos weitestgehend durch subjektive Determinanten bestimmt werden können, greift die Bestimmungsgröße „Eintrittswahrscheinlichkeit“ auf einen Satz von empirischen Beobachtungen (teilweise auch subjektive personengebundene Erfahrungswerte) und Statistiken, die naturgemäß unvollständig sind. Die Unvollständigkeit korreliert gleichzeitig mit dem Attribut der Ungewissheit, die sich aus der eingeschränkten und unvollständigen Möglichkeit zur Beobachtung ergibt. Dieses Dilemma wird im späteren Verlauf anhand der Modifikation der OODA-Schleife näherbeschrieben. Gleichwohl erlauben jedoch empirische Beobachtungen und Statistiken eine sinnvolle Einschätzung von Wahrscheinlichkeiten. In der Summe stellt die Risikoanalyse ein Instrument dar, mit dem man die empirischen Erkenntnisse aus der Vergangenheit für Einschätzungen zu zukünftigen Ereignissen nutzen kann. Bezugnehmend auf die Aspekte der Informationssicherheit verlangt das heutige Verständnis zum sicheren Betrieb von ICS-Netzwerken ein systematisches Vorgehen, um mögliche Risiken zuverlässig zu identifizieren und im Sinne eines präventiven Vorgehens zu eliminieren oder auf ein tragbares Maß zu reduzieren, bevor Systemausfälle oder Verletzungen der Versorgungssicherheit verursacht werden.

Diese Sichtweise wird von der ISO/IEC 27005:2011, im Folgenden vereinfacht ISO/IEC 27005, ISO/DIS 31000:2018 und ISO/FDIS 31010:2019 adaptiert, um ein sicherheits- und informationstechnisches Risikomanagementverfahren zu definieren. Dabei umfasst das technische Risikomanagement der ISO/IEC 27005 sechs zyklische und iterative Verfahrensschritte (Bild 22) (ISO/IEC 27005, 2011, S. 5 f.):

Schritt 1: Kontext der Betrachtung etablieren
Schritt 2: Gefahrenpotenziale bzw. Risiken identifizieren
Schritt 3: Risiken anhand geeigneter Methoden analysieren
Schritt 4: Risiken individuell bewerten und evaluieren
Schritt 5: Risikobehandlung, (Reduzierung des Risikos)
Schritt 6: Übriggebliebenes Restrisiko akzeptieren

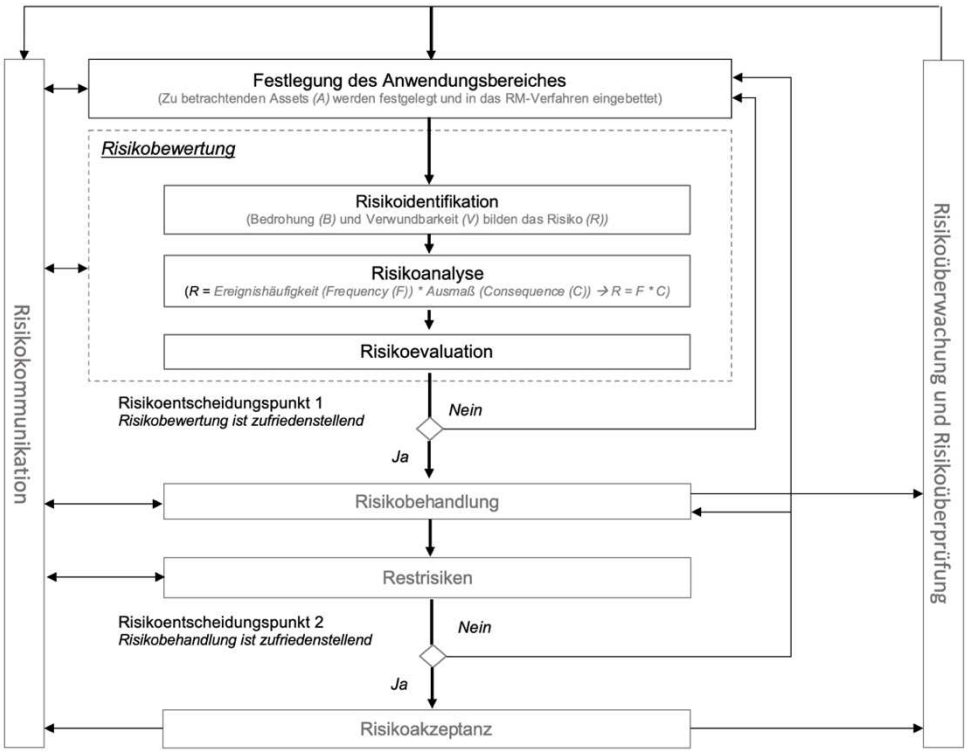


Bild 22: Risikomanagementprozesse für die Informationssicherheit (Quelle: In Anlehnung an ISO/IEC 27005, 2011, S. 8)

Die Risikobewertung wird als integrales Verfahren in das Risikomanagement eingebettet, mit dem festgestellt wird, in welchem Schadensausmaß die definierten Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) im Falle eines Schadensereignisses beeinträchtigt werden. Hierbei spielt die Definition und Festlegung einer Risikoakzeptanzgrenze bzw. eines Risikoakzeptanzwertes eine bedeutsame Rolle. Der Risikoakzeptanzwert stellt eine Art Toleranzgrenze dar, die für die Verteilung der Risikobewertungen innerhalb eines Risikoportfolios eingesetzt werden kann. Liegt ein Risiko sowie dessen Bewertung unterhalb dieser Grenze, wird dieses infolgedessen als ein akzeptables Risiko definiert.

Das akzeptable Risiko wird in diesem Zusammenhang als ein Risiko wahrgenommen, das auf Grund normativer Bestimmungskriterien als erlaubt bzw. zulässig definiert werden kann (vgl. ISO/IEC 27005, 2011, S. 24). Wird dieser Gedankengang auf die Notwendigkeit einer objektiven und reproduzierbaren Bewertungsmethodik für anfallende Schwachstellen und ihre Gefahren für ICS-Netzwerke transportiert, ergeben sich neue Möglichkeiten, um die weltweit generierten CVE in der Analogie zu der technischen Risikoanalyse bewerten zu können. Aus der sicherheitstechnischen Betrachtung her korreliert dieser Wunsch, CVE nach objektiven und reproduzierbaren Mitteln und Verfahren individuell bestimmen zu können und das unmittelbar mit dem Gedankengang der Resilienz-Erhöhung der ICS-Netzwerke.

Die Etymologie des Begriffs „Resilienz“ leitet sich vom lateinischen „resilire“ ab, und bedeutet zurückspringen oder abprallen (Baggio et al., 2015, o. S.) führen an, dass sich das Konzept resilienter Systeme auf den von Tredgold (1818, S. 216) definierten Resilienz-Begriff aus dem Jahr 1818 in den Ingenieurswissenschaften zurückverfolgen lässt, um die Belastbarkeit von Holz zu charakterisieren. Seither existieren unterschiedliche Definitionen. Laut der Definition der US-amerikanischen „National Research Council“ ist Resilienz „[…] die Fähigkeit, sich auf widrige Ereignisse vorzubereiten und zu planen, sie aufzufangen, sich von ihnen zu erholen und sich erfolgreicher an sie anzupassen“ (NAS, 2012, S. 16 (eigene Übersetzung)). Bürkner (2010, S. 24) führt weiterhin folgende Definition an: „‘Resilienz‘ bezeichnet entweder die Fähigkeit von Personen, sozialen Gruppen, Systemen oder Gegenständen, eingetretene Schädigungen zu kompensieren bzw. die verlorene Funktionalität wieder herzustellen, oder aber die Fähigkeit flexibel auf Gefährdungen zu reagieren und mögliche Schädigungen abzuwehren“.

Nach dieser Definition wird grundsätzlich zwischen zwei Varianten von Systemverhalten unterschieden: die Anpassungs- oder auch Veränderungsfähigkeit, welche die Fähigkeit eines Systems darstellt, nach einer vorübergehenden Störung in den Gleichgewichtszustand zurückzukehren (Flexibilität), und die Widerstandsfähigkeit, die die Fähigkeit eines Systems darstellt, Einwirkungen zu aufzunehmen, ohne dass sich der Systemzustand wesentlich ändert (Robustheit) (vgl. Bürkner, 2010, S. 24). Im Kontext der Kritischen Infrastrukturen definiert das NIAC (2009) drei wesentliche Resilienzmerkmale für KRITIS. Diese werden wie folgt beschrieben (NIAC, 2009, S. 16 (eigene Übersetzung)):

- „**Robustheit:** die Fähigkeit, kritische Operationen und Funktionen angesichts einer Krise aufrechtzuerhalten.

- **Reaktionsfähigkeit:** die Fähigkeit, sich geschickt auf eine Krise oder Störung vorzubereiten, darauf zu reagieren und sie zu bewältigen, während sie sich entfaltet.

- **Rapide Wiederherstellung:** die Fähigkeit, nach einer Störung so schnell und effizient wie möglich zum normalen Betrieb zurückzukehren und/oder diesen wiederherzustellen.“

Um die Resilienz aus systembezogener Sicht zu verstehen, ist es daher notwendig zu klären, aus welchem Fachgebiet die Beschreibungen der Systemeigenschaften und -verhalten stammen. Für die ICS-Netzwerke kommen daher zwei typische Auslegungen in Frage. Zum einen die Fähigkeit, sofort zu reagieren, um bestimmte Aufgaben unter vorhersehbaren äußeren Bedingungen zu erfüllen. Zum anderen die Anpassungsfähigkeit eines ICS-Netzwerkes, das von externen Veränderungen stark betroffen sein kann und ständig mit Unerwartetem konfrontiert wird.

Hinsichtlich des in dieser Niederschrift definierten Forschungsproblems kommt die zweite Ausführung zur Verwendung, da es sich hierbei um eine zielgerichtete Robustheit handelt, welche sich im Detail durch detektierende und präventive Maßnahmen zur Identifizierung, Bewertung, Priorisierung und Behandlung von CVE entfalten lässt. Im Kern geht es darum, die Standfestigkeit der ICS-Netzwerke durch Absorbierung von Schwachstellen zu garantieren, ohne dass sich die Qualität und Quantität der kritischen Dienstleistungen wesentlich ändern. Für ICS-Netzwerke kann die Resilienz allerdings als eine „Eigenschaft“ definiert werden, die sich durch „extrinsische“ und „intrinsische“ Aspekte konkretisieren lässt. Dabei existieren die extrinsischen Eigenschaften nur deshalb, weil ein System eine Beziehung zu seiner Umwelt besitzt. Auf die ICS-Netzwerke bezogen, kann die Wechselwirkung zwischen den ICS-Netzwerken und der Cyberumgebung im Allgemeinen oder aber auch der Cyberkriminalitätsumgebung herangezogen werden.

Intrinsische Eigenschaften hingegen umfassen die physischen oder die tatsächlich innewohnenden Aspekte eines Systems. Hinsichtlich der ICS-Netzwerke spielen also Merkmale wie Systemarchitektur, Anzahl der Redundanzen, Anzahl der Schnittstellen, Anzahl der logischen Sicherheitszonen etc. eine wichtige Rolle. So können derartige Aspekte als manifestierte Eigenschaften in Betracht gezogen werden. Folglich können die wesentlichen intrinsischen Attribute eines ICS-Netzwerks nicht entfernt werden, ohne dass das Netzwerk in seiner Gesamtheit erhalten bleibt. Werden die eingesetzten ICS-Netzwerkkomponenten wie Router oder Switche entfernt, so bleibt eine Reihe von verwertbaren Clients und Server übrig, die kein ICS-Netzwerk mehr darstellen. Werden diese Gedankengänge auf den Wunsch eines objektiven und reproduzierbaren Verfahrens zur individuellen und systembezogenen Bewertung und Priorisierung von CVE übertragen, so muss das Rad nicht neuerfunden werden.

Vielmehr lassen sich die erprobten Quantifizierungsmethoden aus dem Risikomanagement sowie die Erkenntnisse aus der Resilienzforschung auf die Forschungsproblematik übertragen, um ein Kohärenzmodell zu definieren, welches in der Lage ist, die anfallenden Sicherheitslücken in den ICS-Netzwerken anhand ihrer Eigenschaften zu bewerten und die entsprechenden zwei Bestimmungsgrößen Eintrittswahrscheinlichkeit und Schadensausmaß zu kategorisieren.

5.2 Vorstellung des Kohärenz- und Berechnungsmodells

Wird der oben aufgeführte Gedankengang weiterverfolgt, so können die Berechnungsmethodik aus der Risikoanalyse und die Resilienz als Systemeigenschaften auf die Aspekte der CVE-Bewertung und Priorisierung übertragen werden (1) und (2). Hieraus ergibt sich die folgende mathematische Formel, die zur Bewertung und Priorisierung einer CVE herangezogen werden kann (3) und (4) (vgl. Koza, 2023, S. 99):

$$\boldsymbol{R} = f(\boldsymbol{F}, \boldsymbol{C}) \rightarrow \boldsymbol{R} = \boldsymbol{F} \times \boldsymbol{C}. \quad (1)$$

$$\boldsymbol{R} = \boldsymbol{CVE} \text{ (Risiko wird durch eine CVE ersetzt)} \quad (2)$$

$$\boldsymbol{F} = \text{Extrinsic CVE factor (Häufigkeitsbestimmung ergibt sich aus dem extrinsischen CVE-Faktor)}$$

$$\boldsymbol{C} = \text{Intrinsic CVE factor (Schadensausmaßbestimmung ergibt sich aus dem intrinsischen CVE-Faktor)}$$

$$\rightarrow \boldsymbol{R} = \boldsymbol{CVE} = f(\boldsymbol{F} = \boldsymbol{Extrinsic\ CVE\ factor}, \boldsymbol{C} = \boldsymbol{Intrinsic\ CVE\ factor}). \quad (3)$$

$$\rightarrow \boldsymbol{CVE} = (\boldsymbol{Extrinsic\ CVE\ factor}) \times (\boldsymbol{Intrinsic\ CVE\ factor}). \quad (4)$$

Um die Bestimmung der einzelnen Faktoren objektiv und nach Faktenlage ermöglichen zu können, wird auf das Konstrukt eines Kohärenzmodells zurückgegriffen. Das übergeordnete, instanziierbare Kohärenzmodell repräsentiert das adaptive Bewertungsmodell, welches sich in Form einer Schablone auf jedes beliebige Konzept zur Bewertung und Priorisierung der CVE und der Handlungsoptionen übertragen lässt. Hierdurch erhalten die Fachanwender die Möglichkeit, das Kohärenzmodell individuell und zugeschnitten auf die einzelnen Prozesseigenschaften zu gestalten und ihr eigenes Bewertungsmodell mit differenzierten Schwerpunkten zu entwickeln. Um die Komplexität zu reduzieren und gleichzeitig die Flexibilität (Anpassbarkeit und Skalierbarkeit) des Kohärenzmodells zu ermöglichen, wird das Kohärenzmodell modular in zwei Metaebenen konzipiert (Bild 23).

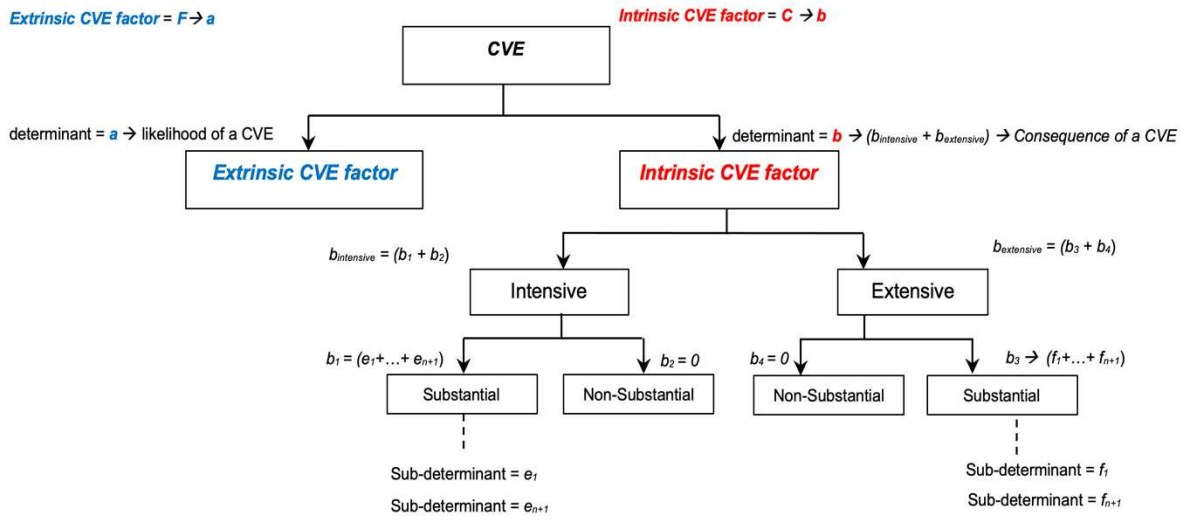


Bild 23: Kohärenzmodell (Quelle: In Anlehnung an Koza, 2022a, S. 2862 | Koza, 2023, S. 99)

Die erste Metaebene umfasst den „**intrinsischen CVE-Faktor**“ (intrinsischer CVE-Faktor **C** → (**b**) = ($b_{intensive}$ + $b_{extensive}$)) und lässt sich durch die internen System- und Netzwerkeigenschaften beschreiben. Das bedeutet, dass das jeweilig zu betrachtende ICS-System und die Netzwerkeigenschaften für die Determinierung der intrinsischen CVE-Faktoren herangezogen werden. Die zweite Metaebene (**F** → **a**) geht auf den „**extrinsischen CVE-Faktor**“ zurück, welcher außerhalb des Systems zu verorten ist und somit durch externe Einflüsse bestimmt werden kann. Die grundsätzliche Idee hierbei ist die Entwicklung eines Kohärenz- und Berechnungsmodells, das in der Lage ist, die globalen Informationen einer CVE mit den individuellen internen Informationen einer ICS-Netzwerklandschaft zu kombinieren, um eine individuelle Bewertung generieren zu können. Diese mathematische Vorgehensweise des Kohärenzmodells wird als „Berechnungsmodell“ bezeichnet, welches im späteren Verlauf mit einem konkreten Beispiel in der Tabelle 19 spezifiziert wird.

5.2.1 Die erste Metaebene des Kohärenzmodells (intrinsische CVE-Faktoren)

Der „**intrinsische CVE-Faktor**“ (erste Metaebene) bildet den ersten Betrachtungsbereich zur Bewertung des Schadensausmaßes einer CVE und umfasst in seiner Gesamtheit Determinanten (inklusive Subdeterminanten), welche für die interne und individuelle Bewertung des CVE-Schadensausmaßes herangezogen werden. Hierbei wird wiederum zwischen „**intensiven**“ (**$b_{intensive}$**) und „**extensiven**“ (**$b_{extensive}$**) Determinanten unterschieden. Während intensive Determinanten die Schadenstiefe einer CVE bewerten, bewerten die extensiven Determinanten den Schadensumfang einer CVE. Die erste Ebene des Modells beschreibt im Detail die Kriterien, die eingesetzt werden, um die anfallenden CVE-Sicherheitsmeldungen nach der Kritikalität der Ausfallfolgen (Business Impact) zu bewerten. Unabhängig der folgenden CVE-Informationsquellen:

- CVE-Sicherheitsmeldungen über eine zentrale CERT-Anbindung,
- CVE-Sicherheitsmeldungen, welche dediziert über Systemhersteller generiert und abgesetzt werden,
- CVE-Sicherheitsmeldungen, die durch das BSI abgesetzt werden und
- CVE-Sicherheitsmeldungen, die in den internationalen CVE-Datenbanken wie z.B. der NIST NVD gesammelt und publiziert werden,

können die intrinsischen Determinanten und Subdeterminanten individualisiert und spezifisch bestimmt und angewendet werden. Hierbei müssen die auserwählten Werte in die jeweiligen ***$b_{intensive}$*** - und ***$b_{extensive}$*** -Felder integriert und nach der Berechnungsformel quantifiziert werden (Bild 23). Beide Bereiche des intrinsischen Risikofaktors fußen auf die internen und objektiven Systemeigenschaften und Systemarchitektur, sodass sich diese als objektive Kriterien zur Bewertung des CVE-Schadensausmaßes eignen. Darüber hinaus existiert zwischen den beiden Bereichen eine wechselseitige Beziehung, die sich als Kohärenz zwischen ***$b_{intensive}$*** und ***$b_{extensive}$*** Subdeterminanten definieren lässt. Wichtig hierbei ist die Berücksichtigung der beiden intensiven und extensiven Bereiche, welche sich in mehrere unterschiedliche Subdeterminanten aufteilen lassen.

Der **„Non-Substantial“** stellt den Bereich dar, in dem die Wirkungstiefe oder der Wirkungsumfang einer CVE als vernachlässigbare Bestimmungsgröße definiert wird. Diese Bestimmungsgröße bezieht sich auf die System- und Netzwerkeigenschaften, die aus der sicherheitstechnischen Betrachtung keine Rolle für die Bestimmung des Schadensausmaßes spielen, jedoch für die mathematische Berechnung und zwecks der Vollständigkeit der Modellierung aufgeführt werden. Die „Non-Substantial“-Determinante wird mit dem Akronym $\boldsymbol{b_2}$ für den intensiven Bereich und $\mathbf{b_4}$ für den extensiven Bereich aufgeführt und jeweils dem Faktor 0 zugeordnet.

Der „**Substantial**“ Bereich stellt nach der vorliegenden Modellierungslogik den Bereich dar, der für die Bestimmung der Schadenshöhe einer CVE eine relevante Rolle spielt. Im Kohärenzmodell wird der intensive **Substantial**-Bereich mit dem Akronym $\boldsymbol{b_1}$ und der extensive Bereich mit dem Akronym $\boldsymbol{b_3}$ charakterisiert. Beide Substantial-Bereiche lassen sich durch eine Vielzahl an Subdeterminanten präzisieren und bestimmen (siehe auch Kap. 5.3). Hierbei lässt sich der Wert des intensiven Substantial-Bereiches durch die Addition seiner Subdeterminanten $\boldsymbol{(e_1 + ... + e_{n+1})}$ bestimmen. Diese Vorgehensweise wird auch in derselben Analogie für die Bestimmung des Wertes von extensiven Substantial-Bereichen ($\boldsymbol{f_1 + ... + f_{n+1}}$) genutzt (8). So lässt sich das Schadensausmaß einer CVE durch die Addition der Teilbestimmungsgrößen als intrinsische Subdeterminanten bestimmen (vgl. Koza, 2022a, S. 2864 | Koza, 2023, S. 100):

$$\text{CVE-Schadensausmaß} = \textit{intrinsischer CVE-Faktor} = C = (b_{extensive} + b_{intensive}) \tag{5}$$

$$C = (b_{extensive} + b_{intensive}) = ((b_1 + b_2) + (b_3 + b_4)) \rightarrow \tag{6}$$

$$C = \underbrace{((f_1 + ... + f_{n+1})}_{= b_3} \underbrace{+0)}_{= b_4} + \underbrace{((e_1 + ... + e_{n+1})}_{= b_1} \underbrace{+ 0)}_{= b_2} \rightarrow \tag{7}$$

$$C = ((f_1 + ... + f_{n+1}) + (e_1 + ... + e_{n+1})) \tag{8}$$

$(b_{intensive})$ wird der y-Achse zugeordnet:

$$\textit{Maximum value: } I_{max}\textit{: } ((|e_1, e_2, e_3, ...e_{n+1}|) \times 3) \tag{9}$$
$$\textit{Average value: } I_{mid}\textit{: } ((|e_1, e_2, e_3, ...e_{n+1}|) \times 2) \tag{10}$$
$$\textit{Minimum value: } I_{min}\textit{: } ((|e_1, e_2, e_3, ...e_{n+1}|) \times 1) \tag{11}$$

Wertebereich für die Klassifizierung der $(b_{intensive})$:

$$\textit{Critical} \rightarrow \textit{Class 3} \rightarrow I_{mid} < b_{intensive} \leq I_{max} \tag{12}$$
$$\textit{High} \rightarrow \textit{Class 2} \rightarrow I_{min} < b_{intensive} \leq I_{mid} \tag{13}$$
$$\textit{Low} \rightarrow \textit{Class 1} \rightarrow 0 < b_{intensive} \leq I_{min} \tag{14}$$

($b_{extensive}$) = wird x-Achse zugeordnet:

$$\text{Maximum value: } E_{max}: ((|f_1, f_2, f_3....f_{n+1}|) \times 3) \quad (15)$$
$$\text{Average value: } E_{mid}: ((|f_1, f_2, f_3....f_{n+1}|) \times 2) \quad (16)$$
$$\text{Minimum value: } E_{min}: ((|f_1, f_2, f_3....f_{n+1}|) \times 1) \quad (17)$$

Wertebereich für die Klassifizierung der ($b_{extensive}$):

$$\text{Critical} \rightarrow \text{Class 3} \rightarrow E_{mid} < b_{extensive} \leq E_{max} \quad (18)$$
$$\text{High} \rightarrow \text{Class 2} \rightarrow E_{min} < b_{extensive} \leq E_{mid} \quad (19)$$
$$\text{Low} \rightarrow \text{Class 1} \rightarrow 0 < b_{extensive} \leq E_{min} \quad (20)$$

Hieraus lassen sich folgende Zuordnungen der intensiven *($b_{intensive}$)* und extensiven *($b_{extensive}$)* Determinanten zu den jeweiligen Klassen definieren (Tabelle 4):

Tabelle 4: Grenzbereiche zur Klassifizierung des CVE-Schadensausmaßes (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 100 (eigene Übersetzung))

I-Class	Einstufung	Gesamtgrenzbereich	$b_{intensive}$ - Wertebereich	$b_{extensive}$ - Wertebereich
I-Class 1	**Low**	**[0, (E_{min} + I_{min})]**	$0 < b_{intensive} \leq I_{min}$	$0 < b_{extensive} \leq E_{min}$
I-Class 2	**High**	**[((E_{min} + I_{min}) +1), (E_{mid} + I_{mid})]**	$I_{min} < b_{intensive} \leq I_{mid}$	$E_{min} < b_{extensive} \leq E_{mid}$
I-Class 3	**Critical**	**[((E_{mid} + I_{mid}) +1), (E_{max} + I_{max})]**	$I_{mid} < b_{intensive} \leq I_{max}$	$E_{mid} < b_{extensive} \leq E_{max}$

So kann das folgende Klassifizierungsschema des (*C*)-Wertes in der ersten Metaebene definiert werden, um CVE hinsichtlich des Schadensausmaßes zu bewerten und zu klassifizieren. So kann dem $b_{intensive}$ - und $b_{extensive}$ -Wertebereich die definierte „*I-Class*“ mit folgender Wertung zugeordnet werden (Bild 24 und Tabelle 5) (vgl. Koza, 2022a, S. 2864 | Koza, 2023, S. 100):

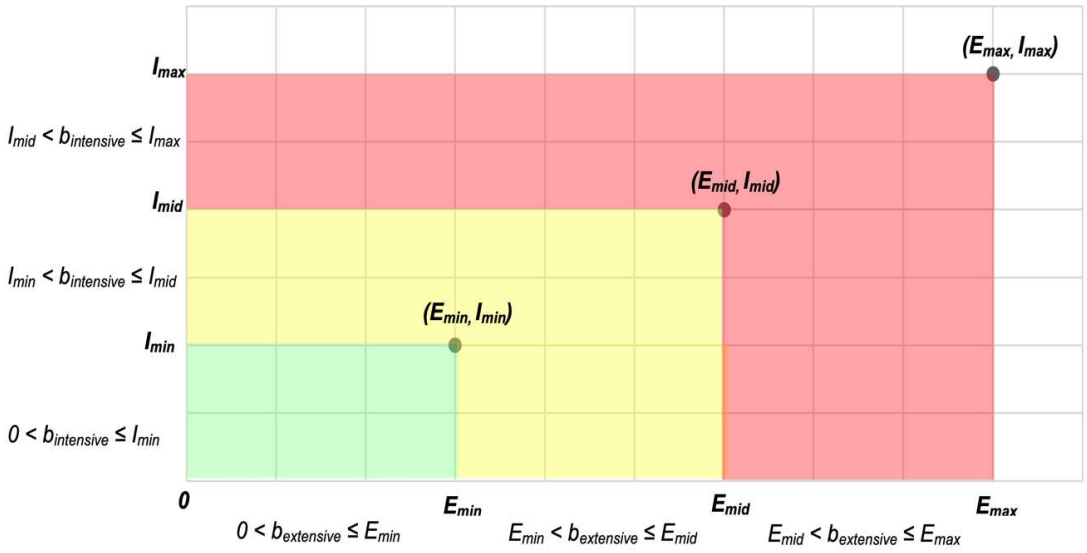


Bild 24: Klassifizierungsschema des (C)-Wertes der ersten Metaebene (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 101)

Tabelle 5: I-Classes und die Wertungen zur Einstufung des CVE-Schadensausmaßes (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 100 (eigene Übersetzung))

I-Class	Wertung	Einstufung	Gesamtgrenzbereich
I-Class 1	*1*	*Low*	$([0, (E_{min} + I_{min})]$
I-Class 2	*2*	*High*	$[((E_{min} + I_{min}) +1), (E_{mid} + I_{mid})]$
I-Class 3	*3*	*Critical*	$[((E_{mid} + I_{mid}) +1), (E_{max} + I_{max})]$

Die intensiven und extensiven Subdeterminanten lassen sich allerdings je nach Systemarchitektur und Netzwerkeinstellungen der Unternehmen anders definieren. Genau hier liegt der erste Vorteil des Kohärenzmodells. Das Kohärenzmodell stellt ein allgemeingültiges Modell dar, welches sich individuell auf die Struktur einer Netzwerklandschaft transportieren lässt. Der zweite Vorteil des Kohärenzmodells liegt in der zuvor beschriebenen wechselseitigen Beziehung, welche zwischen den Subdeterminanten und folglich auch in der Summe zwischen den beiden intrinsischen Bereichen existiert. So wird hier die Annahme getroffen, dass die Schadenstiefe einer CVE unmittelbar auch mit dem Schadensumfang einer CVE in Verbindung steht. Die Schlussfolgerung dieser Annahme stellt also die Möglichkeit dar, dass eine Aussage über den Schadensumfang auch eine Aussage über die Schadenstiefe zulässt (Bild 25). Wie lassen sich diese Zusammenhänge jedoch definieren? Hierfür müssen nun die allgemeinen und standardisierten informationstechnischen und kommunikationstechnischen Verfahren und Modelle genauer betrachtet werden, die im Wesentlichen als einheitliche Grundlage für die Gestaltung und Konzeption der Netzwerkkommunikation, Netzwerkarchitektur, Netzwerkplanung und Netzwerkkonfiguration in den Büro-, bzw. ICS-Netzwerken herangezogen werden können. Die nachfolgende Darlegung dient dem allgemeinen Verständnis, um die genannten kohärenten Beziehungen zwischen den intensiven und extensiven Subdeterminanten besser nachvollziehen zu können.

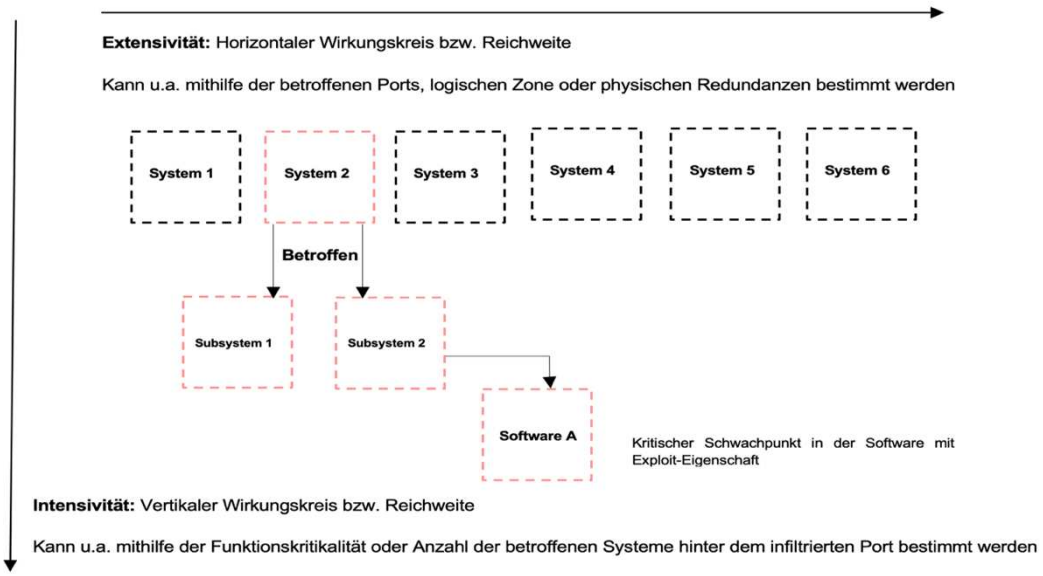


Bild 25: Beziehung zwischen den extensiven und intensiven Determinanten (Quelle: Eigene Darstellung)

Der Aufbau von (industriellen) Netzwerken ist trotz der einheitlichen Nutzung TCP/IP basierter Netzwerktechniken unterschiedlich geprägt. Daher können ICS-Netzwerke differenzierte Reichweiten aufweisen. In der Regel geht es hier um Computernetzwerke, die sich innerhalb eines lokalen Bereiches eines Unternehmens (engl. Local Area Network (LAN)) oder aber auch über sogenannte Wide Area Networks (WAN) über mehrere Standorte hinaus ausspannen lassen (vgl. Wendzel, 2021, S. 8 f.).

Bezugnehmend auf die ICS-Netzwerke können einige ICS-Komponenten innerhalb eines LANs und einige wiederum über WAN miteinander vernetzt werden. Zur Vernetzung der Computernetzwerke wird auf unterschiedliche Netzwerktopologien zugegriffen, die sich zwischen Punkt-zu-Punkt, Bus-, Stern-, Ring-, und Mesh-Topologien unterscheiden. Im Gegensatz zu einer monolithischen Netzwerkarchitektur mit einem einzigen Großrechner nutzen die heutigen ICS-Netzwerke die Vorteile einer Client-Server-Architektur. Hier greifen mehrere verteilte Clients auf eine zentrale Serverstruktur zu, welche wiederum in weitere verteilte und untereinander vernetzte Anwendungssysteme unterteilt werden. Somit kann die heutige Client-Server-Architektur zur Verwendung von Multiuser-Multitasking-Betriebssystemen eingesetzt werden (vgl. Wendzel, 2021, S. 8 f.).

Innerhalb der ICS-Netzwerke greifen die Clients gleichzeitig auf mehrere Server, darunter auf den Fileserver, SCADA-Server, Datenbank-Server, Web-Server, Mail-Server, Backup-Server etc. zu. Dabei lassen sich den Clients zur Verfügung gestellte Dienste und Applikationen dynamisch und schnell ausführen. Von der Rechnerkapazität und der Leistungsfähigkeit her, besitzen die Server eine höhere Rechner- und Speicherkapazität gegenüber den Client-Komponenten. So sind die Server auf Grund ihrer höheren Rechenleistung in der Lage, mehrere Clients gleichzeitig synchron und effizient zu bedienen, was in der Folge zu monetären Vorteilen führt, da hier eine Vielzahl an Clients auf eine wesentliche kleinere Anzahl an Servern zugreifen kann. Weitere wesentliche Vorteile hierbei sind die Datenaktualität, Datensynchronität, Datensparsamkeit, Systemskalierbarkeit und Energiesparsamkeit.

Werden aber die Serverstrukturen in der horizontalen Ebene, wie in Bild 25 dargestellt, jeweils nur einmal ausgelegt, so können diese als sogenannte Single Point of Failure (SPOF) definiert werden, da diese Komponenten keine Redundanzen und Backupsysteme besitzen, um Ausfälle zu kompensieren. Fällt der SCADA-Server aus, so können alle eingebetteten Applikationen und Dienste für alle an den SCADA-Server angeschlossenen Clients zusätzlich ausfallen. Durch die Betrachtung der eingesetzten Komponenten und deren Rückfallebenen kann ein objektives Kriterium abgeleitet werden, das eine Aussage über die Ausfallsicherheit eines ICS-Netzwerkes macht (vgl. Wendzel, 2021, S. 9).

Mit anderen Worten können die Redundanzkritikalität oder die eingesetzten Maßnahmen wie der Kumulations- oder Verteilungseffekt zu Lastverteilungen innerhalb der Netzwerkarchitektur eine Aussage darüber machen, wie die Ausfallsicherheit eines ICS-Netzwerks tatsächlich ist. In der logischen Schlussfolgerung ergibt sich ein objektives *extensives* Bewertungskriterium (R*edundanzkritikalität*), nach dem das intensive Kriterium (*Ausfallsicherheit)* der einzelnen Applikationen und Dienste im Sinne eines Ausfallgrades bzw. der Ausfallfolgenschätzung einer CVE bestimmt werden kann.

Neben der Art und der Anzahl der physischen Netzwerkkomponenten spielen auch Attribute zur Netzwerkkommunikation eine wesentliche Rolle. Die Datenübertragung innerhalb der ICS-Netzwerke findet in der Regel über Pakete und Frames statt, die sowohl Metadaten (Steuerinformationen) als auch die primären Nutzdaten beinhalten. Über die Metadaten werden die Kommunikationsregeln festgelegt, in denen bspw. die Eingänge (Paketempfänger), Ausgänge (Senderknoten) oder auch die Anzahl der primären Nutzdaten definiert werden (vgl. Wendzel, 2021, S. 12-16).

Während die Metadaten zur Realisierung und Gewährleistung der Datenübertragung eingesetzt werden und keine Relevanz für den Endanwender im ursprünglichen Sinne darstellen, stellen die primären Nutzdaten genau die Informationen dar, die von den Endanwendern zur Erledigung der betrieblichen Aufgabestellungen benötigt werden (vgl. Wendzel, 2021, S. 12-16). Um eine einheitliche und interoperable Kommunikation zwischen unterschiedlichen Computernetzwerken mit verschiedenen Betriebssystemen zu gewährleisten, werden Kommunikationsprotokolle eingesetzt. Wie bereits dargestellt greifen die heutigen ICS-Netzwerke in der Regel auf TCP/IP-Techniken zurück. Diese TCP/IP Protokollsuite interagieren in einer Open Systems Interconnection (OSI-) Referenzmodell ähnlichen Kommunikationsstruktur mit vier Schichten (Bild 26). Im Gegensatz zu den proprietären Netzwerken, die auch unter anderem als geschlossene Systeme bezeichnet werden, können nach TCP/IP oder de OSI-Referenzmodell implementierte Systeme auf Grund der einheitlichen und transparenten Protokolle als offene Systeme definiert werden, welche mit anderen Systemen offen kommunizieren können. Damit lässt sich eine Vielzahl an Systemen unabhängig ihres Betriebssystems wie Windows PC, Linux-Server oder auch eingebettete Systeme miteinander kompatibel vernetzen, auch wenn diese sich jeweils eine individuelle oder andere Netzwerktechnologie zu Nutze machen. Durch die Aufteilung der Kommunikationsstruktur in unterschiedliche Schichten (engl. Layer) kann die eigentliche Kommunikation pro Schicht erfolgen, ohne dass eine bestimmte Schicht für die gesamte Kommunikation verantwortlich ist. So kommuniziert jede Schicht mit ihrer logischen Schicht, die als Pendant gegenübersteht (Bild 26) (vgl. Wendzel, 2021, S. 12-16).

TCP/IP-Schicht	***TCP/IP – Modell***	***OSI-Modell***	***OSI-Schicht***
4	Application Layer *(Anwendungsschicht)*	Application Layer *(Anwendungsschicht)*	**7**
		Presentation Layer *(Präsentationsschicht)*	**6**
		Session Layer *(Sitzungsschicht)*	**5**
3	Transport Layer *(Transportschicht)*	Transport Layer *(Transportschicht)*	**4**
2	Internet Layer *(Vermittlungsschicht)*	Network Layer *(Vermittlungsschicht)*	**3**
1	Link Layer (*auch: Network Access Layer*) *(Netzwerkzugangsschicht)*	Data Link Layer *(Sicherungsschicht)*	**2**
		Physical Layer *(Bitübertragungsschicht)*	**1**

Bild 26: Vergleich der Schichten des OSI- und TCP/IP-Modells (Quelle: In Anlehnung an Wendzel, 2021, S. 12-16)

Hinsichtlich der Datenkommunikation in einem ICS-Netzwerk sind die TCP/IP-Schichten transparent, sodass die Systemoperatoren bspw. lediglich die benötigten Applikationen aufrufen müssen, um auf die von dem ICS-Netzwerk angebotenen Dienste zugreifen zu können. Dabei werden die einzelnen TCP/IP-Schichten voneinander eingekapselt. So schließt die „Network Access Layer“ die Daten von „Internet Layer“ in sich um, die ihrerseits die Daten der „Transport Layer“ einkapselt. Die Ebene der „Transport Layer“ schließt weiterhin die Daten von „Application Layer“, in der die eigentlichen primären Nutzdaten der jeweils aufgerufenen Applikation enthalten sind (Bild 27) (vgl. Wendzel, 2021, S. 14).

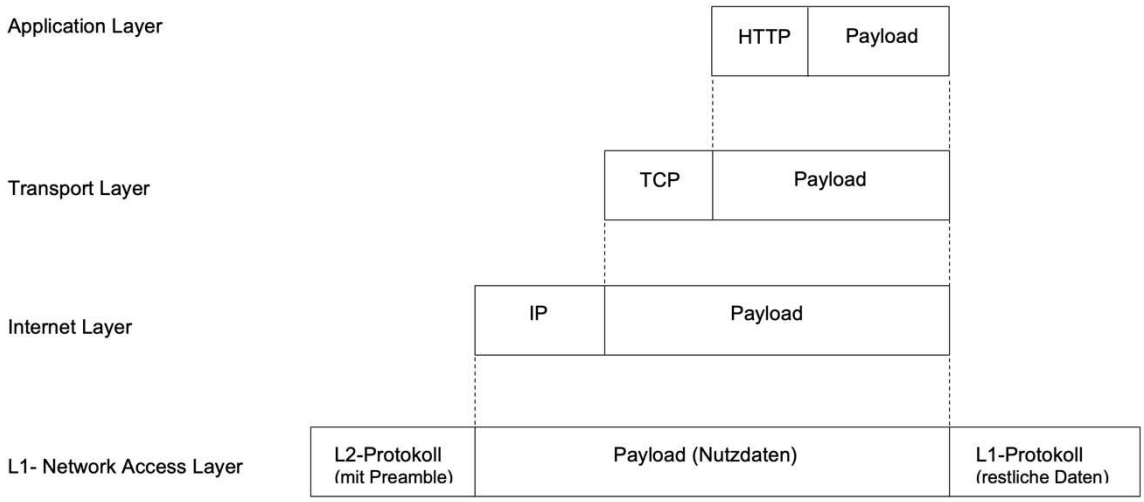


Bild 27: Einkapselung von Layern in TCP/IP am Beispiel eines http-Pakets (Quelle: Wendzel, 2021, S. 14)

Jeder beliebige Kommunikationspartner inklusive Rechner in einem ICS-Netzwerk besitzt zur Identifizierung eine eindeutige IP-Adresse, die über das sogenannte Routing von allen anderen Kommunikationspartnern erreicht werden kann. Das Routing-Prinzip sorgt in diesem Zusammenhang dafür, dass die anfallenden Anfragen über differenzierte Netzwerke ihren Weg zum Zielrechner finden. Hierfür werden Metadaten eingesetzt, die Informationen über diejenigen Router beinhalten, welche zum Zielnetzwerk führen sollen. So legen diese Metadaten fest, über welchen Weg bzw. Router die jeweilige Anfrage geschickt werden muss, um das gewünschte Ziel erreichen zu können. Für die Kommunikation mit dem gewünschten Ziel spielen aber auch die sogenannten „Ports“ eine entscheidende Rolle, die den Anwendungen jeweils zugeordnet werden. Hierdurch besitzt jede beliebige Verbindung zwischen den Netzwerkkommunikationspartnern bzw. Netzwerkteilnehmern auf der Applikationsebene, in diesem Fall zwischen dem Sender und dem Empfänger eines Datenpaketes innerhalb des ICS-Netzwerkes, jeweils zwei Ports. Der Quellport wird dem Sender zugeordnet und der Zielport dem Empfänger zugeordnet (vgl. Wendzel, 2021, S. 26-30). Mit Hilfe des sogenannten Multiplexings übernimmt die Transportschicht nun die Aufgabe, die Verbindung zwischen dem Sender und dem Empfänger eines Datenpaketes zu realisieren und die Datenpakete an die Anwendungsschicht weiterzuleiten. So nutzen Applikationen auf der Anwendungsschicht die ihnen zugeordneten Ports, in dem sie auf diese Ports zugreifen, um Datenpakete senden und empfangen zu können (vgl. Wendzel, 2021, S. 29). Anders ausgedrückt: Die implementierten Applikationen in den ICS-Netzwerken stellen auf einem Port genau einen Dienst zur Verfügung.

Aus der netzwerktechnischen Sicht spielen die Ports für die Realisierung der Netzwerkkommunikation und die damit verbundene Nutzung von Applikationen und Diensten eine wesentliche Rolle. So wie die Applikationen und Dienste auf die ihnen zugeteilten Ports zugreifen, um ihre Dienste zur Verfügung zu stellen, so greifen auch die netzwerkbasierten CVE auf diese Besonderheit zu, um ihre Schadsoftware in diese Systeme einschleusen zu können. Im Umkehrschluss werden die Schadsoftware portspezifisch kodiert. Das bedeutet, dass eine explizite netzwerkbasierte Schadsoftware, die eine Schwachstelle in einer bestimmten Software ausnutzen will, genau auf die Ausnutzung eines bestimmten Ports spezialisiert und kodiert werden muss. Der implementierte Quellcode der Schadsoftware kann nun auf dem der Anwendung zugeteilten Port ausgeführt werden, für den der Angreifer diesen speziellen Quellcode programmiert hat. Kennt der Angreifer die Anwendung und dessen standardisierten Port, weil bspw. die Netzwerkdienste einem expliziten und allgemein bekannten TCP-Port zugeordnet sind, so kann er bei Entdeckung einer Schwachstelle in diesem Netzwerkdienst aus dieser Information einen Angriffsvektor generieren, welcher die entdeckte Schwachstelle über exakt dem zugeordneten Port ausnutzen kann. Zur Verdeutlichung kann das folgende Beispiel herangezogen werden: Der TCP/IP-Port 455 wird bspw. als Netzwerkprotokoll zur Nutzung einiger Windows-Applikationen eingesetzt. Diese Informationen sind somit für jeden zugänglich und bekannt. Entdeckt ein Angreifer eine bestimmte Sicherheitslücke in diesen Windows-Applikationen, so kann er einen spezialisierten Code generieren, der den TCP/IP-Port 445 als Einfallstor zur Ausnutzung der entdeckten Schwachstellen nutzt, um alle in das Netzwerk eingebetteten Windows-Applikationen zu infiltrieren, wie z.B. die „WannaCry“ Schadsoftware mit der Ausnutzung des TCP-Ports 455. So konzentrieren sich viele Angreifer auf Sicherheitslücken von Softwareprodukten, die in die Netzwerklandschaften mehrfach integriert sind und gleichzeitig über einen einzigen Port ausgenutzt werden können.

Zusätzlich hierzu spielen auch die jeweiligen Konfigurationsprofile der Ports innerhalb der Netzwerkarchitektur eine wesentliche Rolle. Hierbei werden die Implementierungseigenschaften eines Ports herangezogen. Im Wesentlichen geht es darum, ob ein Port offen ist (ist der Port über das Medium Internet direkt erreichbar?), halboffen ist (der Port ist über das Medium Internet erreichbar, aber befindet sich logisch hinter einer Firewall, wo die Zugriffe authentisiert und autorisiert werden) oder geschlossen ist (der Port befindet sich in einem autarken isolierten Netzwerk, kann aber noch durch Insider Threats hinter der Firewall angegriffen werden). Bezugnehmend auf das obige Beispiel können die Netzwerkadministratoren bspw. die Nutzung des TCP/IP-Ports 455 gänzlich untersagen und somit den TCP/IP-Port 455 deaktivieren, sodass eine netzwerkbasierte Ausnutzung des TCP/IP-Ports 455 nicht mehr möglich ist.

Aus der obigen Betrachtung lassen sich objektive Bewertungskriterien ableiten, die im Ursprung auf die Porteigenschaften und netzwerkbasierte Schadsoftwareeigenschaften zurückgeführt werden können. Damit lässt sich anhand der jeweiligen extensiven netzwerkspezifischen *Portskritikalität* eine Aussage über die Angriffsdiversität bzw. Angriffsvielfalt und somit eine Aussage über ein intensives objektives Kriterium zum Beeinträchtigungsgrad einer Schadsoftware machen.

Ein weiteres objektives bzw. systembezogenes Kriterium lässt sich aus den Prinzipien der Netzwerksicherheit ableiten. Prinzipien der Netzwerksicherheit können u. a. auf die mehrseitige Sicherheit (engl. Multilateral Security) zurückgeführt werden. Diese Sichtweise impliziert eine mehrseitige Sicherheitsbetrachtung, in der die Sicherheitsanforderungen aller Netzwerkbeteiligten innerhalb eines ICS-Netzwerkes berücksichtigt werden müssen. Dem Purdue-Modell bzw. der Automatisierungspyramide zufolge, sind die ICS-Netzwerke mit den Büronetzwerken vernetzt und besitzen oftmals eine Vielzahl an internen und externen Schnittstellen. So werden unterschiedliche Systeme mit unterschiedlichen Aufgabenprofilen und den dazugehörigen Systemanwendern in einem übergeordneten Netz zusammengetragen. Diese offene Netzwerkkommunikationsstruktur stellt nach Rannenberg et al. (1996, S. 7-10) eine hinreichende Begründung dar, nicht allen Netzwerkteilnehmern per se vertrauen zu müssen. Computersysteme und damit auch die dazugehörigen Netzwerkteilnehmer interoperieren innerhalb eines soziotechnischen Umfeldes. Diese Sichtweise suggeriert die Integration und Verschmelzung von Systemanwendern (menschlicher Faktor) mit technischen Komponenten wie Computernetzwerken (technischer Faktor), wobei jede dieser Ebenen eine eigenständige Sicherheitsanforderung und ein Sicherheitsinteresse verfolgt. Hierzu führt Pfitzmann (2000, S. 17) an, dass die „[*m]ehrseitige Sicherheit* […] die Einbeziehung der Schutzinteressen *aller* Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte, etwa beim Entstehen einer Kommunikationsverbindung“ beschreibt. Diese Merkmale spiegeln sich in den sicherheitstechnischen Prinzipien wider, die aufgesetzt werden, um die einzelnen Ebenen und die daraus resultierenden Sicherheitsanforderungen berücksichtigen zu können.

Dieses Prinzip betrifft auch die automatisierte Kommunikation der Netzwerkkomponenten, sodass diese je nach definiertem Profil und Zweck einseitig, bilateral oder multilateral definiert und ausgeführt werden. Bezugnehmend auf die ICS-Netzwerksicherheit, werden Mechanismen eingesetzt, die den Zustand des ICS-Netzwerkes inklusive seiner Komponenten in der zuvor definierten Qualität und Quantität beschützen sollen. So werden restriktive Mechanismen eingesetzt, um das ICS-Netzwerk in unterschiedlichen Netzwerkzonen und Netzwerksegmenten zu unterteilen. Aus den Methoden der Softwarearchitektur existieren bereits Prinzipien, die den Softwareentwicklern und Systemarchitekten ermöglichen, separate Programmodule zu bilden und diese in weiten Teilen zur Minimierung von Abhängigkeiten (engl. Separation of Concerns) so zu implementieren, dass ein Ausfall eines Moduls keine weiteren Auswirkungen auf die anderen Module hat, sodass hier zum einen die Ausfallsicherheit der Module und zum anderen eine leichtere Lokalisierung und Problembehebung der Module gewährleistet ist. Neben dem Prinzip „Separation of Concerns“ existieren auch weitere Prinzipien, die jedoch aus anderen nicht mit der Informationstechnik verwandten Bereichen stammen. Die militärische Verteidigungsstrategie „Defense in Depth“ basiert auf den Grundsatz, den Angriffskrieg eines Invasors zu verlangsamen oder gar zu verzögern, anstatt den Angriff hauptsächlich zu vermeiden. Diese Strategie spielt vor allem dann eine relevante Rolle, wenn der Angriffskrieg nicht mehr vermeidbar ist. So setzt die Tiefenverteidigung auf mehrere Verteidigungslinien, anstelle einer einzigen Verteidigungslinie, um Zeit zu gewinnen und zusätzliche Verluste auf Seiten des Angreifers zu verursachen.

Sobald der Angreifer an Dynamik verloren hat oder taktisch gezwungen ist, sich auszubreiten, können defensive Gegenangriffe auf die Schwachpunkte des Angreifers geführt werden, mit dem Ziel, den Angreifer in seine ursprüngliche Ausgangsposition zurückzutreiben (vgl. BSI, 2021c, S. 6-9).

Die National Security Agency (o. J., o. S.) modifizierte diese militärische Strategie zu einem umfassenden Ansatz der Schichtungstaktik für Computernetzwerke. Die Idee hinter dem Security Defense-in-Depth-Ansatz in Computernetzwerken besteht darin, ein Netzwerk mit mehreren unabhängigen Schichten gegen unvermeidliche Angriffe zu verteidigen. Hierbei werden die Computernetzwerke ähnlich wie aus der gleichnamigen militärischen Strategie in mehrere Sicherheitszonen und Segmenten unterteilt. Hier wird auch über sogenannte logische und physische Netzwerkzonen und -Segmentierungen gesprochen, um Verwundbarkeiten zu reduzieren, Bedrohungen einzudämmen und Auswirkungen eines erfolgreichen Angriffs zu minimieren. Bezogen auf das Purdue-Modell der ICS-Netzwerke werden die einzelnen Ebenen der Automatisierungspyramide im Sinne der Netztrennung in unterschiedliche Zonen aufgeteilt. Dabei gilt der Grundsatz, dass das ICS-Gesamtnetz mindestens in drei physische Zonen unterteilt werden muss (vgl. NSA, o. J., o. S.). Ein internes Netz, eine demilitarisierte Zone (DMZ) und ein Außennetz mit der direkten Anbindung zum Internet sowie weitere nicht vertrauenswürdige Netze. Zudem werden die zu konzipierenden Zonenübergänge durch entsprechende Firewall-Komponenten voneinander getrennt und abgesichert. Hierdurch ist es nun möglich, den gesamten Datenverkehr zu regulieren und zu überwachen. Dementsprechend können Regelwerke definiert werden, welche ausschließlich erlaubte, authentisierte und autorisierte Kommunikationen, erlauben (engl. Whitelisting). Zusätzlich hierzu wird eine P-A-P-Struktur (**P**aketfilter-**A**pplication-Level Gateway-**P**roxies) implementiert, um bspw. jede ein- und ausgehende Datenkommunikation zu filtern und zu kontrollieren. So muss ein externer Datenverkehr aus einem nichtvertrauenswürdigen Netz durch mindestens zweifache Kontrollinstanzen passieren, um überhaupt einen Zugang in das interne ICS-Netz oder Büronetz erhalten zu können. Neben den bereits definierten Netzwerkzonen erfolgt auch eine sogenannte Netzwerksegmentierung, indem das ICS-Netzwerk durch eine weitere Firewall-Instanz in mehreren weiteren Segmenten getrennt wird. Das Prinzip bleibt hierbei jedoch erhalten. Damit erfolgt die Umsetzung der Trennung nach dem Separation of Concerns aus der Softwarearchitektur, da das Büronetzwerk und ICS-Netzwerk grundsätzlich zwei unterschiedliche betriebliche Ziele verfolgen und dementsprechend auch unterschiedlichen Schutzbedarfsstufen zugeordnet werden können. Die Trennung von Netzsegmenten betrifft die interne Netzplanung und wird zur Segmentierung der internen Netzwerkzone eingesetzt. So werden die Netzdimensionen zur internen Netzwerksegmentierung nach den Schutzbedarfsstufen bestimmt (Bild 28). IT- und ICS-Systeme mit unterschiedlichem Schutzbedarf werden in unterschiedliche Netzsegmente integriert. So werden in der Regel (vgl. BSI, 2021c, S. 6-9):

- die physischen Serverstrukturen des Büro- und ICS-Netzwerks voneinander getrennt und in unterschiedliche räumliche Begebenheiten in unterschiedlichen Bauabschnitten unterteilt (Prävention gegen elementare Gefährdungen und höhere Gewalt),
- die Clients und Server innerhalb des internen Büro- und ICS-Netzwerkes in weitere unterschiedliche Netzsegmente unterteilt,
- die Server mit grundlegender Dienstbereitstellung für die IT-und ICS-Infrastruktur in dedizierten Segmenten platziert,

- Managementdienste zur Administration, Überwachung, zentralen Protokollierung, Authentisierung und Autorisierung ebenfalls in dedizierte Segmente unterteilt,
- ICS-Systeme mit unterschiedlichem Schutzbedarf in unterschiedlichen Segmenten unterteilt (z. B. Altsysteme, welche keinen ausreichenden präventiven und detektierenden Schutz wie Antivirus oder Sicherheitsupdates besitzen, werden in die letzte logische Sicherheitszone positioniert).

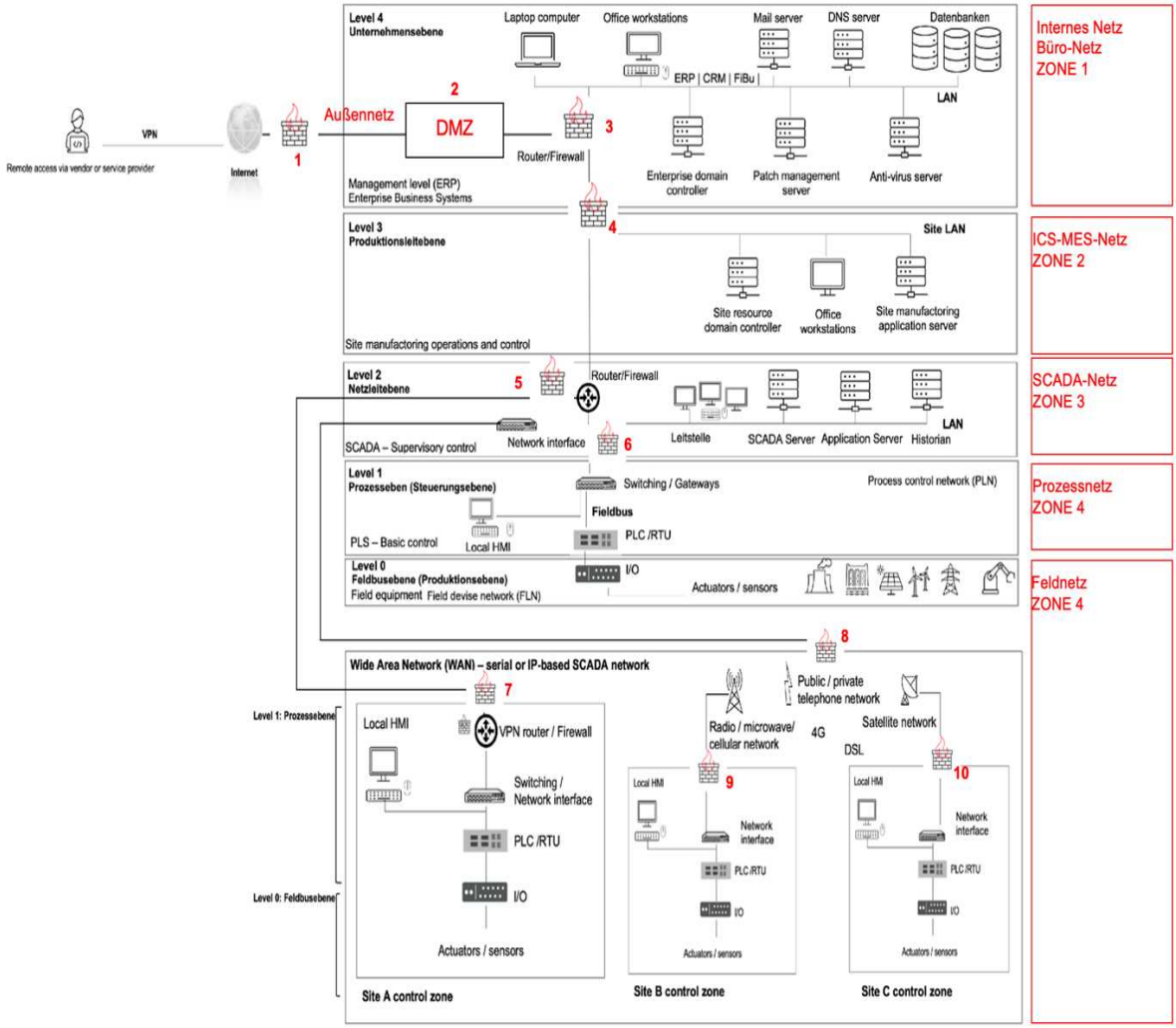


Bild 28: Grobes Zonenkonzept für ein ICS-Netzwerk (Quelle: Eigene Darstellung)

Der internen Netzplanung und der Netzwerkarchitektur zur Folge, kann der Auswirkungsbereich einer CVE einer Zone oder auch mehreren Zonen zugeordnet werden (Bild 28). Je nach spezifischer Netzwerkarchitektur verändert sich diese Kritikalität. Gleichwohl wie die Netzwerkarchitektur konzipiert ist, kann das Zonenkonzept eines ICS-Netzwerk als ein extensives Bewertungskriterium herangezogen werden, das gleichzeitig eine Aussage über die betroffene Funktionskritikalität als intensives Bewertungskriterium erlaubt. Diese Beziehung ergibt sich aus der Tatsache, dass die ICS-Netzwerke unterschiedlichen Aufgaben, Schutzbedarfsstufen und letztlich auch Zonen zugeordnet werden.

Auf Grundlage der bisherigen Darlegungen lassen sich systemabhängige, faktenbasierte und objektive Kriterien definieren, die zur CVE-Bewertung und -Priorisierung herangezogen werden können. Die erforderliche Präzisierung erfolgt in Kap. 5.3, wo die Gesamtheit der Subdeterminanten konkretisiert werden (vgl. BSI, 2021c, S. 6-9).

Nach Darstellung der ersten Metaebene zur Bewertung und Klassifizierung des CVE-Schadensausmaßes erfolgt im nächsten Kapitelabschnitt die Darstellung der zweiten Metaebene des Kohärenzmodells, die zur Integration der Eintrittswahrscheinlichkeit des extrinsischen CVE-Faktors (***F***) konzipiert ist. Bevor jedoch die zweite Metaebene des Kohärenzmodells vorgestellt wird, erfolgt eine konzise Einführung in die EPSS-Methodik, welche als Grundlage der zweiten Metaebene des Kohärenzmodells dient.

5.2.2 Die zweite Metaebene des Kohärenzmodells (extrinsische CVE-Faktoren)

Warum spielt der Gedankengang zur Angriffsvorhersage (engl. Attack Prediction) und Wahrscheinlichkeitsbetrachtung eine bedeutende Rolle für das Kohärenzmodell? Wie bereits eingangs dargelegt, stehen Betreiber technischer Basisinfrastrukturen in der Energie- und Wasserwirtschaft vor der Herausforderung, einen effizienten und wirksamen Vulnerabilitätsmanagementprozess zu etablieren, mit dem bekannte Schwachstellen identifiziert und behoben werden können. Da ICS-Netzwerke jedoch in der Regel mehr Schwachstellen als personelle und finanzielle Ressourcen für deren Behebung besitzen werden, müssen diese Netzwerke eine Bewertungs- und Priorisierungsstrategie anwenden, mit dessen Hilfe die Schwachstellen, die das größte Risiko darstellen, optimal priorisiert werden können, während gleichzeitig die Schwachstellen, die das geringste Risiko darstellen, zurückgedrängt bzw. depriorisiert werden.

Theoretisch versucht eine Organisation, zwei wetteifernde Dynamiken auszugleichen. Einerseits, alle in dem OT-Netzwerk identifizierten Schwachstellen zu beheben, was eine maximal mögliche „Abdeckung" zwischen den entdeckten Schwachstellen und den behobenen Schwachstellen bewirken würde. Diese ganzheitliche Strategie erfolgt unabhängig des Schadensausmaßes und der Eintrittswahrscheinlichkeit einer Schwachstelle. Gleichzeitig führt diese Strategie jedoch zu einem ineffizienten Ressourceneinsatz, da hierbei auch Ressourcen für die Behebung von Schwachstellen verbraucht werden, die ein geringeres Risiko darstellen. Andererseits könnten Organisationen nur eine geringe Anzahl von Schwachstellen mit hohem Schadensausmaß und/oder hoher Eintrittswahrscheinlichkeit beheben. Diese selektive Strategie ist zwar effizient, verbirgt aber auch die Gefahr eine signifikante Anzahl an anderen potenziellen und risikoreichen Schwachstellen offenzulassen. In der Praxis tun sich die meisten technischen Basisinfrastrukturen im Umgang mit Schwachstellen schwer und verwenden daher heuristische Strategien, um die anfallenden Schwachstellen, d. h. CVE zu identifizieren und zu beheben. Eine gängige Vorgehensweise besteht z.B. darin, alle Schwachstellen lediglich nach ihrem erreichten Schadensausmaß zu beheben (vgl. Jacobs et al., 2020, S. 1).

Dennoch zeigt sich, dass diese heuristischen Strategien ungünstig sind und nicht unbedingt besser sind als die beliebige Selektion von zu beseitigenden Schwachstellen (vgl. Dey et al., 2015, S. 462-477 | Allodi/Massacci, 2014, S. 1-20).

Einer der Gründe liegt darin, dass die Betreiber technischer Basisinfrastrukturen nicht in der Lage sind effektiv zu beurteilen, ob eine bestimmte CVE eine relevante Bedrohung für ihre ICS-Netzwerke darstellt. So zeigen frühere Forschungsarbeiten (siehe Kap. 3.2), dass von allen bekannten Schwachstellen nur für 10-15 % ein ausführbarer Quellcode vorhanden ist (vgl. Bozorgi et al., 2010, S. 105-113.).

So zeigen empirische Beobachtungen, dass in der Wirklichkeit nur ein geringer Anteil an Schwachstellen jemals in freier Wildbahn gegen die Organisationen eingesetzt wird. Sabottke et al. (2015, S. 1041-1056) stellen fest, dass nur für einen geringen Teil (1,4 %) der publizierten Schwachstellen eine Ausbeutung beobachtet wurde. Dadurch, dass nur eine marginale Anzahl an Schwachstellen tatsächlich im Fokus von Angreifern steht, besteht ein spezifischer Ansatz zur Beseitigung darin, die Bewertung und die Priorisierung der Schwachstellen so zu gestalten, dass nicht nur das Schadensausmaß einer Schwachstelle, sondern auch die Wahrscheinlichkeit in Verbindung mit dem Schadensausmaß als Bestimmungsgröße definiert wird, um die Anstrengungen der Betreiber technischer Basisinfrastrukturen primär auf die Behebung dieser Schwachstellen auszurichten (vgl. Jacobs et al., 2020, S. 1).

So nimmt die EPSS-Methodik diesen Gedanken auf und bettet die in der freien Wildbahn beobachteten Ausbeutungen als Anhaltspunkt für die Angriffsvorhersage ein. So werden Beobachtungen in Bezug auf exponierte Schwachstellen zur Kompromittierung eines Firmennetzwerks gesammelt und mit Hilfe von mathematischen Modellen zum Aufbau von Prognosemodellen entwickelt. Durch das Sammeln von Informationen über Schwachstellen (CVE) mit Beweisen für die eigentliche Ausnutzung der Schwachstellen und Analysieren dieser Daten versucht EPSS, die Priorisierung von Schwachstellen zu verbessern, indem es die Wahrscheinlichkeit abschätzt, wie eine Schwachstelle ausgenutzt wird. Das EPSS-Modell liefert einen Wahrscheinlichkeitswert zwischen 0 und 1 (0 % und 100 %). Je höher der Wert, desto größer ist die Möglichkeit, dass eine Schwachstelle (innerhalb von 30 Tagen) exploitiert wird (vgl. FIRST, o. J. b). Um das Ziel des EPSS-Modells zu erörtern, müssen also zwei grundlegende Fragen bzw. Attribute beantwortet werden:

a) Sollte die Schwachstelle beseitigt werden?
b) Würde die Schwachstelle in der freien Wildbahn ausgenutzt werden, und wenn ja, wie stark?

Die Antwort auf diese beiden Fragen ermöglicht die Definition von insgesamt vier Kategorien. Diese lassen sich anhand von Bild 29 visualisieren. Der große graue Kreis stellt in diesem Zusammenhang alle weltweit veröffentlichten CVE dar. Zur Veranschaulichung dieser vier Kategorien, wird angenommen, dass ein Betreiber technischer Basisinfrastrukturen der Strategie verfolgt, alle CVE mit einer Wertung bzw. einem CVSS-Score von 7+ in seinen Vulnerabilitätsmanagementprozess einzubetten und diese zu beheben. So repräsentiert der blaue Kreis alle CVE mit einem CVSS-Score 7+. Als Vergleichswert werden auch die CVE in Betracht gezogen, die in der freien Wildbahn ausgenutzt worden sind. Diese CVE werden mit einem roten Kreis illustriert. Die vier Kategorien sind wie folgt zu definieren (vgl. FIRST, o. J. b):

Kategorie 1: True Positives (*TP*) repräsentieren die richtig priorisierten Sicherheitslücken bzw. CVE, die in freier Wildbahn ausgenutzt werden. Hierbei entsteht eine gemeinsame, jedoch marginale Überschneidung zwischen dem roten und blauen Kreis.

Kategorie 2: False Positives (*FP*) repräsentieren CVE, die vermeidlich durch die angewendete Strategie zur Behebung priorisiert wurden, obwohl diese in der freien Wildbahn nicht ausgenutzt werden. Diese Priorisierungsstrategie stellt im Kern eine potenzielle Verschwendung von Ressourcen dar und wird durch die Differenz zwischen dem blauen und roten Kreis innerhalb des blauen Kreises darstellt.

Kategorie 3: False Negatives (*FN*) stellen die CVE dar, die fälschlicherweise nicht zur Weiterbehandlung und Beseitigung eliminiert wurden, obwohl diese in der freien Wildbahn ausgenutzt werden. Diese sind die CVE im roten Kreis, die sich nicht mit den CVE im blauen Kreis überschneiden.

Kategorie 4*:* True Negative (*TN*) stehen für CVE, die richtig eliminiert wurden, da diese in der freien Wildbahn nicht ausgenutzt werden. Diese CVE befinden sich im äußeren grauen Kreis, die weder behoben noch in der freien Wildbahn ausgenutzt werden.

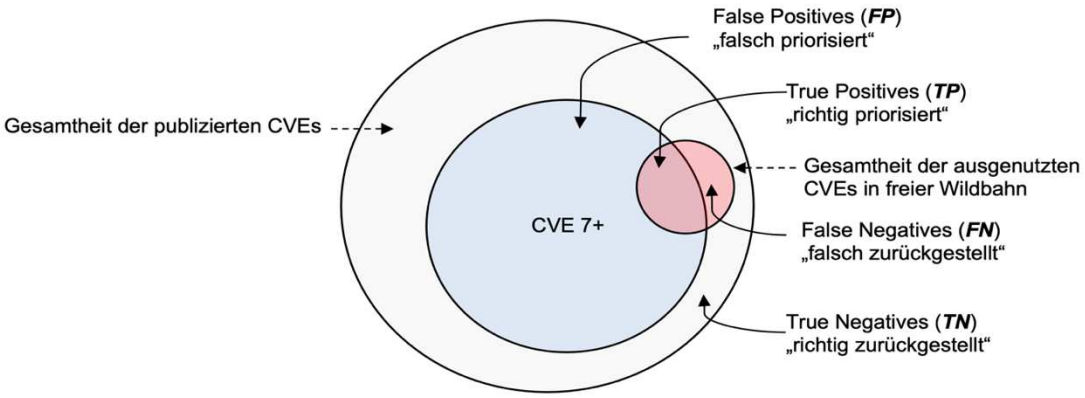


Bild 29: Vier CVE-Kategorien (Quelle: In Anlehnung an FIRST, o. J. b)

Wie im obigen Bild 29 dargestellt, führt die Strategie zur Behebung von Schwachstellen auf der Grundlage von CVE 7+ zu vielen FP (siehe Kategorie 2 (FP) im blauen Kreis) und lässt immer noch eine potenzielle Anzahl der ausgenutzten CVE offen (siehe Kategorie 3 (FN) im roten Kreis). Ableitend aus den oben aufgeführten vier Kategorien (*TP, FP, FN, TN*) lassen sich die zwei Metriken „Abdeckung“ und „Effizienz“ definieren. Der „Abdeckungsgrad“ und die „Effizienz" sind zwei gängige Bewertungskriterien, die in der Informationstheorie und bei Modellen des maschinellen Lernens (Klassifizierung) verwendet werden. In diesem Kontext misst der Abdeckungsgrad die Vollständigkeit der zu priorisierenden CVE. Wie viel Prozent aller Schwachstellen, die behoben werden sollten, wurden behoben? Wenn 100 Schwachstellen ausgenutzt werden, aber nur 15 behoben wurden, beträgt der Abdeckungsgrad dieser Priorisierungsstrategie 15%. Die Abdeckung wird mathematisch als *TP* geteilt durch die Summe der TP und FN dargestellt und ist maximal, wenn die *FN*-Anzahl gegen null tendiert *(TP / (TP + FN)).*

Im obigen Bild 29 ist der Abdeckungsgrad der Anteil des roten Kreises, der durch die gemeinsame Schnittmenge mit dem blauen Kreis abgedeckt wird. Ein niedriger Abdeckungsgrad bedeutet demzufolge, dass nicht viele der ausgenutzten Schwachstellen mit der zuvor definierten Priorisierungsstrategie behoben wurden (vgl. Jacobs et al., 2020, S. 6).

Auf der anderen Seite misst die „Effizienz“ die Wirksamkeit der Beseitigungsmaßnahmen. Wie viel Prozent aller behobenen Schwachstellen hätten behoben werden sollen? Wenn zum Beispiel 100 Schwachstellen beseitigt, aber nur 15 jemals ausgenutzt werden, beträgt die Effizienz dieser Strategie 15 %. Die übrigen 85 % sind Ressourcen, die besser an anderer Stelle eingesetzt worden wären. Die Effizienz wird algebraisch dargestellt als *TP* geteilt durch die Summe der *TP* und *FP*, und wird maximiert, wenn die Anzahl der FP gegen Null tendiert *(TP / (TP + FP))* (vgl. Jacobs et al., 2020, S. 6).

So misst die Effizienz, wie zielorientiert und wirksam die Ressourcen zur Bekämpfung und Beseitigung der CVE eingesetzt werden. In der obigen Bild ist die Effizienz der Anteil des blauen Kreises, der durch den roten Kreis abgedeckt wird. Die ideale Strategie erreicht in diesem Zusammenhang einen 100-prozentigen Abdeckungsgrad und eine 100-prozentige Effizienz. Eine Strategie, die nur Schwachstellen mit hohem Schadensausmaß in den Vordergrund stellt, kann zwar eine gute Effizienz aufweisen, hat aber den Preis einer geringen Abdeckung, da viele Schwachstellen mit öffentlich zugänglichem Quellcode und Angriffstool-Kits ebenfalls einen niedrigen Schweregrad aufweisen können. Andersrum könnte der Abdeckungsgrad erhöht werden, indem mehr Schwachstellen mit niedrigerem Schadensausmaß behoben werden. Allerdings leidet hierbei die Effizienz, da bei dieser Strategie auch Schwachstellen behoben werden, deren Ausnutzung sehr unwahrscheinlich ist.

Das Verständnis für die Effizienz und für den Abdeckungsgrad ermöglicht es den verschiedenen technischen Basisinfrastrukturen, die Behebung von Schwachstellen je nach ihrer Risikotoleranz und ihren Ressourcenkapazitäten unterschiedlich anzugehen. Betreiber technischer Basisinfrastrukturen, welche nicht über viele Ressourcen verfügen, möchten vielleicht mehr Wert auf die Effizienz als auf die Abdeckung legen und versuchen mit den begrenzten Ressourcen die beste Wirkung zu erzielen. Für technische Basisinfrastrukturen, deren Ressourcenkapazitäten ausreichend ausgelegt sind und bei denen die ICS-Sicherheit für den Erfolg entscheidend ist, kann der Schwerpunkt auf einer hohen Abdeckung der Schwachstellen mit dem höchsten Risikowert liegen. Beide Zielsetzungen mit einem hohem Abdeckungsgrad sowie einer höheren Effizienz können besser ausgeführt bzw. erreicht werden, wenn sowohl das Schadensausmaß als auch die Eintrittswahrscheinlichkeit der CVE zur Bewertung und Priorisierung zur Entscheidungsfindung berücksichtigt werden. Die zweite Ebene des Kohärenzmodells soll hier eine Abhilfestrategie liefern. So bettet die zweite Metaebene des Kohärenzmodells den „**extrinsischen CVE-Faktors**“ (**F**) ein, welcher zur Bestimmung der Eintrittswahrscheinlichkeit einer CVE herangezogen wird. Die adäquate Betrachtung einer CVE erfolgt in einer Bivalenz. In einem einschließenden konjunktiven Format, indem sowohl das Schadensausmaß als auch die Eintrittswahrscheinlichkeit bewertet werden müssen. Für diese Betrachtung müssen sowohl die internen als auch die externen Einflüsse berücksichtigt werden, wie bspw. das tatsächliche Vorkommen und die Ausnutzung einer CVE in der freien Wildbahn.

Der „extrinsische CVE-Faktor“ wird in dieser Konstellation über die zuvor vorgestellte EPSS-Methode oder die Ausnutzungswahrscheinlichkeit in CWE (engl. Probability of Exploit) bestimmt und in die zweite Ebene des Kohärenzmodell eingebettet. Die Häufigkeit und Prävalenz der Ausnutzung einer CVE macht also eine Aussage darüber, ob und inwieweit eine CVE als TP bzw. als FN im Sinne einer Wahrscheinlichkeitsbetrachtung definiert werden kann. Hierdurch bekommen die Analytiker die Möglichkeit, eine CVE nicht nur isoliert nach den Ausfallfolgeschäden, sondern auch in Kombination mit der realistischen Eintrittswahrscheinlichkeit der CVE zu bewerten und zu klassifizieren. Die Erwartung liegt hier in der Prämisse, dass eine derartige Bewertungsmethodik mitunter zur Eliminierung oder Reduzierung von FPs führt. Infolgedessen lässt sich dann auch der ineffiziente Einsatz von Personalressourcen vermeiden.

Um diese Überlegung rechnerisch und methodisch zu definieren, muss zunächst die Wahrscheinlichkeit des Auftretens einer CVE quantifiziert (**F**) und dann in der Analogie zur (C)-Wertung und -Klassifizierung in drei Kritikalitätsklassen unterteilt werden. Der Hintergrund hierfür ist, dass hierfür im späteren Verlauf die (C)-Klassifizierung und (**F**)-Klassifizierung zusammentragen werden, um diese in einem Portfoliomodell zwecks finaler CVE-Priorisierung zu visualisieren.

Das EPSS-Modell mit seinem EPSS-Score zur Darstellung der Wahrscheinlichkeit einer CVE oder der CWE-Score (Probability of Exploit) basieren auf eine empirische Datenerhebung der jeweiligen Organisation und geben einen Wahrscheinlichkeitswert an, wie häufig eine CVE in der freien Wildbahn ausgenutzt wird. Die Entscheidung darüber, die Wahrscheinlichkeit des Auftretens über diese *beiden unterschiedlichen* extrinsischen Angaben zu determinieren, hat einen pragmatischen Hintergrund. Im Allgemeinen können nicht alle CVE-Eintrittswahrscheinlichkeiten sofort mit dem EPSS-Modell quantifiziert werden. Da jedoch die CVE-Informationen aus der NIST NVD auf die entsprechende CWE-ID referenziert werden, kann die CWE-Eintrittswahrscheinlichkeit als redundante Methode zur Bestimmung der empirischen Eintrittswahrscheinlichkeit verwendet werden. Zu diesem Zweck werden der quantifizierte EPSS-Score [0-10] und der qualitative CWE-Score vereinheitlicht und anhand einer globalen Konvertierungstabelle zusammengetragen. Wenn bspw. die Wahrscheinlichkeit des Auftretens einer CVE über den EPSS-Score 0,4 (*0,4 x 100= 40%)* beträgt, ist die Wahrscheinlichkeit des Auftretens beim CWE-Score bei „mittel (M)". Die Konvertierungstabelle sowie die dazugehörigen Stufen können wie folgt definiert werden (Tabelle 6):

Tabelle 6: Metaklassifizierung der E-Classes (Quelle: In Anlehnung an Koza, 2022a, S. 2864)

E-Class	**Wertung**	**Einstufung**	**EPSS-Wertebereich**	**CWE-Wertebereich**
E-Class 1	**1**	**Low**	Quantitativ	Qualitativ
E-Class 2	**2**	**High**	Quantitativ	Qualitativ
E-Class 3	**3**	**Critical**	Quantitativ	Qualitativ

Nach der Darstellung der zwei Metaebenen des Kohärenzmodells werden im nächsten Kapitelabschnitt die beiden Metaebenen zusammengeführt, um die jeweilige Wertung nach dem Schadensausmaß und der Eintrittswahrscheinlichkeit in der Analogie zu einem Risikoportfolio in einer 3 x 3 Matrix zu visualisieren und nach einem standardisierten Verfahren zu bewerten und priorisieren.

5.2.3 Portfolio-Bildung aus den extrinsischen und intrinsischen CVE-Faktoren

Durch die Kombination der beiden extrinsischen und intrinsischen Klassen (intrinsische „*I-Class*“ aus der Tabelle 5 und extrinsische „*E-Class“* aus der Tabelle 6) und deren Bild in einem Portfoliomodell mit einer 3 x 3 Matrix können die CVE nun nach den beiden wichtigsten Kriterien (CVE-Schadensausmaß und CVE-Eintrittswahrscheinlichkeit) bewertet werden. Bild 30 stellt das Portfolio aus den beiden Klassen dar und zeigt die abschließende Bewertung und Klassifizierung der CVE, deren Veranschaulichung anhand von acht Determinanten in Kap. 5.3.6. näher beschrieben wird.

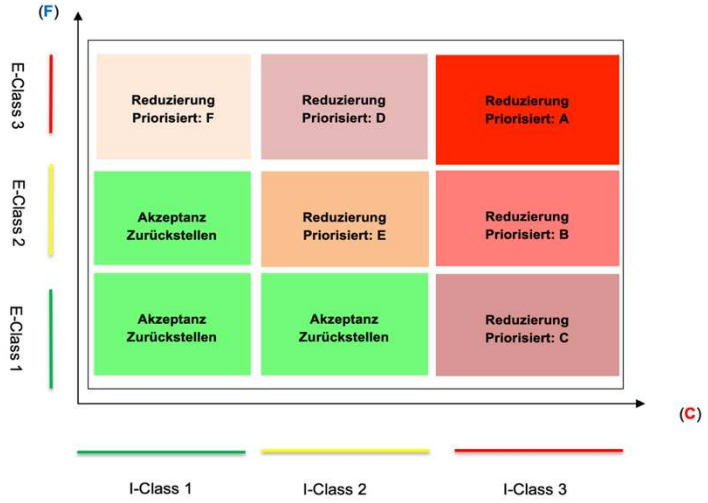


Bild 30: 3 x 3 Matrix zur CVE-Priorisierung (Quelle: In Anlehnung an Koza, 2022a, S. 2865)

Die Bestimmung der zeitlichen Kritikalität der einzelnen CVE-Behandlungen trägt dazu bei, die Ressourcenzuweisungen gezielter zu gestalten. Auf diese Weise können die anfallenden Behandlungen nach dem Ausmaß und der Zeitkritikalität verglichen werden, d.h. danach,

a) welche CVE größere Auswirkungen haben werden,
b) wie die individuelle Eintrittswahrscheinlichkeit für die jeweilige CVE zu definieren ist und c) in welcher zeitlichen Reihenfolge die CVE am effektivsten beseitigt werden können.

„Die Zeitprioritätsskala (A-F) ist eine organisationsspezifische Größe, die in Abhängigkeit von den verfügbaren personellen und technischen Ressourcen festgelegt werden muss“ (Koza, 2023, S. 103 (eigene Übersetzung)). Dennoch greift das Kohärenzmodell hier auf die folgende Zeitprioritätsskala:

- **A** (in zeitlicher Relation sollte die Behebung als Erstes ausgeführt werden),
- **B** (in zeitlicher Relation zu A sollte die Behebung als Zweites, wiederum in Relation zu den anderen Prioritätsstufen als Erstes ausgeführt werden),
- **C** (in zeitlicher Relation zu A und B sollte die Behebung als nächstes, wiederum in Relation zu den anderen Prioritätsstufen als Erstes ausgeführt werden),
- **D** (in zeitlicher Relation zu A, B und C sollte die Behebung als nächstes wiederum in Relation zu den anderen Prioritätsstufen als Erstes ausgeführt werden),
- **E** (in zeitlicher Relation zu A, B, C und D sollte die Behebung als nächstes, wiederum in Relation zu den anderen Prioritätsstufen als Erstes ausgeführt werden),
- **F** (in zeitlicher Relation zu A, B, C, D und E sollte die Behebung als nächstes wiederum in Relation zu den anderen Prioritätsstufen als Erstes ausgeführt werden),
- **Zurückstellen**, die als TN vernachlässigt werden können.

Mit dem Kohärenzmodell können CVE nun organisationsspezifisch und faktenbasiert (unabhängig von der subjektiven Sicht des Entscheidungsträgers) bewertet und klassifiziert werden. Das konzeptualisierte Kohärenzmodell, das Berechnungsmodell und das Portfolio können gemäß der obigen Erklärung instanziiert werden, so dass jede Organisation das obige Verfahren adaptieren und an ihre eigenen Bedürfnisse anpassen kann. Zwecks dieser Operationalisierung erfolgt im nächsten Kapitelabschnitt die Festlegung der intrinsischen und extrinsischen Standard-Subdeterminanten, die in das Modell eingebettet werden.

5.3 Festlegung von Standard-Subdeterminanten

5.3.1 Übersicht der intensiven und extensiven Subdeterminanten

„Um jedoch die erste Metaebene und ihre Subdeterminanten des Kohärenzmodells auf das Berechnungsmodell zu übertragen, müssen die Subdeterminanten in einem skalierten System durch geeignete Merkmale und Definitionen quantifiziert werden. Die globale Definition der Anwendbarkeit bestimmt [(engl. global Definition of Applicability (gDoA))] die übergeordneten Bewertungsmerkmale der jeweiligen [Stufen, die für die Klassifizierung der Subdeterminanten herangezogen werden]. Diese Übertragung dient der Aufrechterhaltung des logischen Zusammenhangs, der zwischen den einzelnen Bestimmungsmerkmalen und der gDoA hergestellt werden muss. Damit wird die Voraussetzung geschaffen, dass alle Teil-Subdeterminanten nach einem einheitlichen Bewertungsschema klassifiziert werden und die logische Verknüpfung als Grundvoraussetzung für die Einhaltung einer objektiven und reproduzierbaren Bewertung genutzt werden kann. Zu diesem Zweck gibt es drei Klassen: niedrig, hoch und kritisch. Nachfolgend sind die übergeordneten Definitionen der jeweiligen Klassifikationsstufen dargestellt“ (Koza, 2023, S. 103 (eigene Übersetzung)) (Tabelle 7):

Tabelle 7: Aufschlüsselung von gDoA (Quelle: In Anlehnung an Koza, 2023, S. 103 (eigene Übersetzung))

Einstufung	***Wertung***	**gDoA I** (Auswirkungsgrad)	**gDoA II** (Behandlungsgrad)
Low	**1**	Die Qualität und die Quantität der Systemdienstleistungen und der betroffenen Assets sind durch das Incident zu keinem Zeitpunkt gefährdet. Diese Einschätzung darf nur dann ausgeführt werden, wenn Systemausfälle und -beeinträchtigungen ausgeschlossen sind.	Die Entscheidung zur Nicht-Behandlung (Akzeptanzstrategie) hat im Sinne der Prognostik keinen negativen Einfluss auf den Auswirkungsgrad (gDoA I).
High	**2**	Die Qualität und die Quantität der Systemdienstleistungen und der betroffenen Assets können durch das Incident spürbar gefährdet werden. Diese Einschätzung darf nur dann ausgeführt werden, wenn nur marginale Systemausfälle und -beeinträchtigungen zu erwarten sind, die jedoch durch die personellen und systemrelevanten Redundanzen kompensierbar sind.	Die Entscheidung zur Nicht-Behandlung (Akzeptanzstrategie) kann im Sinne der Prognostik einen negativen Einfluss auf den Auswirkungsgrad (gDoA I) haben und diesen erschweren.
Critical	**3**	Die Qualität und die Quantität der Systemdienstleistungen und der betroffenen Assets sind durch das Incident gefährdet. Diese Einschätzung führt zu Systemausfällen und -beeinträchtigungen, welche auch die systemrelevanten Redundanzen betreffen.	Die Entscheidung zur Nicht-Behandlung (Akzeptanzstrategie) hat im Sinne der Prognostik einen negativen Einfluss auf den Auswirkungsgrad (gDoA I) und begünstigt diesen.

„Nach der Festlegung eines globalen Bewertungsschemas werden insgesamt acht standardmäßige intrinsische Subdeterminanten definiert, die nach der gDoA-Logik wie folgt klassifiziert werden“ (Koza, 2023, S. 103 (eigene Übersetzung)):

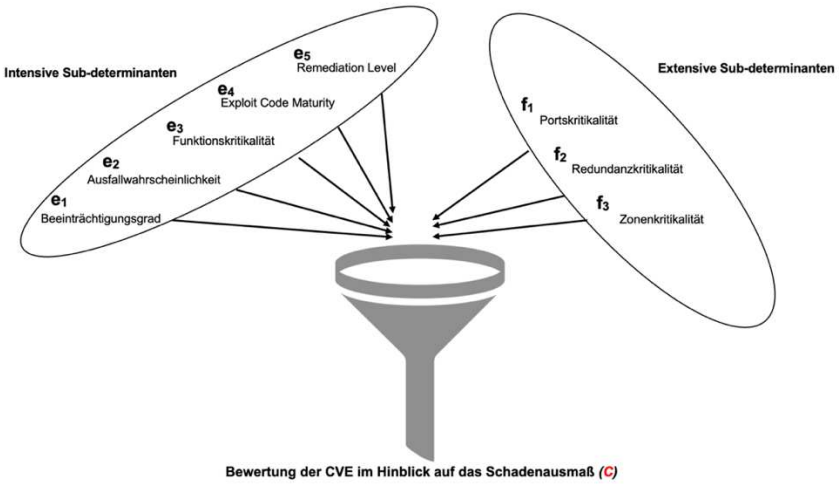


Bild 31: Intrinsische und extrinsische Subdeterminanten (Schadenausmaß) (Quelle: Koza, 2023, S. 104 (eigene Übersetzung))

„Die zuverlässige und objektive Bestimmung des CVE-Schadensausmaßes innerhalb des Kohärenzmodells lässt sich anhand von acht Subdeterminanten bestimmen. Konventionelle Methoden zur Bewertung von Risiken gemäß ISO/IEC 27005, ISO/IEC 27035 und NIST SP 800-53 werden derzeit in der Praxis größtenteils mit einer subjektiven und personenabhängigen Bewertung des Schadensausmaßes und der Eintrittswahrscheinlichkeit wahrgenommen. Die Bewertung des Schadensausmaßes bezieht sich auf negativen Auswirkungen auf die Daten- und Systemsicherheit. Die Eintrittswahrscheinlichkeit stellt eine empirische Analyse dar, die oft […] nicht fundiert in die jeweilige Analyse eingebettet ist. Je nach Erfahrung, persönlichem Empfinden, Wahrnehmung der aktuellen Sicherheitslage (z.B. Pessimismus versus Optimismus), Relevanz, Verhaltensabsicht, Wissen und Fähigkeit des Bewerters erfolgt die Bewertung eines Risikos bzw. einer Sicherheitslücke individuell und kann unterschiedlich ausfallen. In Bezug auf eine CVE-Bewertung soll das Kohärenzmodell daher eine Abhilfe schaffen und sicherstellen, dass die Bewertung nicht subjektiv (unabhängig vom Entscheidungsträger), sondern objektiv und faktenbasiert erfolgt. Um dieses Ziel zu erreichen, werden die oben aufgeführten acht objektiven Subdeterminanten für die Bewertung des Schadensausmaßes herangezogen. Gemäß dem Kohärenzmodell besteht eine Beziehung zwischen den intensiven und extensiven Subdeterminanten“ (Koza, 2023, S. 104 (eigene Übersetzung)). Hierzu spielt die Postulierung aus Kap. 6.2.1 eine relevante Rolle, da die Angriffsextensivität auch direkt mit der Angriffsintensivität zusammenhängt. Schlussfolgernd bedeutet es also, dass eine Aussage über die Schadenstiefe auch eine Aussage über den Schadensumfang erlaubt. Wird diese Prämisse auf die acht Subdeterminanten angewendet, so entsteht ein direkter Bezug zwischen den Subdeterminanten (vgl. Koza, 2023, S. 104).

5.3.2 Beeinträchtigungsgrad e1 und Portskritikalität f1

Der „***Beeinträchtigungsgrad e_1***“ umfasst die erste intensive Subdeterminante. Dieser gibt wieder, wie ausgeprägt der Grad der Kompromittierung einer CVE ist. Daraus ergibt sich ein korrelierter Effekt, bei dem die Bestimmung der extensiven Subdeterminante „**Portskritikalität f_1“** gleichzeitig die Bestimmung der intensiven Subdeterminante **e_1** impliziert (vgl. Koza, 2023, S. 104 f.). Wie bereits in Kap. 5.2.1 aufgeführt, stellen die Anwendungen ihre Dienste in der Anwendungsschicht über die ihnen zugewiesenen Ports sicher. Trojaner, Ransomware, Malware oder vergleichbare Schadsoftware werden dementsprechend portspezifisch entwickelt. So konzentrieren sich die Cyberkriminellen bei der Entwicklung von Schadsoftware auf einen bestimmten und meist in den Netzwerken eingesetzten Port, um über diesen Port einen unautorisierten Zugang und Zugriff auf die ICS-Systeme zu erhalten. So nutzen CVE für den Zugang auf die ICS-Applikationen einen spezifischen Port und können auch nur über diesen expliziten Port den Angriff auf die ICS-Systeme initiieren. Selbst Metamorphe und polymorphe Malware nutzen für den Angriff bzw. Angriffsart diese Vorgehensweise. Wird angenommen an, dass eine CVE (z. B. Ransomware wannaCry) den TCP-Port 445 betrifft, der bspw. mehrfach als Netzwerkprotokoll (z. B. von Windows) verwendet wird und sich nicht einfach deaktivieren lässt, da bei einer Deaktivierung Windowsdienste nicht mehr zur Verfügung stehen könnten. So kann davon ausgegangen werden, dass diese CVE mit ihrer speziellen Codierung zwar nur den TCP-Port 445 ausnutzen kann, aber durch die mehrfache Integration des TCP-Ports 445 innerhalb eines Netzwerks nicht nur einen Bereich, sondern mehrere Bereiche gleichzeitig betroffen sind (vgl. Koza, 2023, S. 105).

Dieser Kumulationseffekt ist durch die ausgeprägte Angriffsvielfalt kritisch und kann dazu führen, dass durch eine einzige CVE mehrere Systeme und Bereiche infiltriert werden können. Anders ausgedrückt, hat dieses Prinzip mit der Angriffsvielfalt einer CVE zu tun, die wiederum mit der internen Konfiguration und den Eigenschaften der eingesetzten Ports korreliert (vgl. Koza, 2023, S. 105).

Während der TCP-Port 455 als kritisch zu definieren gilt, kann ein anderer Port, der vom Internet nicht erreichbar ist und somit nicht über netzwerkbasierte Angriffe attackiert werden kann, als unkritisch eingestuft werden. So kann ein Port als unkritisch definiert werden, wenn die Ein- und Ausgänge nicht vom Internet erreichbar (autarke industrielle Netzwerke bzw. Insellösungen) sind und somit nicht willkürlich über netzwerkbasierte Angriffe attackiert werden können.

Zu diesem Zweck müssen die im ICS-Netz verwendeten Ports identifiziert und nach den Konfigurationsprofilen und -Eigenschaften klassifiziert werden. In diesem Zusammenhang spielen mehrere Faktoren für die Bestimmung der ***Portkritikalität f_1*** eine Rolle. Diese Faktoren werden in der nachfolgenden Tabelle 8 zur Klassifizierung der Ports unter Berücksichtigung der gDoA wie folgt definiert:

Tabelle 8: Klassifizierungsstufen zur Ermittlung der Kritikalität eingesetzter Ports in ICS-Netzwerken (Quelle: In Anlehnung an Koza, 2023, S. 105 (eigene Übersetzung))

Portskritikalität (f_1)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Gesperrte und nur nach innen geöffnete Ports ohne Zugang zum Internet (eigenständige und isolierte Netze)	Low	Low
2	Offene Ports mit Zugang zum Internet, segmentiert durch Firewalls und gleichzeitig überwacht durch Ports Security und Scanning-Systeme	High	High
3	Offene Ports mit Zugang zum Internet, welche nicht durch Ports Security überwacht werden sowie Mehrfachnutzung von Ports in einer oder mehreren logischen Zonen	Critical	Critical

Hierdurch entsteht die Möglichkeit die identifizierten ICS-Ports nach einem einheitlichen Schema zu klassifizieren, um den Grad der Angriffsvielfalt einer CVE zu bestimmen. Durch die vorhandene Beziehung zwischen der ***f_1*** und ***e_1*** lässt sich in der logischen Schlussfolgerung durch die Klassifizierung der Ports sowie durch die Zuordnung der CVE zu dem betroffenen Port gleichzeitig auch die Subdeterminante „**Beeinträchtigungsgrad e_1**“ bestimmen. So wird der TCP-Port 445 als kritisch eingestuft und der Wertung 3 zugeordnet. Alle CVE, die den TCP-Port 445 angreifen, besitzen ebenfalls einen kritischen Beeinträchtigungsgrad.

Diese Beziehung zwischen den intensiven und extensiven Subdeterminanten ***e_1*** und ***f_1*** wird anhand der Tabelle 9 festgelegt:

Tabelle 9: Klassifizierungsstufen zur Ermittlung des Beeinträchtigungsgrades einer CVE (Quelle: In Anlehnung an Koza, 2023, S. 105 (eigene Übersetzung)))

Beeinträchtigungsgrad (e_1)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Korrelierte Bewertung: Beeinträchtigungsgrad einer CVE kann als mäßig eingestuft werden, wenn der vom CVE betroffene Port (f_1) mit der Wertung 1 bewertet wird.	Low	Low
2	Korrelierte Bewertung: Beeinträchtigungsgrad einer CVE kann als hoch eingestuft werden, wenn der vom CVE betroffene Port (f_1) mit der Wertung 2 bewertet wird.	High	High
3	Korrelierte Bewertung: Beeinträchtigungsgrad einer CVE kann als kritisch eingestuft werden, wenn der vom CVE betroffene Port (f_1) mit der Wertung 3 bewertet wird.	Critical	Critical

5.3.3 Ausfallwahrscheinlichkeit e2 und Redundanzkritikalität f2

Die zweite intensive Subdeterminante betrifft die **„Ausfallwahrscheinlichkeit e_2“.** Die Ausfallsicherheit eines Systems ist eine Eigenschaft, die im Wesentlichen von den vorhandenen Systemredundanzen bestimmt wird. So enthält die „**Ausfallwahrscheinlichkeit e_2“** auch eine kohärente Beziehung, wo die Bestimmung des **e_2** von der Kritikalität der Redundanzen „**Redundanzkritikalität f_2“** abhängig ist. Besitzt ein System keine physischen Redundanzen (z. B. ohne Redundanzen in getrennten Brandabschnitten, (Geo-) Redundanz-Backups oder mögliche Auslegung von Systemen, die ohne Berücksichtigung des n-1-Kriteriums entworfen wurden), so kann die Ausfallwahrscheinlichkeit bei einer Kompromittierung als kritisch eingestuft werden, da die Systeme als SPOF zu definieren sind.

Wichtig hierbei ist jedoch auch die Betrachtung von Backup-Systemen und deren physischen und logischen Segmentierungen. Werden die Backup-Systeme bspw. auf denselben physischen und logischen Bereichen konfiguriert, so kann ein CVE als Ransomware durch die fehlende Netzwerksegmentierung auch die gesicherten Daten auf dem Backup-Server mit verschlüsseln. Wenn also das Hauptsystem kompromittiert wird, ist die Wahrscheinlichkeit sehr hoch, dass auch das vorhandene Backup in Mitleidenschaft gezogen wird (Vererbungseffekt). Kompromittiert eine CVE ein ICS ohne Redundanzen und Backup-Systemen oder mit Redundanzen und Backup-Systemen in demselben logischen Netzwerk, ist die logische Schlussfolgerung, dass solche Systeme im Hinblick auf die Ausfallsicherheit und Geschäftskontinuität (engl. Business Continuity) nicht ausreichend gesichert sind. Diese Betrachtung betrifft auch virtuelle Maschinen. Bei dieser Auslegung muss jedoch der Verteilungseffekt der virtuellen Maschinen berücksichtigt werden, da die virtuellen Maschinen im Gegensatz zu den physischen Servern leichter neukonfiguriert und aufgesetzt werden können.

Während ein ICS ohne Redundanzen kritisch definiert wird, kann ein anderes mit Redundanzen in separaten Abschnitten, als unkritisch bzw. weniger kritisch eingestuft werden. Zu diesem Zweck müssen die im ICS-Netz verwendeten Systeme identifiziert und nach der Redundanzkritikalität und der konzipierten Netzwerkarchitektur klassifiziert werden. In diesem Zusammenhang spielen mehrere Faktoren für die Bestimmung der **Redundanzkritikalität f_2** eine Rolle. Diese Faktoren werden in der nachfolgenden Tabelle 10 zur Klassifizierung der Redundanzkritikalität der ICS unter Berücksichtigung der gDoA wie folgt definiert:

Tabelle 10: Klassifizierungsstufen zur Ermittlung der Redundanzkritikalität der ICS-Netzwerke (Quelle: In Anlehnung an Koza, 2023, S. 106 (eigene Übersetzung))

Redundanzkritikalität (f_2)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	ICS haben eine physische 1:1 gespiegelte Geo-Redundanz mit einem Offline-Backup-System - oder ICS besitzen eine Geo-Redundanz	Low	Low
2	ICS und Online-Backup-Systeme sind nur durch unterschiedliche Brandabschnitte physisch getrennt	High	High
3	ICS haben keine Redundanzen und werden als SPOF betrachtet oder haben Redundanzen mit einem Backup-System im gleichen logischen und physischen Segment	Critical	Critical

Hierdurch entsteht die Möglichkeit die identifizierten Systeme nach einem einheitlichen Schema zu klassifizieren, um den durch eine CVE verursachten Grad der Ausfallwahrscheinlichkeit zu bestimmen. Durch die Beziehung zwischen $\mathbf{f_2}$ und $\mathbf{e_2}$ lässt sich durch die Klassifizierung der Systeme sowie durch die Zuordnung der CVE zu den betroffenen Systemen gleichzeitig auch die Subdeterminante „**Ausfallwahrscheinlichkeit e_2**“ bestimmen. So werden Systeme ohne Redundanzen als kritisch eingestuft und der Wertung 3 zugeordnet. Alle CVE, die diese Systeme angreifen und kompromittieren können, besitzen ebenfalls eine kritische Ausfallwahrscheinlichkeit.

Diese Beziehung zwischen den intensiven und extensiven Subdeterminanten $\mathbf{e_2}$ und $\mathbf{f_2}$ wird anhand der Tabelle 11 festgelegt:

Tabelle 11: Klassifizierungsstufen zur Ermittlung von Ausfallwahrscheinlichkeit von ICS (Quelle: In Anlehnung an Koza, 2023, S. 106 (eigene Übersetzung))

Ausfallwahrscheinlichkeit (e_2)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Korrelierte Bewertung: Ausfallwahrscheinlichkeit einer CVE kann als mäßig eingestuft werden, wenn das von der CVE betroffene System (f_2) mit der Wertung 1 bewertet wird.	Low	Low
2	Korrelierte Bewertung: Ausfallwahrscheinlichkeit einer CVE kann als hoch eingestuft werden, wenn das von der CVE betroffene System (f_2) mit der Wertung 2 bewertet wird.	High	High
3	Korrelierte Bewertung: Ausfallwahrscheinlichkeit einer CVE kann als kritisch eingestuft werden, wenn das von der CVE betroffene System (f_2) mit der Wertung 3 bewertet wird.	Critical	Critical

5.3.4 Funktionskritikalität e3 und Zonenkritikalität f3

Die dritte intensive Subdeterminante, die „**Funktionskritikalität e_3**“, enthält ebenfalls eine korrelierte Bewertung. Hier ist die Gewichtung von der extensiven Subdeterminante „**Zonenkritikalität f_3**“ abhängig und korreliert mit dieser. Gemäß dem Sicherheitszonenprinzip werden kritische Systeme und Anwendungen in tiefere Netzwerkzonen integriert und durch Firewalls oder spezielle Sicherheitsgateways von anderen Netzen getrennt (vgl. Koza, 2023, S. 107). Zeitkritische oder geschäftskritische Aufgabenprofile, Systeme und Anwendungen werden von den technischen Basisinfrastrukturen in mehreren logischen Zonen physisch und logisch separiert. Der konzeptionelle Aufbau der ICS-Netzwerkzonen und -segmenten orientiert sich in diesem Zusammenhang an dem Schutzbedarf der betrachtenden Systeme.

Kompromittiert eine CVE z.B. eine Anwendung in den tiefsten logischen Sicherheitszonen, so kann davon ausgegangen werden, dass hierbei wesentliche zeitkritische und geschäftskritische Funktionen (z. B. SCADA-Systeme oder SPS) betroffen sind, die möglicherweise auch einen gesetzlichen Verstoß darstellen (Verletzung der unterberechnungsfreien Energieversorgung, da die Versorgungskontinuität nicht mehr gegeben ist).

Zwar ist die Wahrscheinlichkeit, dass eine derartige CVE soweit und so tief in die ICS-Netzwerken eindringen kann sehr gering. Kommt es jedoch zu einer derartigen Kompromittierung, so sind die Folgen katastrophal. Außerdem können die Folgen einer CVE als katastrophal eingestuft werden, wenn die ICS-Netzwerke nicht ausreichend segmentiert sind. Eine Vielzahl an technischen Basisinfrastrukturen, insbesondere KMU besitzt oft nur eine einzige Netzwerkzone bzw. ein einziges Netzwerksegment. Das bedeutet, dass die Netzwerkzone bzw. das Netzwerksegment automatisch eine kritische Zonenkritikalität besitzt, da eine durch eine CVE verursachte Kompromittierung einer einzigen Netzwerkzone, gleichzeitig die Kompromittierung aller in der Netzwerkzone integrierten und involvierten Systeme und Applikationen bedeutet. Bei dieser Betrachtung muss also die Anzahl der betroffenen Zonen ebenfalls mitberücksichtigt werden. Bezogen auf das Beispiel mit der CVE, die über TCP-Port 455 initiiert wird, kann davon ausgegangen werden, dass aufgrund des mehrfachen Vorkommens des TCP-Ports 455 auch mehrere logische Zonen gleichzeitig betroffen und kompromittiert sind. Zu diesem Zweck müssen die im ICS-Netz definierten Netzwerkzonen und Systeme identifiziert und nach der Zonenkritikalität und dem konzipierten Netzwerkzonenplan klassifiziert werden. In diesem Zusammenhang spielen mehrere Faktoren für die Bestimmung der **Zonenkritikalität f_3** eine Rolle. Diese Faktoren werden in der nachfolgenden Tabelle 12 zur Klassifizierung der Zonenkritikalität der ICS-Netzwerke unter Berücksichtigung der gDoA wie folgt definiert:

Tabelle 12: Klassifizierungsstufen zur Ermittlung der Zonenkritikalität der ICS-Netzwerken (Quelle: In Anlehnung an Koza, 2023, S. 107 (eigene Übersetzung))

Zonenkritikalität (f_3)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Wenn die erste logische Zone (internes Netz) betroffen ist (erste Zone getrennt durch DMZ und/oder die erste Firewall- bzw. Sicherheitsgateways-Ebene)	Low	Low
2	Wenn die zweite logische Zone betroffen ist (zweite Zone getrennt durch die zweite Firewall- bzw. Sicherheitsgateways-Ebene)	High	High
3	Wenn die dritte logische Zone betroffen ist (zweite Zone getrennt durch die dritte/vierte Firewall- bzw. Sicherheitsgateways-Ebene) oder wenn mehrere Zonen betroffen sind, oder wenn nur eine einzige Zone definiert ist.	Critical	Critical

Hierdurch ergibt sich ebenfalls die Möglichkeit die identifizierten ICS-Netzwerkzonen nach einem einheitlichen Schema zu klassifizieren, um die durch eine CVE betroffene Zone und die Kritikalität zu bestimmen. Durch die vorhandene kohärente Beziehung, Klassifizierung der Netzwerkzonen sowie durch die Zuordnung der CVE zu den betroffenen Zonen zwischen f_3 und e_3 lässt sich in der logischen Schlussfolgerung gleichzeitig auch die Subdeterminante **„Funktionskritikalität e_3“** bestimmen. So werden Netzwerke ohne Segmentierung in den höchsten Zonen sowie multiplen Zonen als kritisch eingestuft und der Wertung 3 zugeordnet. Alle CVE, die diese Art der Zonen angreifen und kompromittieren können, kompromittieren ebenfalls kritische Funktionen und Applikationen.

Die Beziehung zwischen den intensiven und extensiven Subdeterminanten $\mathbf{e_3}$ und $\mathbf{f_3}$ wird anhand der nachfolgenden Tabelle 13 festgelegt:

Tabelle 13: Klassifizierungsstufen zur Ermittlung von Funktionskritikalitäten von ICS-Systemen (Quelle: In Anlehnung an Koza, 2023, S. 107 (eigene Übersetzung))

Funktionskritikalität (e_3)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Korrelierte Bewertung: Von einer CVE betroffene Funktionalität kann als mäßig eingestuft werden, wenn die von der CVE betroffene Netzwerkzone (f_3) mit der Wertung 1 bewertet wird.	Low	Low
2	Korrelierte Bewertung: Von einer CVE betroffene Funktionalität kann als hoch eingestuft werden, wenn die von der CVE betroffene Netzwerkzone (f_3) mit der Wertung 2 bewertet wird.	High	High
3	Korrelierte Bewertung: Von einer CVE-betroffene Funktionalität kann als kritisch eingestuft werden, wenn die von der CVE betroffene Netzwerkzone (f_3) mit der Wertung 3 bewertet wird.	Critical	Critical

5.3.5 Exploit Code Maturity e4 und Remediation Level e5

Die vierten und fünften intensiven Subdeterminanten betten die temporären „**Exploit Code Maturity e_4**“ und „**Remediation Level e_5**“ ein, welche signifikante Informationen über eine CVE darstellen. $\mathbf{e_4}$ führt an, inwieweit eine CVE von dem Angreifer operationalisiert werden kann. Dabei greift das Kohärenzmodell auf die Klassifizierung einer CVE, die durch die CVSS-Klassifizierung weltweit einheitlich bestimmt wird. Wenn bspw. eine CVE als „Function (F)“ oder „High (H)“ eingestuft wird, so kann davon ausgegangen werden, dass eine CVE nicht nur theoretisch, sondern auch praktisch mit den im Internet veröffentlichen Codes und Tools von jedem Angreifer weltweit ausgenutzt werden kann. Die öffentliche Verfügbarkeit von einfach zu nutzendem Schadcode, auch Exploit-Code genannt, erhöht die Zahl der potenziellen Angreifer, da nicht nur professionelle Angreifer, sondern auch Scriptkiddies und ungeübte Angreifer in der Lage sind, den Schadcode mit Hilfe von entsprechenden Toolkits zu operationalisieren, was den Schweregrad der Sicherheitslücke erhöht (vgl. FIRST, o. J. c).

Die Ausnutzung einer bestimmten Schwachstelle in der realen Welt kann zunächst nur theoretisch sein. Die Veröffentlichung von Proof-of-Concept Code (POC), funktionalem Schadcode oder ausreichenden technischen Angriffsdetails, die zur Ausnutzung der Schwachstelle erforderlich sind, können jedoch im Verlauf der Zeit konzipiert und der Öffentlichkeit zur Verfügung gestellt werden. Außerdem können sich die verfügbaren Schadcodes von einer (POC-) Demonstration zu einem ausführbaren und lauffähigen Schadcode weiterentwickeln, der die Schwachstelle erfolgreich missbrauchen kann.

In schwerwiegenden Fällen kann er als Nutzlast eines netzwerkbasierten Wurms oder Virus oder anderer automatisierter Angriffswerkzeuge bereitgestellt werden. In einigen schwerwiegenden Fällen kann der Schadcode auch als „Payload“ eines netzbasierten Wurms, Virus oder anderer automatisierter Angriffswerkzeuge übertragen werden (vgl. FIRST, o. J. c). Die Klassifizierungsstufe der „**Exploit Code Maturity e_4**“ wird in der nachfolgenden Tabelle 14 aufgeführt. Hierbei gilt: Je einfacher eine Schwachstelle bzw. eine CVE ausgenutzt werden kann (siehe Einstufung Functional, High in Tabelle 14), desto höher ist die Schwachstellenbewertung.

Tabelle 14: Klassifizierungsstufen zur Exploit Code Maturity (e_4) (Quelle: In Anlehnung an FIRST, o. J. c)

Exploit Code Maturity (e_4)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Unproven (U): Es ist kein Exploit-Code bzw. Schadcode verfügbar, oder eine Ausnutzung ist theoretischer Natur.	Low	Low
2	Proof-of-Concept (P) Proof-of-Concept-Schadcode oder eine reelle Angriffsdemonstration ist für die meisten Systeme nicht funktionsfähig. Der Schadcode oder die Angriffstechnik ist nicht in allen Situationen funktionsfähig und kann erhebliche Modifikationen durch einen erfahrenen Angreifer erfordern.	High	High
3	Functional (F): Funktionaler Schadcode ist verfügbar. Der Code funktioniert in den meisten Situationen, in denen die Schwachstelle existiert. High (H): Es gibt einen funktionalen autonomen Schadcode und die Angriffsdetails sind allgemein zugänglich und verfügbar. Der Schadcode funktioniert in jeder Situation oder wird aktiv über einen autonomen Agenten (z. B. einen Wurm oder Virus) verbreitet. Systeme, die mit einem Netzwerk verbunden sind, werden wahrscheinlich gescannt oder ausgenutzt. Die Ausnutzung derartiger Schwachstellen kann über verfügbare und leicht zu bedienende, automatisierte Tools operationalisiert werden. Not Defined (X): Es können keine ausreichenden Informationen der Schwachstelle zugeordnet werden. Nichtdestotrotz wird die Schwachstelle äquivalent zur Stufe „High“ eingestuft.	Critical	Critical

Die fünfte intensive Subdeterminante „**Remediation Level e_5**“ hingegen betrachtet die andere Kehrseite einer CVE, welche sich im Detail mit dem Vorhandensein der Lösung zur Beseitigung einer CVE als Schwachstelle beschäftigt. Existieren für eine CVE keine von den Systemherstellern definierten Sicherheitsupdates oder Lösungsansätze („Unavailable“ or „Not Defined“), so kann davon ausgegangen werden, dass die Schwachstelle eine Art Zero Day Exploit darstellt, die eine zeitkritische Lösung benötigt. So ist die Behebungsstufe (Remediation Level) einer Sicherheitslücke ein wichtiger Faktor für die Priorisierung einer Schwachstelle.

Nach der Entdeckung und Veröffentlichung einer typischen Schwachstelle existieren noch keine passenden Lösungen, um diese als Sicherheitsupdates den Software- und Systemnutzern zur Verfügung zu stellen. Hier geht es um nicht gepatchte und somit unsichere Systeme. Das Patchmanagement umfasst alle Prozesse, die aufgesetzt werden, um eine entdeckte Sicherheitslücke in einer Software mit entsprechenden Sicherheitsupdates zu beheben. Existieren keine von den Systemherstellern konzipierten und freigegebenen Sicherheitsupdates oder Lösungen, so müssen KRITIS anderweitige (eigene) Lösungsansätze wie z. B. Abschirmen des Dienstes, Netzes oder sogenannte Workarounds als Zwischenlösung ausführen, bis ein offizieller Patch, ein Upgrade oder Sicherheitsupdate veröffentlicht werden. In jeder dieser Phasen erhält die Behebungsstufe eine andere Wertung, die abhängig der Lösungsverfügbarkeit und der Lösungsart definiert wird. Die temporäre Behebungsstufe wird daher zu Anfang bei der Entdeckung einer Schwachstelle als sehr kritisch betrachtet und mit der Zeit und der zur Verfügungstellung von Lösungen nach unten korrigiert, was wiederum die abnehmende Handlungsdringlichkeit widerspiegelt, da offizielle Sicherheitsupdates vollständig definiert sind. Die Klassifizierungsstufe „**Remediation Level e_5**“ wird in Tabelle 15 aufgeführt. Hierbei gilt der Grundsatz: Je weniger offiziell und dauerhaft eine Sicherheitslösung zur Behebung der Schwachstelle ist, desto höher und kritischer fällt die Bewertung der Schwachstellen aus.

Tabelle 15: Klassifizierungsstufen zum Remediation Level (e_5) (Quelle: In Anlehnung an FIRST, o. J. c | Koza, 2023, S. 108)

Remediation Level (e_5)

Wertung		Auswirkungsgrad	Behandlungsgrad
1	Official Fix (O): Eine vollständige Herstellerlösung ist verfügbar. Entweder hat der Hersteller einen offiziellen Patch herausgegeben oder es ist ein Upgrade verfügbar.	Low	Low
2	Temporary Fix (T): Eine offizielle, aber vorübergehende Lösung ist verfügbar. Dazu gehören Fälle, in denen der Hersteller einen temporären Hotfix, ein Tool oder eine Übergangslösung herausgibt.	High	High
3	Workaround (W): Es existiert eine inoffizielle, herstellerunabhängige Lösung. In einigen Fällen erstellen die Benutzer der betroffenen Technologien einen eigenen Patch oder stellen Schritte zur Umgehung oder anderweitigen Entschärfung der Schwachstelle zur Verfügung. Unavailable (U): Keine Lösung verfügbar. Not Defined (X): Es können der Schwachstelle keine ausreichenden Informationen zugeordnet werden. Dennoch wird die Schwachstelle äquivalent zur Stufe „Unavailable“ eingestuft.	Critical	Critical

Die Kombination dieser beiden intensiven Subdeterminanten ermöglicht eine Aussage über die Ausnutzungsmöglichkeit einer CVE in freier Wildbahn. Im nachfolgenden Kapitelabschnitt werden die zuvor dargestellten intrinsischen acht Subdeterminanten und die extrinsische Subdeterminante EPSS-Score in die Berechnungsmethodik des Kohärenzmodells übertragen, um die hierfür erforderlichen Klassifizierungsstufen zur Priorisierung von CVE darzustellen.

5.3.6 Überführung der Standard-Subdeterminanten in das Kohärenzmodell

So implementiert das Kohärenzmodell insgesamt acht intrinsische Subdeterminanten (fünf intensive und drei extensive) und eine extrinsische Subdeterminante, die zur Bewertung und Priorisierung von CVE in die Berechnungsmethodik wie folgt eingebettet werden (vgl. Koza, 2022a, S. 2864 | Koza, 2023, S. 99):

$$\boldsymbol{CVE} = f\,(\boldsymbol{F} = \boldsymbol{Extrinsic\ CVE\ factor},\ \boldsymbol{C} = \boldsymbol{Intrinsic\ CVE\ factor}) \tag{21}$$

$$\rightarrow \boldsymbol{CVE} = (\boldsymbol{Extrinsic\ CVE\ factor}),\ (\boldsymbol{Intrinsic\ CVE\ factor}) \tag{22}$$

$$\rightarrow \boldsymbol{CVE} = (\boldsymbol{E\text{-}Class}),\ (\boldsymbol{I\text{-}Class}) \tag{23}$$

$$I\text{-}Class = (b_{extensive},\ b_{intensive}) = ((b_3 + b_4) + (b_1 + b_2)) \rightarrow \tag{24}$$

$$C = (((f_1 + f_2 + f_3) + 0) + ((e_1 + e_2 + e_3 + e_4 + e_5) + 0)) \rightarrow \tag{25}$$

($f_1 + f_2 + f_3$: $= b_3$; 0: $= b_4$; $e_1 + e_2 + e_3 + e_4 + e_5$: $= b_1$; 0: $= b_2$)

$$C = ((f_1 + f_2 + f_3) + (e_1 + e_2 + e_3 + e_4 + e_5)) = \boldsymbol{Intrinsic\ CVE\ factor} \tag{26}$$

$$\boldsymbol{F} = (EPSS\text{-}Score\ or\ CWE\text{-}Score) = \boldsymbol{Extrinsic\ CVE\ factor} \tag{27}$$

Um das **Schadensausmaß** einer CVE (*C*) zu klassifizieren und nach der Kritikalität des Ausmaßes zu bewerten, wird die mathematische Formel in ein Schema mit differenzierten Klassen übertragen, um das quantifizierte Schadensausmaß interpretieren zu können (vgl. Koza, 2022a, S. 2864 | Koza, 2023, S. 100):

$$C = ((f_1 + f_2 + f_3) + (e_1 + e_2 + e_3 + e_4 + e_5)) = \boldsymbol{Intrinsic\ CVE\ factor} \tag{28}$$

Für die Klassifizierung des erreichten (*C*)-Wertes werden die intensiven $(b_{intensive} = (e_1 + e_2 + e_3 + e_4 + e_5)$ und extensiven $(b_{extensive} = (f_1 + f_2 + f_3))$ Determinanten in einem 2-dimensionalen Klassifizierungsschema kombiniert. Die folgende Berechnung zur Klassifizierung des erreichten (*C*)-Wertes wird hier verwendet (vgl. Koza, 2023, S. 100):

$(b_{intensive})$ wird der y-Achse zugeordnet:

$$Maximum\ value:\ I_{max}: ((|e_1, e_2, e_3, e_4, e_5|) \times 3) = 5 \times 3 = \boldsymbol{15} \tag{29}$$

$$Average\ value:\ I_{mid}: ((|e_1, e_2, e_3, e_4, e_5|) \times 2) = 5 \times 2 = \boldsymbol{10} \tag{30}$$

$$Minimum\ value:\ I_{min}: ((|e_1, e_2, e_3, e_4, e_5|) \times 1) = 5 \times 1 = \boldsymbol{5} \tag{31}$$

Wertebereich für die Klassifizierung der $(b_{intensive})$:

$$Critical \rightarrow Class\ 3 \rightarrow I_{mid} < b_{intensive} \leq I_{max} \rightarrow \boldsymbol{10} < b_{intensive} \leq \boldsymbol{15} \tag{32}$$

$$High \rightarrow Class\ 2 \rightarrow I_{min} < b_{intensive} \leq I_{mid} \rightarrow \boldsymbol{5} < b_{intensive} \leq \boldsymbol{10} \tag{33}$$

$$Low \rightarrow Class\ 1 \rightarrow 0 < b_{intensive} \leq I_{min} \rightarrow \boldsymbol{0} < b_{intensive} \leq \boldsymbol{5} \tag{34}$$

($b_{extensive}$) wird x-Achse zugeordnet:

$$\textit{Maximum value: } E_{max}\textit{: } ((|f_1, f_2, f_3|) \times 3) = 3 \times 3 = \mathbf{9} \quad (35)$$

$$\textit{Average value: } E_{mid}\textit{: } ((|f_1, f_2, f_3|) \times 2) = 3 \times 2 = \mathbf{6} \quad (36)$$

$$\textit{Minimum value: } E_{min}\textit{: } ((|f_1, f_2, f_3|) \times 1) = 3 \times 1 = \mathbf{3} \quad (37)$$

Wertebereich für die Klassifizierung der ($b_{extensive}$):

$$\textit{Critical} \rightarrow \textit{Class 3} \rightarrow E_{mid} < b_{extensive} \leq E_{max} \rightarrow \mathbf{6} < b_{extensive} \leq \mathbf{9} \quad (38)$$

$$\textit{High} \rightarrow \textit{Class 2} \rightarrow E_{min} < b_{extensive} \leq E_{mid} \rightarrow \mathbf{3} < b_{extensive} \leq \mathbf{6} \quad (39)$$

$$\textit{Low} \rightarrow \textit{Class 1} \rightarrow 0 < b_{extensive} \leq E_{min} \rightarrow \mathbf{0} < b_{extensive} \leq \mathbf{3} \quad (40)$$

Hieraus lassen sich folgende Zuordnungen der intensiven *($b_{intensive}$)* und extensiven *($b_{extensive}$)* Determinanten zu den jeweiligen Klassen generieren (Tabelle 16):

Tabelle 16: Grenzbereiche zur Klassifizierung des CVE-Schadenausmaßes (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 100 (eigene Übersetzung))

I-Class	Einstufung	Gesamtgrenzbereich	$b_{intensive}$ - Wertebereich	$b_{extensive}$ - Wertebereich
I-Class 1	**Low**	**[0, 8]**	$0 < b_{intensive} \leq 5$	$0 < b_{extensive} \leq 3$
I-Class 2	**High**	**[9, 16]**	$5 < b_{intensive} \leq 10$	$3 < b_{extensive} \leq 6$
I-Class 3	**Critical**	**[17, 24]**	$10 < b_{intensive} \leq 15$	$6 < b_{extensive} \leq 9$

So kann das folgende Klassifizierungsschema des (*C*)-Wertes mit den acht Subdeterminanten in der ersten Metaebene definiert werden, um CVE hinsichtlich des Schadensausmaßes zu bewerten und zu klassifizieren. So kann dem $b_{intensive}$ - und $b_{extensive}$ -Wertebereich die definierte „*I-Class*“ mit folgender Wertung zugeordnet werden (Bild 32 und Tabelle 17).

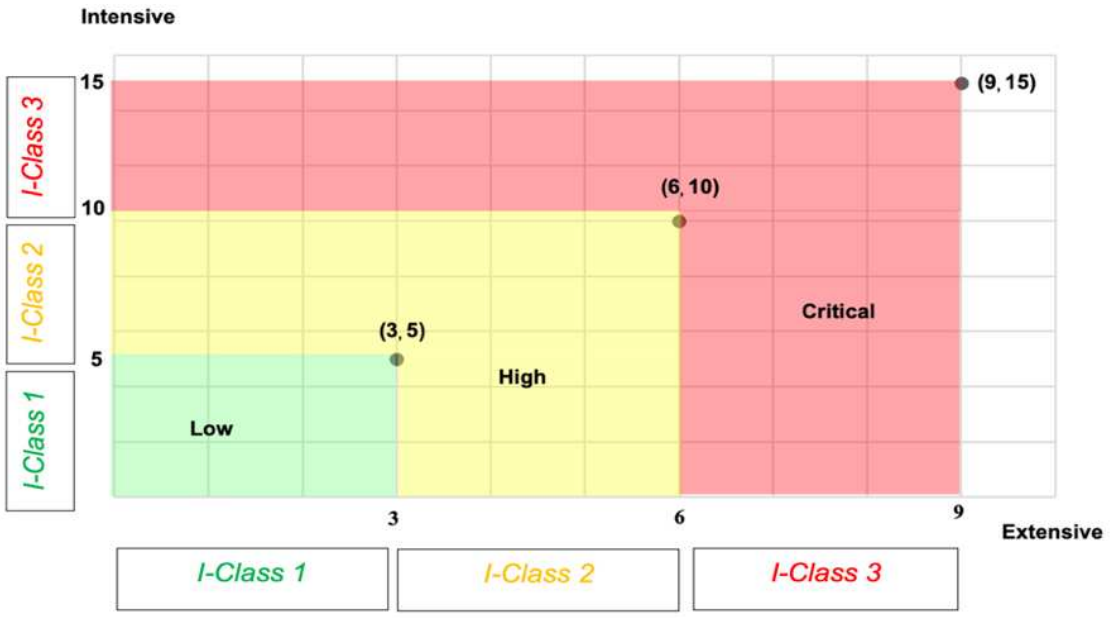


Bild 32: Klassifizierungsschema des (C)-Wertes anhand der acht Subdeterminanten (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 101)

Tabelle 17: I-Classes und die Wertungen zur Einstufung des CVE-Schadenausmaßes (Quelle: Eigene Darstellung)

I-Class	Wertung	Einstufung	Gesamtgrenzbereich für erreichten C-Wert
I-Class 1	*1*	*Low*	**[0, 8]**
I-Class 2	*2*	*High*	**[9, 16]**
I-Class 3	*3*	*Critical*	**[17, 24]**

Die zweite Metaebene des Kohärenzmodells ist der „***extrinsische CVE-Faktor***“ (***F***)

F *= (EPSS-Score or CWE-Score) =* ***Extrinsic CVE factor***

welcher zur Bestimmung der Eintrittswahrscheinlichkeit einer CVE herangezogen wird und den E-Classes zugeordnet wird.

Tabelle 18: E-Classes und die Wertungen zur Einstufung der CVE-Eintrittswahrscheinlichkeit (Quelle: In Anlehnung an Koza, 2022a, S. 2864 | Koza, 2023, S. 102 (eigene Übersetzung))

E-Class	Wertung	Einstufung	EPSS-Wertebereich	CWE-Wertebereich
E-Class 1	1	Low	*0 < F ≤ 0,3*	Low (L)
E-Class 2	2	High	*0,3 < F ≤ 0,6*	Medium (M), Default (D), Unknown (UK)
E-Class 3	3	Critical	*0,6 < F ≤ 1,0*	High (H), Not applicable (NA)

Durch die Kombination der beiden extrinsischen und intrinsischen Klassen (intrinsische „*I-Class*“ aus Tabelle 17 und extrinsische „*E-Class*“ aus Tabelle 18) und deren Darstellung in einem Portfoliomodell mit einer 3 x 3 Matrix können die CVE nun nach den beiden wichtigsten Kriterien (CVE-Schadensausmaß und CVE-Eintrittswahrscheinlichkeit) spezifiziert und bewertet werden. Bild 33 zeigt die abschließende Bewertung und Klassifizierung der CVE sowie die zeitliche Kritikalität und die geschätzten Ausfallfolgen.

$$\rightarrow \textbf{CVE} = (\textbf{I-Class}) \times (\textbf{E-Class}) \quad (41)$$

$$\textbf{CVE} = (1) \times (1) = 1 \rightarrow \textit{Final-Value (F-Value)} \quad (42)$$
$$\textbf{CVE} = (1) \times (2) = 2 \rightarrow \textit{Final-Value (F-Value)} \quad (43)$$
$$\textbf{CVE} = (1) \times (3) = 3 \rightarrow \textit{Final-Value (F-Value)} \quad (44)$$
$$\textbf{CVE} = (2) \times (1) = 2 \rightarrow \textit{Final-Value (F-Value)} \quad (45)$$
$$\textbf{CVE} = (2) \times (2) = 4 \rightarrow \textit{Final-Value (F-Value)} \quad (46)$$
$$\textbf{CVE} = (2) \times (3) = 6 \rightarrow \textit{Final-Value (F-Value)} \quad (47)$$
$$\textbf{CVE} = (3) \times (1) = 3 \rightarrow \textit{Final-Value (F-Value)} \quad (48)$$
$$\textbf{CVE} = (3) \times (2) = 6 \rightarrow \textit{Final-Value (F-Value)} \quad (49)$$
$$\textbf{CVE} = (3) \times (3) = 9 \rightarrow \textit{Final-Value (F-Value)} \quad (50)$$
(51)

I-class	E-class	F-Value	Behandlungsstrategie	Kategoriezuordnung	Priorisierungsstrategie
1	1	1	Akzeptanz	True Negatives (*TN*)	**Zurückstellen**
1	2	2	Akzeptanz	True Negatives (*TN*)	**Zurückstellen**
1	3	3	Reduzierung	True Positives (*TP*)	**F**
2	1	2	Akzeptanz	True Negatives (*TN*)	**Zurückstellen**
2	2	4	Reduzierung	True Positives (*TP*)	**E**
2	3	6	Reduzierung	True Positives (*TP*)	**D**
3	1	3	Reduzierung	True Positives (*TP*)	**C**
3	2	6	Reduzierung	True Positives (*TP*)	**B**
3	3	9	Reduzierung	True Positives (*TP*)	**A**

Bild 33: Kombination der I- und E-Classes zur Entscheidungsfindung (Quelle: Koza, 2023, S. 102 (eigene Übersetzung))

Die Realisierung des Kohärenzmodells sowie der dazugehörigen Standard-Subdeterminanten, die für die Bewertung und Priorisierung der CVE und der Schwachstellen herangezogen werden, erfolgt in IRET. Bevor jedoch die Machbarkeitsprüfung des Kohärenzmodells anhand dieser Softwarelösung operationalisiert werden kann, wird in einem Zwischenschritt das hierfür notwendige Rahmenwerk definiert, das auf Basis der modifizierten OODA-Schleife von John Boyd konzipiert ist. Im nächsten Kapitelabschnitt wird die hierfür modifizierte OODA-Schleife vorgestellt, welche im späteren Verlauf in Kap. 5.5 mit Hilfe der softwarebasierten Lösung operationalisiert und anhand von Anwendungsbeispielen zur Bewertung und Priorisierung von CVE veranschaulicht wird.

5.4 OODA-Schleife im Kontext des Kohärenzmodells

5.4.1 Einführung in die OODA-Schleife

Während der Luftkämpfe im Koreakrieg entwickelte John Boyd, ein Oberst der US Air Force, die OODA-Schleife (vgl. Boyd, zitiert nach Hammond, 2018, S. 1-6). Die Grundidee bestand darin, einen iterativen Entscheidungsunterstützungszyklus zu entwickeln. Boyd stellt ein mehrdimensionales, dynamisches Modell mit vier Schritten vor und keinen nach dem allgemein aufgefassten Verständnis, linearen Prozess dar (vgl. Tremblay, 2015, S. 19 | Boyd, zitiert nach Hammond, 2018, S. 385). In der ersten Phase (Observe) beobachtet der Teilnehmer die Umgebung. Diese Beobachtungen werden sowohl mit den internen als auch mit den externen Einflüssen und Faktoren abgeglichen. In der nächsten Phase (Orient) werden die Beobachtungen analysiert und interpretiert. Diese Interpretationen werden durch mentale Muster (konzeptionelle, strategische und erfahrungsorientierte Denkmodelle) beeinflusst, um die Faktoren zu analysieren (vgl. Boyd, 1976, S. 1).

Aus der Zuordnung der Beobachtungen zu den mentalen Mustern ergibt sich eine Reihe von möglichen Handlungsoptionen. In der dritten Phase (Decide) wird aus den bereits erarbeiteten Optionen auf der Basis von Beobachtungen und Orientierungen die effektivste Alternative ausgewählt und zur Operationalisierung vorbereitet. In der letzten Phase (Act) wird die Entscheidung umgesetzt. Anschließend werden die Ergebnisse der ausgeführten Handlungsoptionen beobachtet, und der Zyklus beginnt von neuem. In diesem OODA-Modell hängt der Erfolg von einer effizienten Ausführung ab. Diese Effizienz spiegelt sich in der Geschwindigkeit wider, mit der die OODA-Schleife im Vergleich zu dem Gegner durchlaufen wird. In dieser Konstellation trainierte die OODA-Schleife die Teilnehmer, einschließlich der Soldaten, dazu, trotz des Informationsdefizits, zeitkritische Entscheidungen schnell zu treffen. In einem weiteren Modell definierte Boyd ein komplexeres und nuancierteres Meta-Paradigma, welches als OODA-Schleife für intellektuelles Wachstum und Evolution in einer sich ständig wandelnden und unsicheren Landschaft eingesetzt wird. Zu diesem Zweck modifizierte Boyd den Zyklus und konzipierte einen iterativen und inkrementellen Analyse- und Entscheidungsprozess mit mehreren integrierten Feedback-Mechanismen. Im Vergleich zum ersten Modell eignet sich die neu gestaltete Schleife als ein fortlaufender zyklischer Prozess mit vielfältigen Rückkopplungen (Bild 34) (vgl. Boyd, zitiert nach Hammond, 2018, S. 8).

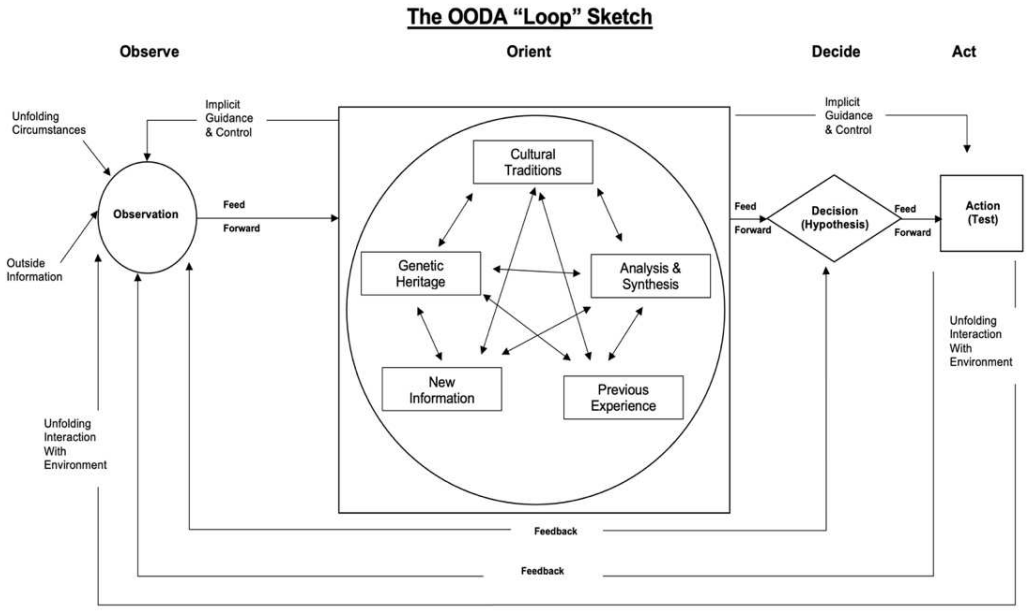


Bild 34: John Boyd's OODA loop (vgl. Boyd, zitiert nach Hammond, 2018, S. 384)

Die OODA-Schleife ist eines der international bekanntesten Modelle zur Entscheidungsunterstützung und wird von großen Unternehmen wie Dell oder Netflix eingesetzt, um Wettbewerbsvorteile zu erzielen (vgl. Lewis, 2016, o. S. | Laskowski, 2013, o. S | Boyd, zitiert nach Hammond, 2018, S. 7). Bevor die OODA-Schleife im Kontext des Kohärenzmodells vollständig dargestellt werden kann, ist es notwendig, einige grundlegende Konzepte aufzulisten. Boyd kombinierte ein tiefes Verständnis der Militärgeschichte und des strategischen Denkens mit einem breiten Spektrum anderer wissenschaftlicher Bereiche und Theoreme, einschließlich der Quantenmechanik, Kybernetik, Chaostheorie und Neodarwinismus (vgl. Boyd, zitiert nach Hammond, 2018, S. 237, S. 358).

Um die OODA-Schleife wirklich zu verstehen, muss daher eine Vertrautheit mit den wissenschaftlichen und philosophischen Entwicklungen sein, die zu der Entstehung beigetragen haben. Das grundlegende Ziel seiner Untersuchung fußt auf den Wunsch das Implizite trotz vorherrschender Unsicherheit durch den Einsatz eines lernenden Systems explizit zu machen. Boyds OODA-Schleife stellt im Kern ein Lernsystem bestehend aus einer Methode zum Umgang mit Ungewissheit und aus einer Strategie zum Gewinnen dar. Dazu greift Boyd auf die sogenannten mentalen Muster zurück (vgl. Boyd, 1976, S. 1).

Mentale Muster unterstützen Verständnis- und Entscheidungsprozesse und sind in der Regel kulturell geprägt, vererbt und sogar genetisch bedingt (vgl. Boyd, zitiert nach Hammond, 2018, S. 384). Mentale Muster können einerseits sehr spezifisch sein, z. B. die Einhaltung bestimmter Sicherheitsregeln zum Umgang und Betrieb mit einer technischen Anlage, oder sie können sich auf das individuelle gesellschaftliche Verhalten von Menschen beziehen, z.B. auf konventionelle Verhaltensregeln. Andererseits können mentale Muster globaler und allgemeiner Natur sein, wie z. B. funktionsübergreifende Grundsätze auf Unternehmensebene oder Fachgebiete (Psychologie, Datenschutz, Compliance, Wissenschaft, Militärdoktrinen über die Einsatzregeln und Informationssicherheit). Da Boyd mehr daran interessiert war, die OODA-Schleife als Organisationsprinzip für eine große Strategie zu nutzen, konzentrierte er sich auf die abstrakteren Arten von mentalen Mustern (vgl. Boyd, zitiert nach Hammond, 2018, S. 15).

Boyd verweist in der Folge auf drei philosophische und wissenschaftliche Prinzipien, um zu zeigen, dass der Versuch, einen sich zufällig verändernden Zustand mit bereits existierenden und statischen mentalen Modellen (dies impliziert auch die Sicherheitsmodelle) zu verstehen, nur zu Verwirrung, Inkonsistenz und zusätzlicher Unsicherheit führen wird (vgl. Boyd, zitiert nach Hammond, 2018, S. 237). Die Grundlage dieser Prinzipien ist nicht nur im menschlichen Verständnis oder in der Logik verwurzelt, sondern auch in den wissenschaftlichen Grundprinzipien des Universums verankert sind. Diese drei Prinzipien umfassen Beweise der Gödelschen Unvollständigkeitssätze, die Heisenbergsche Unschärferelation und den zweiten Hauptsatz der Thermodynamik (vgl. Boyd, 1976, S. 4-6).

Nach Boyd beobachten Menschen, um Konzepte zu spezifizieren und sie definieren Konzepte, um Beobachtungen vollziehen und verstehen zu können. Demzufolge werden Konzepte verwendet, um die Genauigkeit und Interpretation von Beobachtungen zu präzisieren. Da jedoch die Entwicklung eines Konzeptes auf Ungewissheit und auf einen unvollständigen Satz an Informationen zurückgeführt werden kann, kann in der Folge postuliert werden, dass ein Konzept letztlich auch unvollständig sein muss, da eine Abhängigkeit von einer dynamischen und volatilen Reihe von Beobachtungen existiert. So leitet Boyd aus Gödels Unvollständigkeitssätzen ab, dass jedes logische Modell der Realität unvollständig und möglicherweise inkonsistent ist und angesichts neuer Beobachtungen ständig verfeinert und angepasst werden muss (vgl. Boyd, zitiert nach Hammond, 2018, S. 322).

Um die Beobachtungen der Welt immer präziser und subtiler zu definieren, muss noch ein zweiter Grundsatz in Betracht gezogen werden. Dies betrifft die eingeschränkte Fähigkeit die Realität vollständig und korrekt zu beobachten, was sich ursächlich durch die Heisenbergsche Unschärferelation genauer erklären lässt. Das Prinzip der Heisenbergschen Unschärferelation zeigt, dass die Geschwindigkeit und die Position eines Teilchens nicht gleichzeitig bestimmt werden können. Die Position oder die Geschwindigkeit eines Teilchens kann bestimmt oder gemessen werden, aber nicht beides gleichzeitig. Je genauer ein Wert (Geschwindigkeit oder Position) bestimmt werden kann, desto ungenauer wird die Messung bzw. die Bestimmung des anderen Wertes. Indem Boyd dieses Prinzip auf das Verständnis der Welt und die Umwelt transformierte, kam er zu dem Schluss, dass eine genauere Beobachtung in einem bestimmten Bereich wahrscheinlich eine größere Unsicherheit in einem anderen Bereich zur Folge hat. Die Fähigkeit, die Realität genau zu beobachten, ist in diesem Zusammenhang begrenzt (vgl. Boyd, zitiert nach Hammond, 2018, S. 321).

Zur besseren Veranschaulichung im VM und IRM-Bereich kann der Fall des Universitätsklinikums Düsseldorf als Beispiel herangezogen werden (vgl. BSI, 2020b, o. S.). Nach dem Bekanntwerden der Schwachstelle in VPN-Produkten des Herstellers Citrix (CVE-2019-19781) haben die Cybersicherheitsingenieure die vom Hersteller konzipierten Sicherheitsupdates zur Behebung der Sicherheitslücke unverzüglich nach der offiziellen Freigabe des Herstellers auf die Systeme installiert.

Zwei Spezialfirmen hatten nach der Installation des Sicherheitsupdates die Systeme forensisch überprüft, ohne Hinweise auf eine Restgefährdung durch die bereits geschlossene Sicherheitslücke zu erhalten. Trotz des schnellen Patchs haben die Angreifer es dennoch geschafft, ein Backdoor-Programm einzuschleusen, um dieses später mit einer Ransomware aufzuladen und die Gesundheitsdaten des Krankenhauses zu verschlüsseln. Hierbei können zwei mögliche Ursachen herangezogen werden: Die Entscheidungsträger waren entweder so sehr auf das herkömmliche und isolierte Ausführen von Scanning-Programmen und dem Patchen des betroffenen VPN-Servers fixiert, sodass sie die weiteren möglichen Schnittstellen und Systeme nicht mehr in Betracht gezogen haben, oder sie hatten von vorne rein keine transparenten Kenntnisse über die bestehenden Schnittstellen und die bestehende CVE-Angriffsvielfalt, die unmittelbar mit der individuellen Netzwerkarchitektur, Netzwerkplanung und Netzwerkkonfigurationen in Verbindung steht. Wird eine CVE bekannt, so wird als erstes nach einem Sicherheitsupdate gesucht, um die identifizierte Sicherheitslücke zeitnah beseitigen zu können. Sind die Sicherheitsupdates zunächst installiert, so entsteht der optimistische Gedankengang, dass die Sicherheitslücke auch tatsächlich abgeschlossen ist. Existiert jedoch kein grundlegendes Wissen über die CVE-Angriffsvielfalt, Funktionskritikalität und Ausfallwahrscheinlichkeit der eigenen Software- und Hardwarelandschaft, so läuft man die Gefahr, die Gefahrenlage falsch einzuschätzen und infolgedessen sich nur auf ein statisches mentales Sicherheitsmodell zu stützen. Indem die Entscheidungsträger konsequent an ihrem mentalen Sicherheitsmodell festhielten, überraschte sie am Ende die Tatsache, dass sich der Angriffsvektor um sie herum schnell veränderte, was schließlich dazu führte, dass die kritischen Dienstleistungen zur Aufnahme, Diagnostik, Therapie und Pflege des Krankenhauses für mehrere Tage nicht mehr aufrechterhalten werden konnten.

Diese Ausführung zeigt, dass ein reines Patchen der Systeme ohne eine genauere und spezifische (systembezogene) Analyse von Sicherheitslücken kein sachdienliches und ganzheitliches Schutzkonzept der Systeme darstellt. So kam Boyd zu dem Schluss, dass Organisationen, die nicht mit ihrer Außenwelt oder Umwelt kommunizieren, folglich auch keine aktuellen und zielgerichteten Informationen oder neue Informationen über ihre Umwelt und Umgebung erhalten (zweiter Hauptsatz der Thermodynamik) und sich infolgedessen wie ein geschlossenes System verhalten. So wie geschlossene Systeme in der Natur eine zunehmende Entropie oder Unordnung aufweisen, so weisen auch Organisationen eine geistige Entropie oder Unordnung auf, da sie von der Außenwelt und neuen Informationen abgeschnitten sind. Innerhalb der sicherheitstechnischen Betrachtung kann ein mangelhaftes Lagebewusstsein die Folge sein, das möglicherweise zu fatalen Fehlern und Folgen führen kann (vgl. Boyd, 1976, S. 6).

So verhält sich auch ein ICS-Netzwerk, welches entweder eine konsequente isolierte interne Betrachtung verfolgt oder aber auch die eingehenden externen Informationen nicht adäquat mit den internen Informationen verbindet und auswertet. Der isolierte Netzwerkanalytiker hat wahrscheinlich eine Vorstellung oder ein Sicherheitsmodell davon, welche Cyberrisiken, Schwachstellen und Gefährdungen existieren und welches Ausmaß sie verursachen können, aber die Gefahrenlage hat sich seit der letzten Beurteilung grundlegend geändert. Da der Netzwerkanalytiker weiterhin mit seinem veralteten mentalen Muster gegen eine sich verändernde Gefahrenlage arbeitet, sind Unsicherheiten, Inkonsistenz und Systementropie die natürliche Folge.

Unsicherheit entsteht oft auch dadurch, dass Organisationen interne Prozesse betrachten und somit ihr Handeln auf das „Bekannte“ stützen. Der argumentative Kernpunkt von Boyd, warum Ungewissheit und Inkonsistenz im Überfluss vorhanden ist, ist, dass Organisationen oft vertraute mentale Muster anwenden, die in der Vergangenheit funktioniert haben. Diese adaptive Übertragung auf VM und IRM-Prozesse findet auch dann statt, wenn diese Netzwerkanalytiker versuchen, neue Probleme und Herausforderungen mit alten und statischen Sicherheitsmodellen zu lösen. Angesichts einer sich verändernden Realität am Gewohnten festzuhalten, beschreibt das sogenannte „Mann-mit-Hammer-Syndrom“. Indem Boyd diese beiden o. g. Prinzipien umformulierte, um eine umfassende Sicht auf die Welt und ihre Umgebung zu erhalten, kam er zu dem Schluss, dass genauere Beobachtungen nur objektabhängig gemacht werden können. Daraus ergibt sich instinktiv die Gefahr, sich auf ein Kernobjekt oder einen Beobachtungsgegenstand zu konzentrieren und folglich auf ein einziges mentales Denkmodell zurückzufallen (vgl. Boyd, 1976, S. 3). So ist es auch bei Betreibern technischer Basisinfrastrukturen, die mit einem oder zwei statischen Sicherheitsmodellen im VM und IRM-Bereich arbeiten. In dem Boyd die Prinzipien auf eine operative und ausführbare Ebene konzeptualisierte und diese auf ein Entscheidungsunterstützungsmodell übertrug, verfeinerte er die OODA-Schleife, um einen dynamischen Rahmen dafür zu schaffen, damit Entscheidungsträger und Strategen die internen und externen relevanten Informationen beobachten, orientieren und interpretieren können, um sachdienliche Entscheidungen treffen zu können.

5.4.2 Modifizierte OODA-Schleife

Die modifizierte OODA-Schleife übernimmt die Logik der ursprünglichen Konzeption von Boyd, verändert jedoch die drei entscheidenden Phasen: Beobachten, Orientieren und Entscheiden, um die spezifischen Aspekte des Kohärenzmodells in die OODA-Schleife zu integrieren (vgl. Koza, 2023, S. 108 | Koza, 2022a, S. 2865 | Koza, 2022b, S. 55). Schnelligkeit ist nur eine Komponente eines Entscheidungsprozesses. Qualität, bzw. Präzision ist eine zweite Komponente. Wie stehen diese beiden Komponenten in Wechselwirkung zueinander? Wird das Heisenbergsche Unschärfeprinzip auf diese beiden Komponenten übertragen werden, so kann postuliert werden, dass eine isolierte Konzentration auf schnelle Entscheidungen zu einer schlechteren Qualität führt. Die Präzision einer Entscheidung nimmt daher ab, wenn die Geschwindigkeit zunimmt. Es gibt jedoch eine dritte Komponente. Neben der Geschwindigkeit und der Präzision der Entscheidungsfindung spielt das Timing (d.h. der genaue Zeitpunkt, zu dem eine Entscheidung getroffen wird, eine wichtige Rolle (vgl. Meilinger, 2017, S. 93-94 | Qiong, 2017, S. 18-28 | Osinga, 2007, S. 197)

Innerhalb dieses komplexen Themenfeldes des Kohärenzmodells spielen alle drei Komponenten eine entscheidende Rolle. Während die Entscheidungsgeschwindigkeit wichtig ist, um bspw. korrektive Maßnahmen einzuleiten, welche das Ausmaß der Schäden eingrenzen und minimieren sollen, liegt der Schlüssel zum effizienten Handeln im Sinne der Informationssicherheit nicht darin, schneller zu entscheiden, sondern die Entscheidungen zum richtigen Zeitpunkt mit der richtigen Qualität zu treffen, um präventiv dafür zu sorgen, dass die Eintrittswahrscheinlichkeit und der Schaden eines Ereignisses deutlich reduziert werden. In diesem Sinne bestreben wir die Fähigkeit agieren und reagieren können.

ICS-Umgebungen sind volatil, ungewiss und komplex. Um die Sicherheit und Nachhaltigkeit einer solchen ICS-Umgebung zu gewährleisten, müssen effiziente und richtige Entscheidungen getroffen werden. Die Qualität und das Timing von Sicherheitsentscheidungen in Bezug auf CVE-Bewertungen und Priorisierungen werden jedoch von derzeitigen Modellen nicht auf praktische, dynamische und effiziente Weise dargestellt.

Die OODA-Schleife repräsentiert allerdings mehr als einen Entscheidungsprozess und enthält mehr Elemente für den Sieg als Informationsüberlegenheit und Geschwindigkeit. Nach Boyds Theorie vernachlässigt eine falsche Auslegung der OODA-Schleife wesentliche Merkmale: Die Entwicklung, Aufrechterhaltung und Umgestaltung der eigenen Orientierung im Bereich der Informationssicherheit. Zunächst ist Geschwindigkeit bei einer Entscheidung, oder besser gesagt das Tempo, nicht zielführend, wenn auf eingehende Informationen nicht angemessen reagiert werden kann oder die Ereignisse falsch interpretiert werden. Die Orientierung prägt die Art und Weise, wie mit der ICS-Umwelt interagiert wird. Die Orientierung bestimmt, wie und was beobachtet, entschieden und gehandelt wird. Die Orientierung wirkt sich in diesem Zusammenhang vorwärts und rückwärts aus und ist die Schlüsselphase in der modifizierten OODA-Schleife. Nachhaltige, objektive und nach Faktenlage getroffene Entscheidungen und Behebungsmaßnahmen erscheinen weniger wirksam, wenn die Beobachtungen aufgrund einer unzureichenden Orientierung erfolgen (vgl. Boyd, zitiert nach Hammond, 2018, S. 320).

Die Orientierung setzt sich im Sinne des VM aus der Erfahrung und den sich entfaltenden Gefahrenumständen im ICS-Umfeld zusammen. Die Orientierung wird durch das Zusammenspiel dieser Faktoren geprägt. Sie ist der genetische Code eines Informationssicherheitsorganismus oder einer Organisation. Für jedes Entscheidungskonzept ist die Orientierung demzufolge der Schwerpunkt. Um Vorhersehbarkeit zu vermeiden und die Anpassungsfähigkeit an eine Vielzahl von Herausforderungen und Gefahrensituationen zu gewährleisten, reicht es nicht aus, nur eine einzige Orientierung, ein einziges Denkmuster, ein einziges Reaktionssystem wie reines „Patchen“ zu besitzen, um allen operativen Eventualitäten wirksam entgegen treten zu können (vgl. Boyd, zitiert nach Hammond, 2018, S. 384).

Es ist daher wichtig, über ein Repertoire an objektiven Orientierungsmustern zu verfügen und die Fähigkeit zu besitzen, je nach Situation das richtige Muster nach der Kritikalität von Zeit und der Ausfallfolgen auszuwählen und der Gefahrensituation gerecht zu werden. Um die Reaktionsvielfalt aufrechtzuerhalten zu können, sollte bei der Erstellung von Orientierungsmustern eine gewisse objektive Vielfalt eingebaut werden. Dies kann erreicht werden, indem der Netzwerkanalytiker und Entscheidungsträger mit unterschiedlichem Hintergrund und Erfahrung einbezieht und sie als Gruppe mit unterschiedlichen Situationen konfrontiert.

Boyd ist sich darüber im Klaren, dass bei der Auswahl von Personen in der Entscheidungsebene und auch in der operativen Handlungsebene, sehr vorsichtig entschieden werden muss (vgl. Boyd, zitiert nach Richards/Spinney, 2012, S. 1). Dieses Konzept erfordert wiederum eine gemeinsame Sichtweise, da die Einheiten sonst auf völlig unerwartete Weise reagieren könnten. So spielt eine grundlegende objektive Entscheidungsbasis eine zentrale Rolle, mit dessen Hilfe die getroffenen Entscheidungen transparent, nachvollziehbar, reproduzierbar und objektiv generiert werden können. Ohne die Fähigkeit zur ordnungsgemäßen Kommunikation und einer objektiven Entscheidungsgrundlage übermitteln die isolierten und/oder personenabhängigen Entscheidungen widersprüchliche, unvollständige, inkonsistente Ergebnisse, die möglicherweise zu fatalen Fehlern (Konzentration auf FP) und infolgedessen zu ineffizienten Ressourcenallokationen führen. Dadurch wird einem Entscheidungsträger die Fähigkeit genommen, sich ein ausgewogenes Urteil über die Sicherheitslücken und den daraus folgenden Beeinträchtigungen zu bilden. Boyd bezeichnet dies als eine Situation, in der ein Entscheidungsunterstützungs- und Kontrollsystem isoliert nach innen gerichtet ist. Eine solche Situation führt immer zu ineffizienten Entscheidungen, da eine Vielzahl an zur Verfügung stehenden Informationen nicht miteinander kombiniert werden kann, um daraus wertvolles Wissen generieren zu können (vgl. Boyd, 1976, S. 4 f.).

Boyd plädiert im Zusammenhang mit der Orientierung an die Notwendigkeit über ein Repertoire relevanter objektiver Schemata zu verfügen, die mit der Fähigkeit verbunden ist, dieses vor und während Beobachtungen und Orientierungen zu validieren, um eine gewisse Flexibilität auf sich ständig verändernde Gefahrensituationen entwickeln zu können (vgl. Boyd, 1976, S. 6 f.). Diese Perspektive ist vor allem in sich schnell verändernden CVE-Informationsumgebungen relevant. So ist das Lernen eine wesentliche Voraussetzung zur effizienten CVE-Bewertung und Anpassungsfähigkeit.

Netzwerk- und Sicherheitsanalytiker können zwar sehr schnell auf sich entfaltende Ereignisse reagieren, aber wenn sie trotzdem immer wieder überrascht werden, sind sie offenbar nicht in der Lage gewesen, die Erkenntnisse aus wiederholten Beobachtungen und Handlungen in eine bessere Einschätzung der Gefahrenlage umzumünzen, d. h. sie haben nicht gelernt, sondern weiter nach bestehenden Orientierungsmustern, z. B. „reines Patchen“, gearbeitet. Entscheidend ist, existierende Systemeigenschaften und Entscheidungsstrategien zu überprüfen und diese ggf. rechtzeitig zu modifizieren. Ein wichtiger Aspekt in VM-Prozessen ist zudem die Fähigkeit, sich weiterzuentwickeln, anzupassen und zu lernen. So müssen die übergeordneten Entscheidungsträger in den zentralen VM-Einheiten den „Entscheidungsraum“ der untergeordneten operativen Mitarbeitenden gestalten, um durch einen gemeinsamen Bezugsrahmen und eine gemeinsame Ausrichtung in Form einer objektiven Bewertung- und Priorisierungsgrundlage miteinander verbunden zu bleiben. In Verbindung mit einer sich deckenden objektiven CVE-Bewertungsgrundlage und einem gleichen Verständnis über die Kritikalität der eingesetzten Soft- und Hardwarekomponenten in den ICS-Netzwerken, können alle VM-Prozessbeteiligten eine einheitliche Sprache entwickeln. Wenn jeder den Zweck der CVE-Bewertungsprozesse oder die Absicht des Entscheidungssystems klar versteht und darauf eingestimmt ist, ist eine explizite ausführliche Kommunikation über das Ziel hinaus für eine Verteidigungseinheit überflüssig. Aufgrund der gemeinsamen Sichtweise und Sprache ist klar, was zu tun ist und was von dem Entscheidungssystem erwartet werden kann, seien es strategische Verteidigungseinheiten, operative Verteidigungseinheiten oder Informationssicherheitsbeauftragte.

Das Setzen auf implizite Kommunikation und einem gemeinsamen Verständnis spart Zeit in der OODA-Schleife und macht eine detaillierte und aufwändigere Kontrolle überflüssig. Dies gewährleistet die rechtzeitige und angemessene Anpassung des Systems als Ganzes. Es ermöglicht den operativen und dezentralen Verteidigungseinheiten somit, ihre Umgebung zu erkennen und die getroffenen CVE-Bewertungen und -Priorisierungen folglich nachvollziehen zu können. Die höheren Entscheidungsebenen können so die Grenzen und die Richtung vorgeben, ob eine CVE als TP zu beheben ist und in welchem zeitlichen Rahmen die notwendigen Behebungsmaßnahmen (nicht nur Patchen, sondern auch Abschirmen des Dienstes, Einführung von Workaround-Lösungen bis hin zu Deaktivierung des Dienstes oder Neukonfiguration) erfolgen müssen. Damit ist der Spielraum für die unteren operativen Verteidigungsebenen definiert, sodass diese die Möglichkeit erhalten die anfallenden CVE nach der eigenen Kapazität, aber auch nach der Kritikalität von Zeit und der Ausfallfolgen zu beheben. Grundsätzlich plädiert Boyd jedoch für laterale Beziehungen und die Vermeidung eines hierarchischen Systems von oben nach unten. So muss ein VM-Prozess zur Bewertung und Priorisierung von CVE sowohl einen Top-Down-, Lateral- als auch Bottom-Up-Prozess darstellen (vgl. Osinga, 2007, S. 170). So kann eine ständige offene Kommunikation in beide Richtungen integriert werden. So soll eine in sich konsistente Kommunikationsphilosophie entwickelt werden, nach der man in der Lage ist, sich besser und schneller an sich verändernde Gefahrensituationen anzupassen, aus diesen zu lernen. Die offene Kommunikation ist für den Erfolg der modifizierten OODA-Schleife unerlässlich. So kann die Auftragstaktik für die Entscheidungsträger zur Bewertung und Priorisierung der CVE neu formuliert werden.

Die modifizierte OODA-Schleife definiert diese Taktik der zentralen Entscheidungsträger zur CVE-Bewertung und Priorisierung als eine organisationale Aufgabe, in der sichergestellt wird, dass sich alle zentralen und dezentralen Verteidigungseinheiten innerhalb der ICS-Netzwerke anpassen können, während sie sich als eine homogene Verteidigungseinheit in eine gemeinsame Richtung bewegen. Nach Boyd stellt diese offene Kommunikationsphilosophie sicher, dass Verteidigungseinheiten auf allen Ebenen ein ausreichendes und zielführendes Maß an Interaktion mit ihrer ICS-Umgebung aufrechterhalten können. Im abstrakten Sinne handelt es sich um einen selbstkorrigierenden Mechanismus, ähnlich wie Mechanismen aus dem PDCA-Zyklus, die durch selbstkorrigierende Maßnahmen angetrieben werden (vgl. Osinga, 2007, S. 89 f.). Im nachfolgenden Bild 35 werden die einzelnen Phasen der modifizierten OODA-Schleife im Kontext des Kohärenzmodells illustriert. Die modifizierte OODA-Schleife überträgt die Logik der OODA-Schleife von Boyd, ändert jedoch die drei entscheidenden Phasen Observe, Orient und Decide. Diese werden um spezifische Aspekte des Kohärenzmodells ergänzt und in die OODA-Schleife integriert (vgl. Koza, 2022a, S. 2865 | vgl. Koza, 2023, S. 108 (eigene Übersetzung)).

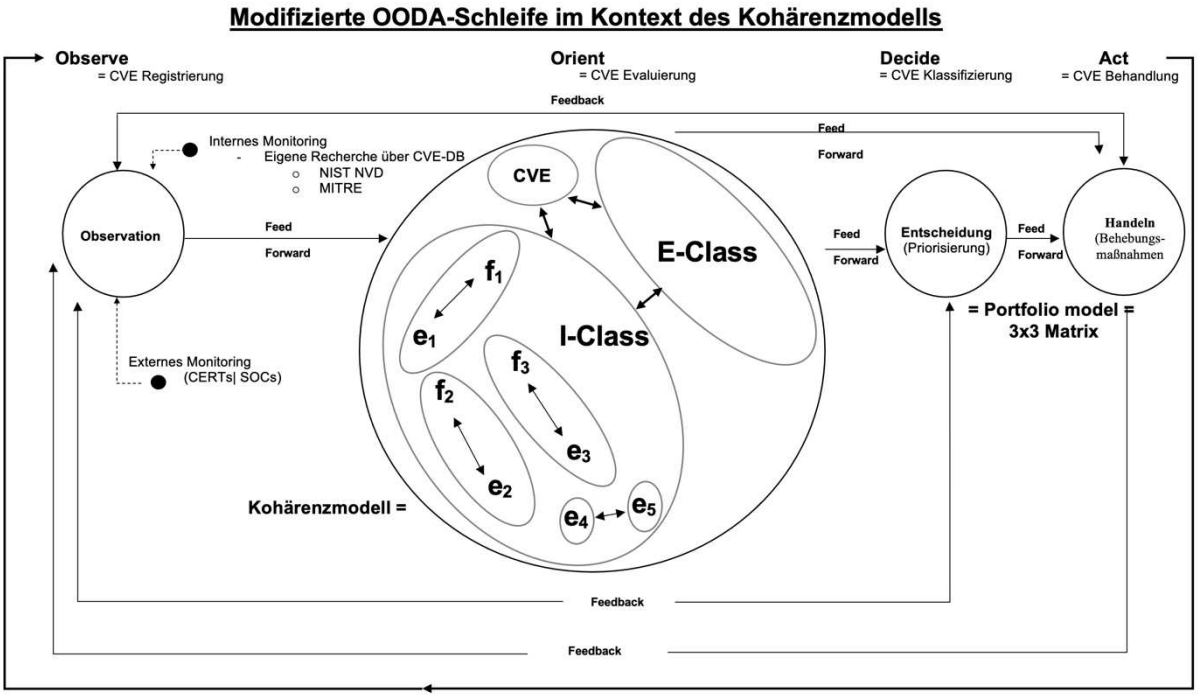


Bild 35: Modifizierte OODA-Schleife im Kontext des Kohärenzmodells (Quelle: In Anlehnung an Koza, 2023, S. 109 | Koza, 2022a, S. 2865 | Koza, 2022b, S. 55 (eigene Übersetzung))

Die erste Modifikation findet in der Phase „Observe“ statt und erfolgt durch die Integration der Prinzipien des Situationsbewusstseins. Die „Observe“ Phase ist ein ereignisgesteuerter Prozessschritt, welcher auf ständig wechselnde Umstände und unvollkommene Informationen reagiert. Damit gewinnt diese Phase eine essenzielle Rolle für die VM-Prozesse. Mit der Phase „Observe“ wird der Versuch unternommen gegen den zweiten Satz der Thermodynamik zu wirken und diesen möglicherweise zu überwinden, indem laufend neue Informationen über sich verändernde ICS-Umgebungen und der Cybergefahrenlage durch CVE und Sicherheitslücken gesammelt und dynamisch in die Entscheidungsfindungsprozesse integriert werden (vgl. Koza, 2023, S. 108 | Koza, 2022a, S. 2865 | Koza, 2022b, S. 55).

Dabei wird das Spektrum der CVE-Informationsgewinnung in einem offenen System abgebildet, um die Cybersicherheitsingenieure in die Lage zu versetzen, mit der Vernetzung und Kombination der gewonnenen Informationen das relevante Wissen und Verständnis zu generieren, welches für die Bildung neuer Sicherheitsmodelle und Abwehrstrategien entscheidend ist (vgl. Koza, 2022a, S. 2865 | Koza, 2022b, S. 55).

Aus fachlicher Sicht ist die Präzisierung der Informationsgewinnungsquellen für eine effektive Beobachtung von großer Bedeutung. Hierfür definieren die beiden spezifischen Verfahren ISO/IEC 27035 und NIST SP 800-61 eine Reihe von Beobachtungszielen und -Instrumenten, welche als effiziente Werkzeuge zum „Detect“ bereits ihre Feuertaufe in der Praxis überstanden haben. Somit werden die zwei Phasen „Detection and Reporting“ der ISO/IEC 27035 und „Detection and Analysis“ der NIST SP 800-61 in die Phase „Observe“ integriert.

Der Zweck dieser Integration beruht auf der Tatsache, dass die in den spezifischen Standards konzipierte Vorgehensweise die State of the Art im organisatorischen Bereich des VM und IRM darstellt. Die Integration der bereits bestehenden Konzepte als Best Practices ermöglicht zum einen, dass die modifizierte OODA-Schleife mit einem wissenschaftlich und praktisch erprobten Vorgehen arbeitet und zum anderen sich die Transformation der bestehenden Prozesse in die OODA-Schleife vereinfachen lässt, insbesondere für Organisationen, die ihr VM und IRM nach diesen Prinzipien implementiert haben. Primär wird die „Observe“ Phase als eine laufende Überwachungsphase gesehen, in der Cybersicherheitsingenieure und Entscheidungsträger dazu aufgefordert werden, zielgerichtete Informationsgewinnungsquellen zu selektieren. Dabei reicht es oft nicht aus, nur interne Netzwerkanomalien und Unregelmäßigkeiten über IDS, Intrusion Prevention Systeme oder Security Information and Event Management-Lösungen zu implementieren. Diese Echtzeitdatenverkehrsüberwachungssysteme sind mehr als komplementäre Überwachungstechnologien zu verstehen, deren Zielsetzung in der kontinuierlichen Überwachung und Erkennung von netzwerkbasierten und signaturbasierten Angriffen verankert ist. Hierdurch erhalten die Cybersicherheitsingenieure die Möglichkeit bei Erkennung von Anomalien eine Echtzeitreaktion zu initiieren und sofortige korrektive Maßnahmen zur Schadensbegrenzung einzuleiten. Im Gegensatz dazu ist die Gewinnung von globalen Informationen über mögliche Schwachstellen und Sicherheitslücken eine präventive Maßnahme, um die Ausnutzung einer Schwachstelle erst gar nicht geschehen zu lassen. Hierbei sollten Betreiber technischer Basisinfrastrukturen ihre Informationsgewinnungsquellen diversifizieren, indem diese sich bspw. an spezifische CERT-Einheiten (z. B. CERT-Bund, dCERT, Siemens ProductCERT) sowie an Herstellerprozesse zur Behandlung und Offenlegung von Schwachstellen und an die globalen CVE-Datenbanken anbinden, um gezielte und effektive externe Informationen über CVE und Sicherheitslücken zu erhalten, die ihre ICS-Umgebung betreffen. Die Diversität der Informationsgewinnungsquellen erlaubt den Anwendern in der „Observe“-Phase ihren Fokus gleichzeitig zu spezifizieren und zu vervielfältigen und sich somit auf die Gefahren zu konzentrieren, die die Unternehmensrealität betreffen. Die Wahrnehmung von gezielten Informationen über Sicherheitslücken kann als eine Fähigkeit gesehen werden, Informationen über geeignete Kanäle aktiv aufzunehmen, zu verarbeiten und diesen einen Sinn zu verleihen. Dieser Prozess ermöglicht, die Gefahrensituationen individuell zu interpretieren.

Das Ziel der „Observe“-Phase liegt darin, vollständige und konsistente Informationen über existierende Sicherheitslücken zu gewinnen. Hierfür sollte daher zunächst eine Art Scanning der eingesetzten Soft- und Hardwarekomponenten erfolgen, um bestimmen und dokumentieren zu können, welche Technologien, Softwarekomponenten, in welcher Version, Edition und von welchem Hersteller eingesetzt werden. Die Aufnahme und Identifizierung der eingesetzten Technologien und Softwarekomponenten hilft den Anwendern die CERT-Meldungen bspw. ICS-spezifisch zu customizen und somit nur die Meldungen zu erfassen, die auch genau die Sicherheitslücken in den von der Organisation eingesetzten ICS-Komponenten betreffen. Bei diesem Vorgehen in der „Observe“ Phase sollten auch die Entscheidungsträger die grundlegende Entscheidung treffen, ab welchem CVE-Basis-Score die Sicherheitslücken in das interne Bewertungs- und Priorisierungsverfahren eingebettet werden sollen.

Alle CVE mit einem Basis Score 7+ sollten in der Regel selektiert und in das interne Bewertungs- und Priorisierungsverfahren integriert werden. Aber auch hier spielen die internen Ressourcenkapazitäten eine wesentliche Rolle.

Nach dem die Entscheidungsträger in den ICS-Netzwerken ihre ICS-spezifischen Technologien und Softwarekomponenten ausgewählt und die grundlegende Entscheidung über die CVE-Integration getroffen haben, kann in der „Observe“ Phase eine gezielte Aufnahme von CVE erfolgen, die eine reelle Gefahrensituation für die ICS-Netzwerke darstellen. Allerdings bedeuten die gewonnenen Informationen ohne ein adäquates Urteilsvermögen wenig, auch wenn diese gezielt und konsistent vorliegen. Diese Postulierung basiert auf der Prämisse, dass mehr Informationen und Daten sowie Kontrolle nicht zwangsläufig zu besseren Entscheidungen führen, sondern ein ausgeprägtes Urteilsvermögen, das zum Erkennen von Mustern und nachhaltigem Wissen führt, in der Lage ist, aus den bestehenden Informationen Wissen nachhaltige und effiziente Entscheidungen generieren zu können.

Um die gewonnenen CVE-Informationen zwecks einer effizienten Entscheidungsfindung nutzen zu können, werden die globalen Informationen, die über das interne und externe Monitoring gesammelt wurden, mit den internen objektiven und systembezogenen Informationen verknüpft. Die internen objektiven Informationen werden durch die intrinsischen Subdeterminanten repräsentiert. Die Verknüpfung der internen und externen Informationen erfolgt in der „Orient“ Phase durch die Integration des Kohärenzmodells. Die CVE-Informationen werden in dieser Phase zunächst der ersten Faktorgruppe „I-Class“ zugeordnet. Dabei werden die intensiven und extensiven Subdeterminanten als Orientierungs- (Bewertungs-) Kriterien zur Bewertung des Schadensausmaßes der integrierten CVE einbezogen. Die zweite Faktorgruppe „E-Class“ umfasst die extrinsische Determinante, die als Orientierungs- (Bewertungs-) Kriterium zur Bestimmung der Wahrscheinlichkeit des Auftretens der integrierten CVE eingefügt wird.

So wird in der „Orient“ Phase mithilfe der Verknüpfung der externen CVE-Informationen mit den internen Informationen der Weg für die objektive und faktenbasierte Bewertung und Priorisierung einer CVE vorbereitet. Die Ergebnisse werden anschließend durch das Portfolio mit einer 3 x 3 Matrix in der „Decide“ Phase visualisiert, um CVE-Behandlungsstrategien und die chronologische Reihenfolge der CVE-Behandlungen zu bestimmen. In der „Act“ Phase werden die erreichten Ergebnisse an die operativen Verteidigungseinheiten überreicht, die letzten Endes für die operative Beseitigung und Behebung der Sicherheitslücken gemäß der definierten Bewertungs- und Priorisierungsstrategie verantwortlich sind.

Um die Entscheidungsakzeptanz der operativen Verteidigungsebene zu sichern und eine kommunikative Brücke zwischen den Analytikern als strategische Verteidigungseinheiten und operative Systemadministratoren als operative Verteidigungseinheiten zu sichern, werden in der Orient-Phase sogenannte Orient-Workshops eingesetzt, um die standardisierten intrinsischen Subdeterminanten:

- Beeinträchtigungsgrad (e_1)
- Ausfallwahrscheinlichkeit (e_2)
- Funktionskritikalität (e_3)
- Exploit Code Maturity (e_4)
- Remediation Level (e_5)
- Portskritikalität (f_1) (mit Kohärenz zu e_1)
- Redundanzkritikalität (f_2) (mit Kohärenz zu e_2)
- Zonenkritikalität (f_3) (mit Kohärenz zu e_3)

gemäß der Klassifizierungsstufe aus den Kap. 5.3.2 bis 5.3.5 zu klassifizieren. Zur fachlichen Operationalisierung des Kohärenzmodells werden folgende Prozessschritte ausgeführt:

Tabelle 19: Prozessschritte zur Einbettung des Kohärenzmodells in die OODA-Schleife (Quelle: Eigene Darstellung)

Prozessschritte (PS)	Beschreibung
Orient	
PS 1: Bestimmung der Portskritikalität (f_1)	Innerhalb des PS 1 werden alle in den ICS-Netzwerken eingesetzten Ports identifiziert und nach dem Klassifizierungsschema aus Tabelle 8 klassifiziert. Jeder Port erhält gemäß seiner Kritikalitätsklassifizierung einen mathematischen Wert zwischen 1 und 3.
PS 2: Bestimmung der ergänzenden Portskritikalitäten (f_1)	Neben der Identifizierung und Klassifizierung der eingesetzten Ports, müssen auch weitere Eventualitäten berücksichtigt werden. Die erste Eventualität tritt dann auf, wenn keine ICS-Ports betroffen sind. Das kann mitunter dann der Fall sein, wenn die identifizierte CVE zwar einen bestimmten Port betrifft, dieser Port aber innerhalb des ICS-Netzwerks keine Anwendung besitzt oder vollständig deaktiviert ist. Hierbei wird die Deklaration „kein Port ist betroffen“ ausgewählt und dem Wert 0 zugeordnet. Eine zweite Eventualität bezieht sich auf die nicht netzwerkbasierten Angriffsvektoren, die lediglich über Insider Threats, also Innentäter ausgeführt werden können. Hierbei wird die Deklaration „Insider Threats“ ausgewählt und dem Wert 3 zugeordnet.

PS 3: Bestimmung der Redundanzkritikalität (f_2)	Innerhalb des PS 3 werden alle in den ICS-Netzwerken eingesetzten Systeme identifiziert und nach dem Klassifizierungsschema aus Tabelle 10 klassifiziert. Jedes System erhält gemäß seiner Kritikalitätsklassifizierung einen mathematischen Wert zwischen 1 und 3.
PS 4: Bestimmung der ergänzenden Redundanzkritikalität (f_2)	Neben der Identifizierung und Klassifizierung der eingesetzten Systeme, müssen auch weitere Eventualitäten berücksichtigt werden. Die erste Eventualität tritt dann auf, wenn keine ICS betroffen sind. Das kann mitunter dann der Fall sein, wenn die identifizierte CVE zwar ein bestimmtes System betrifft, dieses aber innerhalb des ICS-Netzwerk keine Anwendung besitzt oder vollständig innerhalb des segmentierten Büronetzwerks implementiert ist. Hierbei wird die Deklaration „kein System ist betroffen“ oder „nur Systeme des Büronetzwerkes sind betroffen“ ausgewählt und dem Wert 0 zugeordnet. Sollte jedoch keine strikte Netzwerksegmentierung zwischen dem ICS- und Büronetzwerk existieren, so muss die Deklaration „nur Systeme des Büronetzwerkes sind betroffen“ mit 3 bewertet werden, denn hierbei kann eine Kompromittierung des Büronetzwerkes eine unmittelbare Kompromittierung des ICS-Netzwerkes mit sich ziehen. Eine zweite Eventualität bezieht sich auf die mehrfache Betroffenheit von Systemen. Hierbei wird die Deklaration „multiple Systeme sind betroffen“ ausgewählt und dem Wert 3 zugeordnet.
PS 5: Bestimmung der Zonenkritikalität (f_3)	Innerhalb des PS 5 werden alle in den ICS-Netzwerken eingesetzten Zonen identifiziert und nach dem Klassifizierungsschema aus Tabelle 13 klassifiziert. Jede Zone erhält gemäß seiner Kritikalitätsklassifizierung einen mathematischen Wert zwischen 1 und 3.
PS 6: Bestimmung der ergänzenden Zonenkritikalität (f_3)	Neben der Identifizierung und Klassifizierung der eingesetzten Zonen, müssen auch weitere Eventualitäten berücksichtigt werden. Die erste Eventualität tritt dann auf, wenn keine ICS-Zonen betroffen sind. Das kann mitunter dann der Fall sein, wenn die identifizierte CVE zwar eine bestimmte Zone betrifft, diese aber innerhalb des ICS-Netzwerks keine Anwendung besitzt oder vollständig innerhalb des segmentierten Büronetzwerks eingebettet ist. Hierbei wird die Deklaration „keine ICS-Zone ist betroffen“ ausgewählt und dem Wert 0 zugeordnet. Sollte jedoch keine strikte Netzwerksegmentierung zwischen dem ICS- und Büronetzwerk existieren, so muss die Deklaration „keine ICS-Zone ist betroffen“ mit 3 bewertet werden, denn hierbei kann eine Kompromittierung des Büronetzwerkes eine unmittelbare Kompromittierung des ICS-Netzwerkes mit sich ziehen. Eine zweite Eventualität bezieht sich auf die mehrfache Betroffenheit von Zonen. Hierbei wird die Deklaration „multiple Zonen sind betroffen“ ausgewählt und dem Wert 3 zugeordnet.
PS 7: Identifizierung und Bestimmung der eingesetzten Technologien und Softwarekomponenten	Innerhalb des PS 7 werden alle in den ICS-Netzwerken eingesetzten Technologien und Softwarekomponenten identifiziert. Dieser Schritt erfolgt unter dem Motto: Kenne deine ICS-Umgebung. Hierfür müssen alle eingesetzten Software- und Hardwarekomponenten im Rahmen eines Assetmanagements sorgfältig aufgenommen und mit detaillierten Informationen (Hersteller, Version, Edition, patchfähig (manueller Patch oder automatisierter Patch), IP, Netzbereich, Netzmaske, Verantwortlichkeitsbereich) dokumentiert werden. Hierbei müssen die Systeme identifiziert werden, die als obsolete Systeme zu definieren sind, und somit nicht patchfähig sind und unter Obsoleszenzmanagement weiterbehandelt werden sollen.

PS 8: Zyklische Revision (zeitgesteuert | ereignisgesteuert)	Alle identifizierten Ports, Systeme, Zonen sollten in turnusmäßigen Abständen neu evaluiert und ergänzt werden. Dieser Prozess kann jeweils in einem dreimonatigen Zyklus zeitgesteuert durchgeführt werden. Die zyklische Revision muss aber dann ausgeführt werden, wenn ein neues System, eine neue Softwarekomponente, Datenmigration, Systemintegration oder Neuinstallationen ausgeführt wird. In diesem Fall ist die zyklische Revision ereignisgesteuert.

Observe-Vorbereitung

PS 9: CERT-Anbindung (externes Monitoring)	Innerhalb des PS 9 muss eine aktive Verbindung zu einer speziellen CERT-Einheit zur Generierung von gezielten CVE-Meldungen hergestellt werden. Hierbei sind die Entscheidungsträger dann in der Lage, die Qualität und die Quantität der erforderlichen Informationen bedarfsgerecht zu bestimmen, indem sie die CVE-Meldungen angepasst an ihre im Prozessschritt 7 identifizierten ICS-Technologien und Softwarekomponenten generieren lassen. So erhalten die Entscheidungsträger die CVE-Meldungen, die für sie eine signifikante Rolle spielen.
PS 10: Hersteller-Anbindung	Neben einer spezifischen CERT-Anbindung sollten auch Anbindungen an die ICS-Hersteller sichergestellt werden, um gleichzeitig auch produktspezifische CVE-Informationen und Sicherheitslücken sowie explizite Handlungsempfehlungen und Abhilfemaßnahmen zu erhalten.
PS 11: Interne Recherche über CVE-Datenbanken (internes Monitoring)	Neben den Möglichkeiten zur automatisierten Generierung von CVE-Meldungen über CERT- und Hersteller-Anbindungen sollten auch manuelle Recherchen erfolgen, um vorhandene CVE-Datenbanken wie die NVD NIST eigenhändig nach Zusatzinformationen und Sicherheitslücken zu durchsuchen.
PS 12: Tägliche Überwachung	Um die identifizierten CVE fortlaufend beobachten zu können, sollten täglich Beobachtungszeiten eingeplant werden. Die täglichen Beobachtungszeiten dienen insbesondere der Revision der temporäreren CVE Metriken. Diese betreffen vor allem die Exploit Code Maturity e_4 und den Remediation Level e_5, die im Verlauf der Zeit unkritischer, aber auch kritischer werden können. Die tägliche Beobachtung der temporären CVE Metriken stellt zudem die Belastbarkeit und Zuverlässigkeit der durchgeführten Bewertungen sicher. Verändern sich die temporären CVE Metriken, so müssen die Bewertungsergebnisse evaluiert und ggf. neue Bewertungsprozesse ausgeführt werden.
PS 13: Strategische Entscheidung über CVE-Basis-Score zur Aufnahme	Bevor die operative Observe-Realtime durchgeführt werden kann, muss abhängig der internen fachlichen und personellen Ressourcenkapazitäten entschieden werden, ab welchem CVE-Basis-Score eine CVE zur Bewertung und Priorisierung eingebettet werden sollte. Eine 7+ Strategie kann als Durchschnittswert vorgeschlagen werden.

Observe-Realtime

PS 14: CVE-Registrierung	Innerhalb des PS 14 in der „Observe-Realtime“-Phase werden die automatisierten spezifischen CVE-Meldungen aufgenommen und dokumentiert. Hierbei ist unerlässlich, die CVE-Informationen sehr sorgfältig und präzise zu bestimmen. Durch die Zuordnung einer CVE zu den eingesetzten Technologien und Softwarekomponenten kann eine direkte Zuordnung der externen CVE-Informationen zu internen Informationen (betroffenes Asset, Port, System und Zone) gewährleistet werden.
PS 15: CVE-Zuordnung	Innerhalb des PS 15 in der „Observe-Realtime“ Phase werden die aufgenommenen globalen CVE-Informationen systembezogen spezifiziert. Hierfür erfolgen folgende Zuordnungen: Welcher Port ist durch die CVE betroffen? Welches System ist betroffen? Welche Zone ist betroffen? Wie ist die Exploit Code Maturity e_4 definiert? Wie ist der Remediation Level e_5 definiert?
PS 16: CVE-Schadensausmaßbewertung (***C***)	Während die oben aufgeführten Daten identifiziert und festgehalten werden, können die Angaben im Hintergrund der einzelnen Stufen aus der Orient-Phase PS 1 - PS 6 zugeordnet werden. Wird eine CVE einem Port zugeordnet, der in PS 1 mit dem Wert 3 klassifiziert ist, so wird dieser Wert aufgenommen und in die Berechnungsformel integriert. In derselben Analogie werden die weiteren Zuordnungen quantifiziert und in die Berechnungsformel aufgenommen. Hierdurch können die extensiven Subdeterminanten f_1, f_2 und f_3 objektiv bewertet werden. Durch die Beziehung zwischen $f_1 \rightarrow e_1$, $f_2 \rightarrow e_2$ und $f_3 \rightarrow e_3$, können die Werte der extensiven Subdeterminanten f_1, f_2 und f_3 automatisch auf die intensiven Subdeterminanten e_1, e_2 und e_3 übertragen werden. Hierdurch können die intensiven Subdeterminanten e_1, e_2 und e_3 objektiv bewertet werden. Zusätzlich hierzu werden die Angaben aus PS 15 von e_4 und e_5 ebenfalls mit aufgenommen und in die Berechnungsformel integriert. Im Anschluss kann die Summe dieser Additionsformel quantifiziert und den definierten I-Class-Stufen zur Bestimmung des Schweregrads einer CVE zugeordnet. Beispiel: **CVE: Aufnahme:** CVE-2021-44228 **CVE-Zuordnung:** Betroffener Port durch CVE-2021-44228: **TCP-Port 389** Betroffenes System durch CVE-2021-44228: **SCADA (Master Terminal Unit (MTU))** Betroffene Zone durch CVE-2021-44228: **Zone 4** Zuordnung des betroffenen Ports, der Systeme und Zonen zu der Wertung: Portskritikalität f_1 der TCP-Port 389 → **3** *Critical* Redundanzkritikalität f_2 des SCADA (MTU) → **2** *High* Zonenkritikalität f_3 der Zone 4→ **3** *Critical*

$f_1 = 3$
$f_2 = 2$
$f_3 = 3$

Übertragung der f_1, f_2 und f_3 – Wertungen auf e_1, e_2 und e_3:

$f_1 \rightarrow e_{1,\,so}\ e_1 = 3$
$f_2 \rightarrow e_{2,\,so}\ e_2 = 2$
$f_3 \rightarrow e_{3,\,so}\ e_3 = 3$

$e_1 = 3$
$e_2 = 2$
$e_3 = 3$

Bestimmung der $\mathbf{e_4}$ und $\mathbf{e_5}$ aus PS 15:

$e_4 = 2$
$e_5 = 3$

Integration in die Berechnungsformel:

$C = ((b_{extensive}) + (b_{intensive}))$
$C = ((f_1 + f_2 + f_3) + (e_1 + e_2 + e_3 + e_4 + e_5))$

$C = ((3 + 2 + 3) + (3 + 2 + 3 + 2 + 3)) = 21$

$C = (21)$

Bestimmung der Schadenklasse über I-Classes:

I-Class	Wertung	Einstufung	Gesamtgrenzbereich für erreichten C-Wert
I-Class 1	*1*	*Low*	[0, 8]
I-Class 2	*2*	*High*	[9, 16]
I-Class 3	*3*	*Critical*	[17, 24]

$C = (21)$ wird *I-Class 3* mit der Wertung 3 zugeordnet.

PS 17:

CVE-Eintrittswahrscheinlichkeit (*F*)

Im Anschluss der Bestimmung des CVE-Schadensausmaßes erfolgt die Bestimmung der CVE-Eintrittswahrscheinlichkeit, die entweder über den EPSS-Score oder CWE-Likelihood-Score abgebildet wird.

Beispiel:

CVE: Aufnahme: CVE-2021-44228

F = (EPSS-Score or CWE-Score)

CWE Likelihood Score: **High**

E-Class	Wertung	Einstufung	EPSS-Wertebereich	CWE-Wertebereich
E-Class 1	1	Low	$0 < E \leq 0{,}3$	Low (L)
E-Class 2	2	High	$0{,}3 < E \leq 0{,}6$	Medium (M), Default (D), Unknown (UK)
E-Class 3	3	Critical	$0{,}6 < d \leq 1{,}0$	High (H), Not applicable (NA)

F = High

Bestimmung der Eintrittswahrscheinlichkeitsklasse über E-Classes:

F = 3

F = 3 wird *E-Class 3* mit der Wertung 3 zugeordnet.

Observe-Decide-Realtime

PS 18:

Finale Bewertung der CVE

Nach Festlegung des CVE-Schadensausmaßes und der CVE-Eintrittswahrscheinlichkeiten werden die beiden erreichten Klassen I-Class und E-Class mithilfe des Portfoliomodells in eine 3 x 3 Matrix zur finalen Bewertung und Priorisierung integriert.

Beispiel:

CVE: Aufnahme: CVE-2021-44228

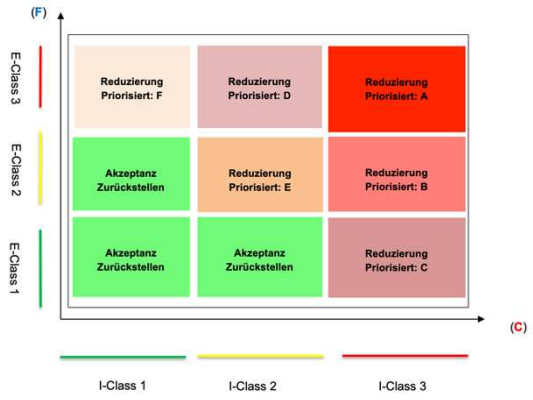
C = 21 wird *I-Class 3* mit der Wertung 3 zugeordnet.
F = 3 wird *E-Class 3* mit der Wertung 3 zugeordnet.

CVE = (C) x (F)
CVE = (I-Class) x (E-Class)

CVE= F-Value = (3) X (3) = 9

I-class	E-class	F-Value	Behandlungsstrategie	Kategoriezuordnung	Priorisierungsstrategie
1	1	1	Akzeptanz	True Negatives (*TN*)	Zurückstellen
1	2	2	Akzeptanz	True Negatives (*TN*)	Zurückstellen
1	3	3	Reduzierung	True Positives (*TP*)	F
2	1	2	Akzeptanz	True Negatives (*TN*)	Zurückstellen
2	2	4	Reduzierung	True Positives (*TP*)	E
2	3	6	Reduzierung	True Positives (*TP*)	D
3	1	3	Reduzierung	True Positives (*TP*)	C
3	2	6	Reduzierung	True Positives (*TP*)	B
3	3	9	Reduzierung	True Positives (*TP*)	A

CVE-2021-44228 wird als TP definiert und der Prio-Klasse A zugeordnet.



	CVE-2021-44228 muss gemäß der Priorisierungsklasse und aufgrund seines Schweregrades bezugnehmend auf die Ausfallfolgen- und Zeitkritikalität unverzüglich in den ersten 24 Stunden beseitigt bzw. behoben werden. ▪ **A** (in zeitlicher Relation sollte die Behebung als Erstes ausgeführt werden) *****_Dieses Beispiel wird in Kap. 5.5.3. mithilfe des Prototyps IRET zur besseren Veranschaulichung als Anwendungsbeispiel näher betrachtet._
Observe-Act-Realtime	
PS 19: Beseitigung der Schwachstelle	Bevor die Entscheidungs- und Priorisierungsergebnisse den operativen Verteidigungseinheiten mitgeteilt werden, werden weitere signifikante Informationen über mögliche Lösungsansätze aufgeführt. Dazu gehört: - Ob das betroffene System patchbar ist. - Ob ein Restart nach der Installation der Sicherheitsupdates notwendig ist. - Ob das Patchen automatisiert oder manuell ausgeführt werden muss. - Wie viele operative Verteidiger hierfür vonnöten sind, - Wie viele Stunden für die Behebung vonnöten sind, - Wie viel die Abhilfemaßnahmen kosten (personelle Kosten, Softwarelizenzen und Hardware- oder Softwareanschaffungskosten) - Wie hoch der monetäre Schaden ist, der durch Untätigkeit und durch die Ausnutzung der Sicherheitslücke entsteht, sowie die - qualitative Bewertung, die zusätzlich als Empfehlung in die Entscheidungsfindung eingebettet wird.
PS 20: Beseitigung der Schwachstelle	Die Entscheidung zur unverzüglichen Beseitigung bzw. Behebung der Sicherheitslücke wird den zuständigen operativen Verteidigungseinheiten mitgeteilt. Die Behebungs- bzw. Abhilfemaßnahmen werden überwacht und der Abschluss der Sicherheitslücke wird dokumentiert.
Der Prozess beginnt wieder bei **PS 14** und wird laufend fortgesetzt.	

5.4.3 Notwendige Voraussetzungen zur Anwendung des Kohärenzmodells

Unter folgenden Annahmen kann das Kohärenzmodell angewendet werden:

a) Die relevanten Stammdaten zur Identifizierung und Klassifizierung der acht Sub-Determinanten müssen in adäquater Form vorliegen.

b) Die Stammdaten müssen gemäß dem angegebenen Schema in das Kohärenzmodell sowie in das Berechnungsmodell eingebettet sein.

c) Zur adäquaten Priorisierung müssen die individuellen Behandlungs- und Priorisierungsstrategien übereinstimmend festgelegt sein.

5.5 Ausführung des Kohärenzmodells

5.5.1 Funktionen des Prototyps

In diesem Abschnitt werden Ergebnisse aus der vierten und fünften Forschungsphase des Methodenaufbaus vorgestellt. IRET übernimmt als Prototyp die Aufgabe der Realisierung und Operationalisierung des Kohärenzmodells und der modifizierten OODA-Schleife und versucht dieses im Sinne einer effizienten Lösung im industriellen Umfeld einer technischen Basisinfrastruktur in der Energiewirtschaft zwecks Evaluierung und Machbarkeitsvalidierung zu implementieren. Um die zuvor dargestellten Prozessschritte realisieren zu können, muss eine Vielzahl an Funktionen konzipiert werden, um auch die weiteren entscheidenden Ziele (Bild 20) erreichen zu können. IRET wurde mit der Programmiersprache Visual Basic for Application (VBA) mit Makroprogrammierung entwickelt. Diese Entwicklung ist das Ergebnis eines pragmatischen Ansatzes, um lange Entwicklungszeiten des Prototyps zu verkürzen und gleichzeitig die Integration des Prototyps in der Industrie zu erleichtern. Betreiber technischer Basisinfrastrukturen besitzen in der Regel Lizenzen für Microsoft (MS)-Office-Produkte und benötigen für die Integration von IRET keine zusätzlichen Softwarelizensierungen. Zudem ist die Handhabung von IRET in dieser Form benutzerfreundlich und selbsterklärend, da auch eine Vielzahl der Anwender bereits grundlegendes Wissen im Umgang und der Interaktion mit MS-Office-Produkten hat. Ein weiterer Vorteil, der aus dem Sicherheitsblickwinkel eine wesentliche Rolle spielt, ist er „Stand-alone“-Betrieb von IRET, da der Prototyp in diesem Format eigenständig, ohne weitere Schnittstelleprogrammierungen oder weitere Anbindungen an Datenbanken mit dem Anwender interagieren kann und somit auch lokal installiert und ausgeführt werden kann. Zu diesem Zweck bietet IRET zwei visuelle Interaktionsoberflächen an, um die Zugriffsrechte zwischen den IRET-Anwendern und den Administratoren voneinander zu separieren. Im Frontend stellt IRET den Anwendern insgesamt 35 Funktionen über unterschiedliche Dialogfenster zur Verfügung. Die Navigation wird über die „Startseite“ dem „Dashboard“ sowie über die Navigationsbar realisiert und bietet den Anwendern je nach Zielsetzung eine Orientierung durch die Anwendung. Die nachfolgende Tabelle 20 illustriert die auf der Dashboard-Dialogoberfläche implementierten Funktionen, die in IRET eingebettet sind.

Tabelle 20: IRET-Dashboard-Dialogfenster und die dazugehörigen Funktionen (Quelle: Eigene Darstellung)

Dialogfenster: Dashboard

Funktionen	***Zuordnung zu Prozessschritten | Prozessbeschreibungen***
Observe	PS 14 bis PS 17
Orient	PS 1 bis PS 8
Decide	PS 18
Act	PS 19 und PS 20
Monitoring	PS 20 sowie Entwicklung von Key-Performance-Indikatoren
Reporting	Kommunikationsprozesse (Management Summary und ISMS-Report)
IRET Guidance	Link zum Benutzerhandbuch
Leave	Beenden der Applikation

Die übergeordneten Hauptfunktionen werden durch weitere Unterfunktionen verfeinert, die wie folgt aufgelistet werden können:

Tabelle 21: Übersicht der wichtigsten Funktionen in IRET (Quelle: Eigene Darstellung)

Dialogfenster: ***Observe***

Funktionen	***Funktionsbeschreibung (inklusive Subfunktionen)***
Add CVE	***@Add CVE:*** Wenn der Anwender eine CVE hinzufügen möchte, werden essenzielle Informationen abgefragt. Diese werden in zwei Kategorien unterteilt. Innerhalb der Kategorie *Basic Metrics* werden grundlegende Informationen gefordert wie bspw. die Komplexität des Angriffs. Die zweite Kategorie *Temporal Metrics* verwendet Informationen, welche sich mit der Zeit ändern können, wie bspw. der Impact Score, darunter auch e_4 und e_5. Um den Eintrag zu speichern, muss jedes mit * gekennzeichnete Feld (Pflichtfeld) ausgefüllt werden. Über den „Save and Continue" Button kann der Eintrag abgeschlossen und fortgeführt werden. CVE werden über die CVE-ID als Primary Key in der IRET Database abgespeichert. Zurück kann der Anwender mithilfe des „Back" Buttons. Dann verwirft der Anwender jedoch die eingetragenen Informationen. Klickt der Anwender nun auf „Save and Continue" müssen im nächsten Schritt die CVE-Metadaten angegeben werden. ***@CVE Metadata:*** Im nächsten Schritt kann der Anwender die Metadaten für den zuvor eingetragenen CVE eingeben. Das **Pflichtfeld „CVE Description"** muss dabei zwingend ausgefüllt werden, damit der Anwender fortfahren kann. Hier hat der Anwender ebenfalls die Möglichkeit, zum Dashboard zu gelangen. Dann werden die zuvor gespeicherten Informationen hinterlegt. Klickt der Anwender auf „Save & Continue" werden die Metadaten gespeichert und der Anwender gelangt zur Evaluation des CVE. ***@Evaluate CVE:*** In diesem Dialogfenster werden die zuvor eingegeben Daten in „CVE-Information" konsolidiert wiedergegeben. Im Folgenden hat der Anwender die Möglichkeit, die betroffenen internen Ports, ICS-Systeme und die Netzwerkzonen, die dieser zuvor in der Orient-Phase festgelegt hat, über ein Drop-down Menü auszuwählen. IRET übernimmt die Angaben (e_4, e_5) sowie die Angaben zu den betroffenen Ports, Systemen und Zonen und ordnet diese automatisiert den definierten Port-, System- und Zonenkritikalitäten sowie dem Beeinträchtigungsgrad, der Ausfallwahrscheinlichkeit und Funktionskritikalität (f_1, f_2, f_3, e_3, e_4 und e_5) zu. Im Hintergrund ruft IRET die Logik des Kohärenzmodells und des Berechnungsmodells auf und rechnet das Schadensausmaß (*C*) automatisiert aus. Der Anwender kann ebenfalls „No port/system/zone is affected" auswählen, wenn die Schwachstelle keine internen Ports, Systeme oder Zonen betrifft. Über „Save and Continue" gelangt der Anwender auf die nächste Seite, wo alle relevanten Informationen übersichtlich aufgeführt werden. ***@Result of CVE Evaluation:*** Hier erhält der Anwender eine Übersicht über die angegebenen Informationen in „CVE Information" und „CVE Basic & Temporal Metrics". Unter „Incident results" ist der entsprechende Wert zum Schadensausmaß und die Einstufung des CVE-Schadensausmaßes angegeben, die von IRET automatisiert berechnet und der I-Class als Schadenklasse zugeordnet werden. Bei dem oben aufgeführten Beispiel ergibt sich ein Schadensausmaßwert „Incident-Wert" (Incident value) von 21 (8, 13) sowie eine Schadensausmaßklasse von 3, nach der eine Reduzierung der Sicherheitslücke empfohlen wird. Als Pflichtfeld muss der Anwender den erwartenden monetären Schaden bei der Ausnutzung der Sicherheitslücke quantifizieren und einen Wert zwischen 0 bis 1.000.000.000 € angeben. Über „Save and Continue with response evaluation" gelangt der Anwender auf die nächste Seite (Evaluate of Reponse).

@Evaluation of Response: In diesem Dialogfenster werden Angaben zur Response auf die CVE angegeben. Die mit * gekennzeichneten Felder sind Pflichtfelder. In diesen werden wichtige Angaben und Informationen für die operative Verteidigungsebene gemacht. Unter „CVE Information, CVE Basic & Temporal metrics“ und „Incident results“ werden die Ergebnisse des Dialogfensters „@Result of CVE Evaluation“ konsolidiert weitergegeben und aufgeführt. Hierbei müssen obligatorische Informationen über Systemeigenschaften, Patchmanagement und Kosten zu Abhilfe- und Beseitigungsmaßnahmen gemacht werden:

- Ist das betroffene System patchbar oder handelt es sich hierbei um ein obsoletes System ohne Patchfähigkeiten?
- Ist ein Restart nach dem Patchen vonnöten?
- Erfolgt das Installieren und Ausführen von Sicherheitsupdates manuell oder automatisiert?
- Wie viele Personen, mit wie vielen Stunden und mit welchem Stundensatz werden zur operativen Ausführung der Behebungsmaßnahmen benötigt?
- Sind neue Software-Lizenzen vonnöten, wenn ja, wie viel kostet die Anschaffung?
- Sind neue Hardware-Komponenten vonnöten, wenn ja wie viel kostet die Anschaffung?

Im Anschluss rechnet IRET die angegeben Kosten zur Maßnahmenbehandlung automatisiert aus und stellt dies gegenüber dem monetären Schadensausmaß. Zum Gelangen auf die nächste Seite muss der Anwender auf „Save and Continue with response evaluation“ klicken.

@CVE Prediction: In diesem Dialogfenster werden die Daten aus den vorherigen Dialogfenstern erneut konsolidiert weitergegeben. Zudem erfolgt hier die Einstufung des EPSS-Scores oder CWE Likelihood-Score zur Bestimmung der Eintrittswahrscheinlichkeit (*F*). Über das Drop-down-Menü können die passenden Angaben gemäß der Logik des Kohärenzmodells ausgewählt werden. Während dieser Angaben rechnet IRET die entsprechende E-Class zu dem angegebenen Eintrittswahrscheinlichkeitswert und speichert dies, wie auch alle anderen berechneten Werte, in die „IRET Database“. Bei dem oben aufgeführten Beispiel wird die E-Class 3 berechnet und gespeichert. Über „Save & Continue to final decision“ gelangt der Anwender auf die nächste Seite, auf der alle relevanten Informationen zum Erfassen und Handhaben der CVE dargestellt werden (Final Decision).

@Final Decision: Neben den konsolidierten Informationen aus den vorherigen Dialogfenstern erhält der Anwender nun die Gesamtbewertung der CVE sowie die Kategorisierung, anhand dieser der Anwender erkennen kann, welche Behandlungs- und Priorisierungsstrategie zur Minimierung der Sicherheitslücke erfolgen muss. IRET übernimmt für die Berechnung der finalen Entscheidung die Daten (*Incident Class bzw. I-Class*) aus der IRET Database, die über die Dialogfenster *@Result of CVE Evaluation und @CVE Prediction* generiert wurden und überträgt die Angaben nach der Logik des Portfoliomodells in eine 3 x 3 Matrix. So rechnet IRET den Final-Value automatisiert aus und bestimmt die endgültige Bewertung und Priorisierungsstrategie. Bei dem oben aufgeführten Beispiel wird die F-Value 9 und die Priorisierungsstrategie A ausgegeben, womit der Anwender an dieser Stelle unverzügliche Abhilfemaßnahmen einleiten muss. Unter „Final Results“ kann die Berechnung zur Einstufung der Behandlungsstrategie visuell vollzogen werden. Über „Save & Continue“ gelangt der Anwender zur Management Summary.

@Management Summary: Hier erhält der Anwender eine kurze Übersicht über relevante Informationen und Ergebnisse des CVE-Bewertungs- und Evaluierungsprozesses.

Das Management Summary integriert darüber hinaus die Möglichkeit zur qualitativen Bewertung, in dem der Analytiker seine Empfehlungen und Kommentare zusätzlich zu den quantifizierten Berechnungen integrieren kann. Das Management Summary kann im Anschluss zur operativen Durchführung der Beseitigungs- und Abhilfemaßnahmen an die operativen Verteidigungseinheiten weitergeschickt werden. Hierfür muss der Analytiker lediglich bei den Verwaltungsaspekten jeweils einen Haken setzen. Abschließend wird die Zusammenfassung über „Save & Create PDF“ als PDF-Datei auf dem lokalen Rechner gespeichert und per E-Mail an weitere Verteidigungseinheiten verschickt.

Revise CVE Evaluation

@Revise CVE Evaluation:

Über die Funktion „Revise CVE Evaluation“ kann der Analytiker die **Evaluation** eines zuvor angelegten CVE überarbeiten. Dies kann dann der Fall sein, wenn die temporären Daten einer CVE sich bspw. im Laufe der Zeit in eine kritische Richtung verändern (z. B. „POC“ Eigenschaft der Exploit Code Maturity einer CVE wird auf „High (H)“ oder „Function (F)“ hochgestuft, was im Detail eine sehr ernstzunehmende Bedrohungslage durch die veränderten zeitlichen Metriken darstellt).

@Search CVE: Im ersten Schritt muss der Anwender angeben, welche CVE überarbeitet werden soll. Dazu gibt er die entsprechende CVE-ID ein und klickt anschließend auf „Search.“ Refresh aktualisiert die Seite, sofern der Analytiker eine andere CVE auswählen bzw. seine Eingaben korrigieren möchte. Nun werden alle gespeicherten Informationen aus der IRET Database aufgerufen und in dem Dialogfenster ausgegeben. Nun kann der Analytiker Änderungen an seiner ursprünglichen Evaluation unter „Revise temporal Matrices/CVE evaluation“ durchführen. Abschließend müssen die Änderungen über die „Save“ Schaltfläche abgespeichert werden. Über die Schaltfläche „Back“ gelangt der Anwender zurück in den Observe Bereich.

Revise CVE Details

@Revise CVE Details: Über diese Funktion kann der Analytiker **Details** einer zuvor angelegten CVE anpassen. Der Vorgang wird in der Analogie zu *@Revise CVE Evaluation* ausgeführt.

Revise CVE Comment

@Revise CVE Comment: Über diese Funktion kann der Analytiker Kommentare und Empfehlungen für einzelne CVE überarbeiten. Der Vorgang wird in der Analogie zu *@Revise CVE Evaluation* ausgeführt.

Dialogfenster: ***Orient***

Set Criticality

@Set Criticality: Der Bereich Orient bietet zwei Kernunterbereiche. Innerhalb des *@Set Criticality* (1) Bereichs werden die Kritikalitäten für die Ports, Redundanzen von Systemen und Sicherheitszonen festgelegt. Im *@Revise Criticality* (2) Bereich können die angegebenen Kritikalitäten (zeitgesteuert oder ereignisgesteuert) überarbeitet werden. Die Orient-Phase bildet das Herzstück des Kohärenzmodells, da hier die wesentlichen objektiven und systembezogenen Eigenschaften und deren Kritikalitätsstufen festgelegt werden, die für die CVE-Bewertungspriorisierung eine entscheidende Rolle spielen. Durch die Identifizierung der in den ICS-Netzwerklandschaften eingesetzten Ports, Systeme und Zonen sowie durch die Bestimmung der Kritikalitäten, können die CVE diesen Angaben gezielt zugeordnet werden. So muss der Analytiker lediglich eine CVE über die Funktion @Evaluate CVE den betroffenen Komponenten zuordnen. IRET rechnet dann automatisiert das Schadensausmaß einer CVE.

Innerhalb dieses Dialogfensters werden die Ports, Systeme und Netzwerkzonen mit ihren Namen und den Kritikalitäten festgelegt und in den hierfür vorgesehenen Bereichen im Backend gespeichert. Um eine Übersicht der jeweiligen Kritikalitäten zu erhalten, kann der Analytiker die „Overview" Funktion aufrufen. Hierbei erhält er eine Übersicht über die eingetragenen Werte.

Revise Criticality

@Revise Criticality: Über diese kann der Analytiker die Kritikalitäten für Ports, Systeme und Sicherheitszonen überarbeiten. Wichtig ist zu beachten, dass vorgenommene Änderungen hier nicht die Ergebnisse alter, bestehender CVE mit ändern. D.h., dass die hier vorgenommenen Änderungen nur für neue CVE gelten. Ältere bewertete CVE müssen aktiv durch den Analytiker über die Funktion @*Revise CVE Evaluation* gesucht und geändert werden. Innerhalb der Funktion @*Revise Criticality* kann der Analytiker zwischen @*Revise Ports Criticality* (1), @*Revise Redundancies Criticality* (2), @*Revise Zones Criticality* (3), @*Port Overview* (4), @*System Overview* (5), @*Zone Overview* (6) entscheiden.

@Revise Ports Criticality: Über diese Funktion können die Ports und deren angegebenen Kritikalitäten überarbeitet werden. Hier kann der Analytiker zunächst nach einem bestimmten Port über die „Search-Funktion" suchen. Die Search-Funktion sucht entsprechende Ports aus der Datenbank aus und gibt die Informationen über den Port und die Kritikalität aus. Anschließend kann der Analytiker Änderungen an der Kritikalität des Ports vornehmen. Die Änderungen an der Portskritikalität können durch Änderungen an der Systemarchitektur, Konfigurationen oder durch Änderungen an Ein- und Ausgängen eines Ports verursacht werden. Um die Änderungen zu speichern, klickt der Analytiker auf „Save and Continue".

@Revise Redundancies Criticality*:* Über diese Funktion können die Systeme und deren angegebenen Kritikalitäten überarbeitet werden. Diese Funktion wird in der Analogie zu @*Revise Port Criticality* ausgeführt.

@Revise Zones Criticality*:* Über diese Funktion können die Zonen und deren angegebenen Kritikalitäten überarbeitet werden. Diese Funktion wird in der Analogie zu @*Revise Port Criticality* ausgeführt.

@Port Overview, @System Overview, @Zone Overview**:** Die drei Overview-Funktionen ermöglichen dem Analytiker einen Überblick über vorhandene Ports, IT-Systeme und Zonen sowie deren Kritikalitäten, die angelegt wurden. Hierbei erhält der Analytiker einen Einblick (nur Leseberechtigung) in die angelegten Datenstämme.

Dialogfenster: ***Decide***

CVE Results

Das Dialogfenster „Decide" bietet drei Subfunktionen: @*CVE Results* (1), @*Response Results* (2), @*Final Results* (3). Hier erhält der Analytiker eine Übersicht zu der CVE-Bewertung, -Priorisierung und zur Response (u.a. Angaben zu den Kosten zur Beseitigung). Hier werden lediglich Informationen angezeigt. Änderungen können nur im Bereich Orient durchgeführt werden.

@Incident Results: Der Anwender kann über die implementierte „Search-Funktion" nach einer bestimmten CVE suchen, indem er die CVE-ID in das Suchfeld einbettet. IRET sucht in der Database nach der entsprechenden CVE-ID und gibt die CVE-Informationen und CVE-Auswertungsergebnisse hinsichtlich des Schadensausmaßes und der erreichten I-Class (siehe @ *Result of CVE Evaluation*) im Anschluss aus.

Response Results

@Response Results: Der Anwender kann über die implementierte „Search-Funktion“ nach einer bestimmten CVE suchen, indem er die CVE-ID in das Suchfeld einbettet. IRET sucht in der IRET Database nach der entsprechenden CVE-ID und gibt die CVE-Abhilfeinformationen (siehe @*Evaluation of Response*) im Anschluss aus.

Final Results

@Final Results: Der Anwender kann über die implementierte „Search-Funktion“ nach einer bestimmten CVE suchen, indem er die CVE-ID in das Suchfeld einbettet. IRET sucht in der Database nach der entsprechenden CVE-ID und gibt die CVE-Auswertung, -Priorisierungsinformationen, sowie entsprechende I-Class und E-Class (siehe @*Final Decision*) im Anschluss aus.

Dialogfenster: ***Act***

Act CVE

@Act CVE: Im Act CVE-Bereich erhält der Analytiker die Möglichkeit einen Überblick über die letzten fünf ausgewerteten und priorisierten CVE zu bekommen. Hierbei werden Informationen über das Schadensausmaß (*I-Class*), die Eintrittswahrscheinlichkeit (*E-Class*) und das finale Auswertungsergebnis zusammengetragen. Zudem kann der Analytiker über die Suchfunktion nach weiteren (älteren) CVE suchen. Dieser Bereich dient dem operativen Monitoring der CVE-Auswertungen.

Dialogfenster: ***Reporting***

Management Summary

Der Bereich Reporting umfasst zwei weitere Bereiche. Zum einen @*Management Summary* (1) und zum anderen @*ISMS-Report* (2).

@Management Summary: Innerhalb des Management Summary-Bereichs kann der Analytiker über die Such-Funktion und über CVE-ID nach einer CVE suchen und anschließend das Management Summary dazu generieren und als PDF abspeichern. Das gleiche Formular ist auch in *@Add CVE* zur Weiterleitung an die operativen Versorgungseinheiten integriert.

ISMS-Report

@ISMS-Report: Innerhalb des ISMS-Reports öffnet sich das Formular für den ISMS-Report. Das gleiche Formular lässt sich auch im Dashboard-Monitoring-Bereich aufrufen. Der ISMS-Report inkludiert die beiden Monitoringberichte und wird in Form eines Berichts an den Informationssicherheitsbeauftragten weitergeleitet. Dabei werden textliche Informationen und Key-Performance-Indikatoren definiert, die

- A. 16.1.3 „Reporting information security weaknesses“
- A.16 1.4 „Assessment of and decision on information security events“
- A.16.1.5 „Response to information security incidents“
- A.16.1.6 „Learning from information security incidents“

aus dem Anhang A der DIN EN ISO/IEC 27001 adressieren (vgl. DIN EN ISO/IEC 27001, 2017, S. 20). Hat der Analytiker die notwendigen Informationen eingegeben, kann er über die „Create PDF-Funktion“ die Monitoringberichte 1 und 2 anhängen und als PDF-Dateien an die zuständigen Verantwortlichen im ISMS-Bereich weiterleiten.

Dialogfenster: ***Monitoring***

Monitoring 1	***@Monitoring 1:*** Der Monitoring-Bereich veranschaulicht dem Analytiker mithilfe von Key Performance Indicators (KPI) weitere Informationen u.a. darüber, wie viele CVE sich im Status Work in Progress (WIP) und DONE befinden und gibt eine Übersicht darüber, wie viele CVE zurückgestellt (Deprioritize) und priorisiert (A-F) werden müssen. Hierbei werden aus den operativen Datensätzen mithilfe von Abfrage-Funktionen quantifizierte Indikatoren generiert. - Tabellarische Darstellung: CVE-Evaluationsstatus (in Bearbeitung, bereits abgeschlossen) - Visuelles Kreisdiagramm: Prozentsatzrechnung der erreichten Ergebnisse bezugnehmend auf den CVE-Evaluationsstatus - Tabellarische Darstellung: CVE Berichtstatus - Visuelles Balkendiagramm: Prozentsatzrechnung der erreichten Ergebnisse bezugnehmend auf den CVE-Berichtstatus - Tabellarische Darstellung: Überblick aller CVE-Priorisierungsergebnisse - Visuelles Balkendiagramm: Absolute Zahlen der CVE-Priorisierungsergebnisse Mit der „Create PDF-Funktion“ wird eine PDF- Datei des Monitorings 1 erstellt. Klickt der Analytiker auf „Continue with Monitoring 2“, gelangt er zum Monitoring 2.
Monitoring 2	***@Monitoring 2:*** Der Monitoring-Bereich veranschaulicht dem Analytiker mithilfe von KPIs ergänzende Informationen zu *@Monitoring 1.* - Tabellarische Darstellung: eingesetzte CVE-Behandlungsstrategie (akzeptierte CVE im Vergleich zu den reduzierten CVE) - Visuelles Kreisdiagramm: Prozentsatzrechnung der erreichten Ergebnisse bezugnehmend auf die CVE-Behandlungsstrategien - Tabellarische Darstellung: Kostenüberblick, verursachte Kosten durch die Nichtbehandlung der CVE, Kosten zur Beseitigung der CVE, Gegenüberstellung der beiden Posten) - Visuelles Balkendiagramm: Prozentsatzrechnung der erreichten Ergebnisse bezugnehmend auf die Ausfall- und Beseitigungskosten

Nach der Darstellung der IRET Haupt- und Sub-funktionen werden im nächsten Kapitelabschnitt mithilfe der Unified Modeling Language (UML)-Modellierung und der eEPK die einzelnen Schritte zur Interaktion mit der Softwarelösung IRET näherbeschrieben. Anschließend werden zwei Anwendungsbeispiele für ein besseres Verständnis ausgeführt.

5.5.2 Prozessschritt „Orient“

Um IRET mit der eingebetteten Logik des Kohärenzmodells für die Bewertung und Priorisierung von CVE operationalisieren zu können, muss zunächst mit der Orient-Phase begonnen werden. Die wichtigste Modifikation der OODA-Schleife, die von IRET übernommen wird, betrifft die Orient-Phase. Hier werden für das Kohärenzmodell relevante subjektive und systembezogene Determinanten bestimmt und klassifiziert. Dazu werden Inhalte aus dem „Relationship of objects in an information security incident“ der ISO/IEC 27035-1 übernommen, modifiziert, durch extrinsische und intrinsische Determinanten ersetzt und in die OODA-Schleife eingefügt (siehe Kap. 5.4.2 und Bild 35) (vgl. Koza, 2023, S. 108 | Koza, 2022a, S. 2865 | Koza, 2022b, S. 55).

Zu diesem Zweck wird die Funktion „*@Set Criticality*“ entworfen und in IRET integriert. Die Orientierungsphase kann als Vorimplementierungs- oder Vorbereitungsphase definiert werden. Bevor die Logik des Kohärenzmodells auf die CVE angewendet werden kann, muss festgelegt werden, wie die ICS-Netzwerklandschaft im Einzelnen konzipiert ist. Insbesondere müssen die extensiven Subdeterminanten Portskritikalität (f_1), Redundanzkritikalität (f_2) und Zonenkritikalität (f_3) sorgfältig bestimmt und anschließend nach dem vorgegebenen Klassifikationsschema kategorisiert werden (siehe Tabellen 8, 10 und 12). Es werden insgesamt sechs Funktionen (drei Add-Funktionen und drei Revise-Funktionen) definiert, die in der Orient Phase in IRET eingebettet werden. Diese Funktionen ermöglichen es den Analysten und den Informationssicherheitsbeauftragten, die relevanten Informationen aus bestehenden IT-Asset-Management-Tools oder dem ISMS-Tool zu extrahieren und diese dann in IRET einzubetten. Die Orient-Phase dient der Ermittlung und Klassifizierung der internen Informationen, die später mit den externen CVE-Informationen korreliert werden, um das Ausmaß des durch eine CVE verursachten Schadens nach Faktenlage zu definieren.

5.5.3 Prozessschritte „Observe“, „Decide“ und „Act“

Nach der Aufnahme und Klassifizierung der extensiven Subdeterminanten können das Kohärenzmodell und Berechnungsmodell auf die Auswahl der CVE angewendet werden. In diesem Zusammenhang markiert die Registrierung einer CVE den Beginn der operativen Beobachtungsphase und erfolgt über die Funktion *„@Add CVE*“. Über ein internes Monitoring über NIST NVD und MITRE-Datenbanken oder CVEDetails.com können die CVE identifiziert und zu IRET hinzugefügt werden. Eine weitaus effektivere Vorgehensweise ist jedoch die CVE-Informationsgenerierung, die über CERT-Anbindungen erfolgen kann. Der Vorteil einer externen CERT-Anbindung liegt in der Möglichkeit die CERT-Dienstleistungen in Anspruch zu nehmen. So kann eine automatisierte Identifizierung von ICS-spezifischen CVE ermöglicht werden, die explizit die vom Betreiber eingesetzten ICS-Systeme betrifft. Zudem sind die CERT-Meldungen in der Regel kompakter, sodass hierbei alle wesentlichen Meldungen konsolidiert nach eingesetzten ICS-Produkten angegeben werden, womit eine gewisse Anzahl an Stunden zur Ermittlung dieser erforderlichen Informationen gespart werden kann. Um jedoch ein vollständiges 360-Grad Monitoring zu gewährleisten, bietet es sich hier an, ein hybrides Modell bestehend aus internem und externem Monitoring zu implementieren (vgl. Koza, 2022b, S. 54). Zusätzlich hierzu muss zunächst eine einheitliche und grundsätzliche Selektionsstrategie gewählt werden. Unternehmen mit ausreichenden Personalkapazitäten können z.B. eine größere Anzahl von CVE in IRET aufnehmen (CVE mit dem Basis-Score ab 6,5), während Unternehmen mit geringeren Personalkapazitäten eine geringere Anzahl von CVE (CVE ab 8,5 oder 9,0) in IRET aufnehmen können. Die Entscheidung, ab welchem Schwellenwert eine CVE in IRET und damit in das Kohärenzmodell aufgenommen werden soll, bleibt eine unternehmensindividuelle Entscheidung, die auf Basis der eigenen Ressourcen und der Kritikalität der Geschäftsprozesse getroffen werden muss. IRET bietet entsprechende Speicherkapazitäten für die Registrierung einer CVE an, um eine große Menge an wichtigen Informationen (Base Metrics einer CVE) zu einer angemessenen Dokumentation aufzunehmen.

Allerdings müssen die gesammelten Base Metrics einer CVE um die zeitlichen Metriken erweitert werden. IRET implementiert die beiden zeitlich wichtigsten Metriken, die unter Exploit Code Maturity (e_4) und Remediation Level (e_5) zusammengefasst werden und durch die Funktion *„@Add CVE*“ in IRET eingebettet werden. Das bedeutet jedoch, dass die Analysten diese beiden Subdeterminanten durch eigene Recherchetätigkeit bestimmen müssen, sofern diese nicht in den CERT-Meldungen ausgegeben werden. Nach der Registrierung einer CVE kann die Funktion *„@Evaluate CVE*“ gewählt werden, um die gesammelten externen Informationen mit den zuvor in der Orientierungsphase ermittelten internen extensiven Subdeterminanten abzugleichen. Hier muss der Analyst nur noch bestimmen welcher Port, welches ICS-System und welche Zone von der registrierten CVE betroffen ist. Die erste Faktorengruppe I-Class umfasst die Beziehung der intrinsischen Determinanten. Daher werden die intensiven und extensiven Subdeterminanten als Orientierungs- (Bewertungs-) Kriterien für die Gewichtung der erfassten internen und externen Informationen zur Beurteilung des Ausmaßes der eingehenden CVE einbezogen. Während der Analyst diese Informationen an IRET überträgt, berechnet und quantifiziert es im Hintergrund das Schadensausmaß der registrierten CVE automatisch. Innerhalb der Funktion *„@Result of CVE Evaluation*“ wird der Schadensausmaßwert I-Class visualisiert.

In einem letzten Schritt muss der Analyst den EPSS-Score oder den CWE-Likelihood-Score für die Wahrscheinlichkeit der Ausnutzung bestimmen, um die Wahrscheinlichkeit des Auftretens der identifizierten CVE zu bestimmen. Auch hier führt IRET die Berechnungen im Hintergrund durch und ermittelt den Wert für die E-Class. Anschließend fasst IRET die beiden Klassen zusammen und integriert das Ergebnis in das Portfolio. Die 3 x 3-Matrix Portfoliomatrix berechnet die endgültige Priorisierungsstrategie, um CVE-Behandlungsstrategien und die chronologische Reihenfolge der CVE-Behandlungen zu bestimmen. Zu diesem Zweck wird die Funktion *„@Final Decision*“ entworfen und in die softwarebasierte Lösung „IRET“ integriert.

5.5.4 Prozessschritt „Set Criticality” in der Orient-Phase

Um die Interaktionsschritte mit IRET und die bisherigen Prozessschritte besser darstellen zu können, werden die einzelnen Anwendungsfälle des Kohärenzmodells und der modifizierten OODA-Schleife in den nachfolgenden Kapitelabschnitten mit Hilfe von UML Use Cases (Anwendungsfällen) modelliert und aufgeführt. Zu jedem Anwendungsfall werden auch die dazugehörigen IRET-Dialogfenster mit aufgeführt. Ferner wird auch das Systemverhalten anhand unterschiedlicher CVE in verschiedenen Einsatzgebieten mit differenzierten Netzwerkeigenschaften und Netzwerkarchitekturen thematisiert. Der Fokus liegt hierbei auf der Plausibilitätsprüfung des Kohärenzmodells, um anhand der unterschiedlichen Modifikationen bzgl. der Kritikalitätsbetrachtungen, der Angriffswahrscheinlichkeit und des Angriffsvektors, die jeweils zu erwartende Priorisierungsstrategie zu ermitteln und darstellen zu können.

Zur Operationalisierung des Kohärenzmodells müssen zunächst die Prozessschritte PS 1 bis PS 8 aus Tabelle 19 ausgeführt werden, die den Anwendungsfall „Set Criticality“ (Bild 36) repräsentieren. Der blaue Pfad zeigt den Interaktionsweg mit den dazugehörigen Funktionen, die in IRET zur Erfüllung der ersten Prozessschritte zur Bestimmung der Ports-, Redundanz-- und Zonenkritikalitäten konzeptualisiert sind.

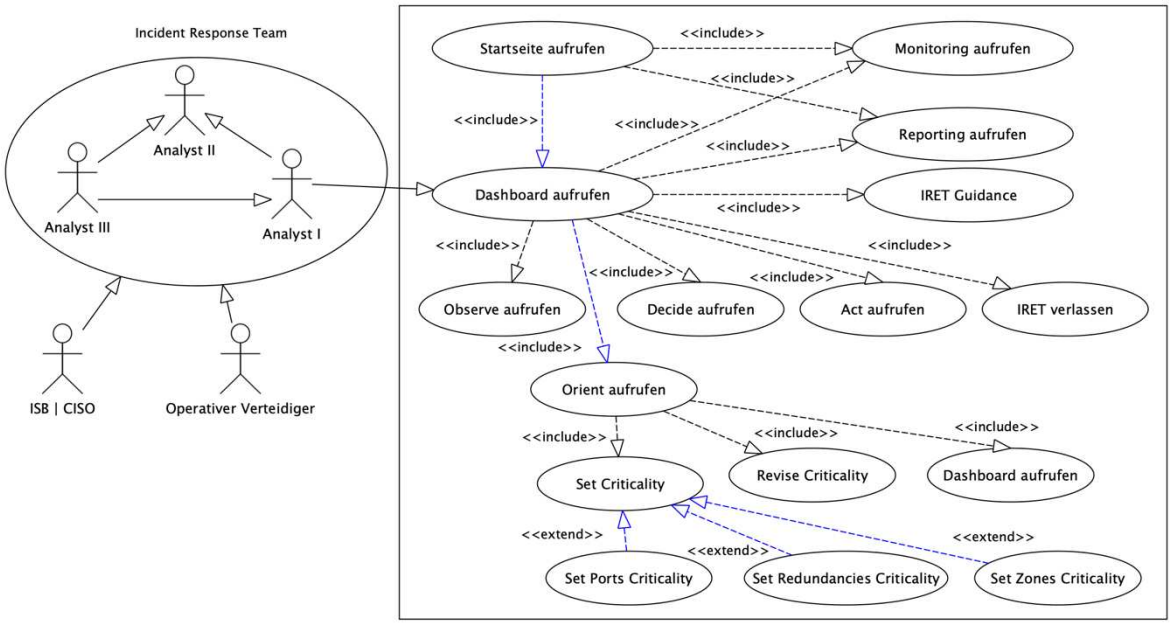


Bild 36: Use Case: Set Criticality in der Orient-Phase (Quelle: Eigene Darstellung)

Um den Anwendungsfall in IRET realisieren zu können, wird innerhalb eines Orient-Workshops nach der Ermittlung der in den ICS-Netzwerken eingesetzten Ports, Systeme und Zonen durch das Zusammenkommen aller relevanten strategischen und operativen Verteidigungseinheiten der Versuch unternommen, die jeweiligen Kritikalitäten der ICS-Komponenten zu bestimmen.

Zu diesem Zweck startet der Systemanwender, in diesem Fall der Analyst I, das Anwendungstool IRET, um die Kritikalitätsklassen, Standardeinträge sowie die Integration der identifizierten ICS-Komponenten und deren Kritikalitäten in IRET einbetten zu können. Nach dem Öffnen des Tools wird das erste interaktive Dialogfenster, die „Startseite“, angezeigt. Hier erhält der Analyst I die Möglichkeit auf die „Dashboard“, „Monitoring“ und „Reporting“-Funktionen zuzugreifen (siehe Anhang A.1). Über die Schaltfläche „Dashboard“ gelangt der Analyst I auf die grafische Oberfläche, in der dem Analysten u.a. die vier Phasen Observe, Orient, Decide und Act als weitere Schaltflächen zur Verfügung gestellt werden (siehe Anhang A.2).

Um die Kritikalität der identifizierten Ports, Redundanzen und Zonen bestimmen zu können, greift der Analyst I auf die Schaltfläche „Orient“, um zu weiterführenden Funktionen in der grafischen Oberfläche „Orient“ zu gelangen. Innerhalb des Dialogfensters „Orient“ werden drei Funktionen „Set Criticality“ zur Bestimmung der Kritikalitäten, „Revise Criticality“ zu Änderungen der bereits festgelegten Kritikalitäten und „Dashboard“ zur Navigation auf dem Dashboard-Dialogfenster angezeigt (siehe Anhang A.3). Zur Bewertung und Priorisierung des Anwendungsbeispiels der CVE-2021-44228 legen die Analysten zunächst die Kritikalität des Ports TCP/IP 389, des SCADA-Servers (MTU) und die betroffene Zone 4 fest.

Über die Schaltfläche „Set Criticality“ gelangt der Analyst I zu den wichtigsten Funktionen „Set Criticality“, die im Dialogfenster mit denselben Namen grafisch dargestellt werden (siehe Anhang A.4).

Die Bestimmung der Kritikalitäten sollte durch die Beteiligung aller relevanten Personen erfolgen. Damit kann ein wesentliches Ziel zur Akzeptanz der Bewertungsstrategie erreicht werden, da die Klassifizierung der Kritikalitäten von allen relevanten Akteuren getroffen wird. Daraus wird eine steigende Belastbarkeit und Nachvollziehbarkeit des Verfahrens erreicht. Hierdurch entsteht ein einheitliches Verständnis für alle Akteure, vor allem für die operativen Verteidigungseinheiten, welche für die Umsetzung der Behebungs- und Abhilfemaßnahmen verantwortlich sind.

Zudem kann das Miteinbeziehen von operativen Einheiten, die tiefergehende Kenntnisse über ihre zu betreuenden Systeme und Komponenten haben, zu einer besseren Einstufung der Kritikalitäten führen. Diese Vorgehensweise kann bei präziser Ausführung zu besseren Entscheidungsfindungen führen. Nachdem die Kritikalitäten kollektiv bestimmt und in IRET eingebettet wurden, können die eingegebenen Daten zwecks Überprüfung über die integrierte „Overview“-Funktion eingesehen werden.

Die eingegebenen Daten werden in den jeweils zugehörigen Datenblättern gespeichert, welche im Anhang A.5 dargestellt werden.

5.5.5 Prozessschritt „Add CVE” in der Observe-Phase

Nachdem im ersten Anwendungsfall die Stammdaten über die Orient-Funktion eingebettet wurden, erfolgt im nächsten Anwendungsfall die operative Echtzeitdatenerfassung, Bewertung und Priorisierung von einzelnen CVE, die als Schwachstellen in IRET eingebettet werden. Der Anwendungsfall „Add CVE“ umfasst die Observe-Realtime, Observe-Orient-Realtime und Observe-Act-Realtime Prozessschritte PS 14 bis PS 20 aus Tabelle 19. Im Gegensatz zum ersten Anwendungsfall können die Echtzeitdatenerfassungs- und Bewertungsprozesse von nur noch einem Analysten ausgeführt werden. Hierdurch können mehrere Analysten bei komplizierten Netzwerkarchitekturen über mehrere Standorte hinaus parallel arbeiten.

Der wesentliche Vorteil liegt in der Tatsache, dass die CVE-Bewertungen und Priorisierungen nach der einheitlichen Bestimmung der Bewertungsgrundlage aus dem ersten Anwendungsbereich sowie der Hinzunahme von objektiven Determinanten nun unabhängig vom Entscheidungsträger erfolgen können. Das bedeutet, dass jeder Analyst auf dieselbe objektive Grundlage zur Bewertung zurückgreift, sodass die Entscheidungen zur Bewertung und Priorisierung der CVE zum gleichen Ergebnis führen, unabhängig davon welcher Analyst die Entscheidungsprozesse durchführt.

Die Prozesse zur CVE-Erfassung, CVE-Zuordnung, CVE-Schadensausmaßbewertung, CVE-Eintrittswahrscheinlichkeit und den CVE-Priorisierungen werden im nachfolgenden Bild 37 Use Case „Add CVE“ modelliert.

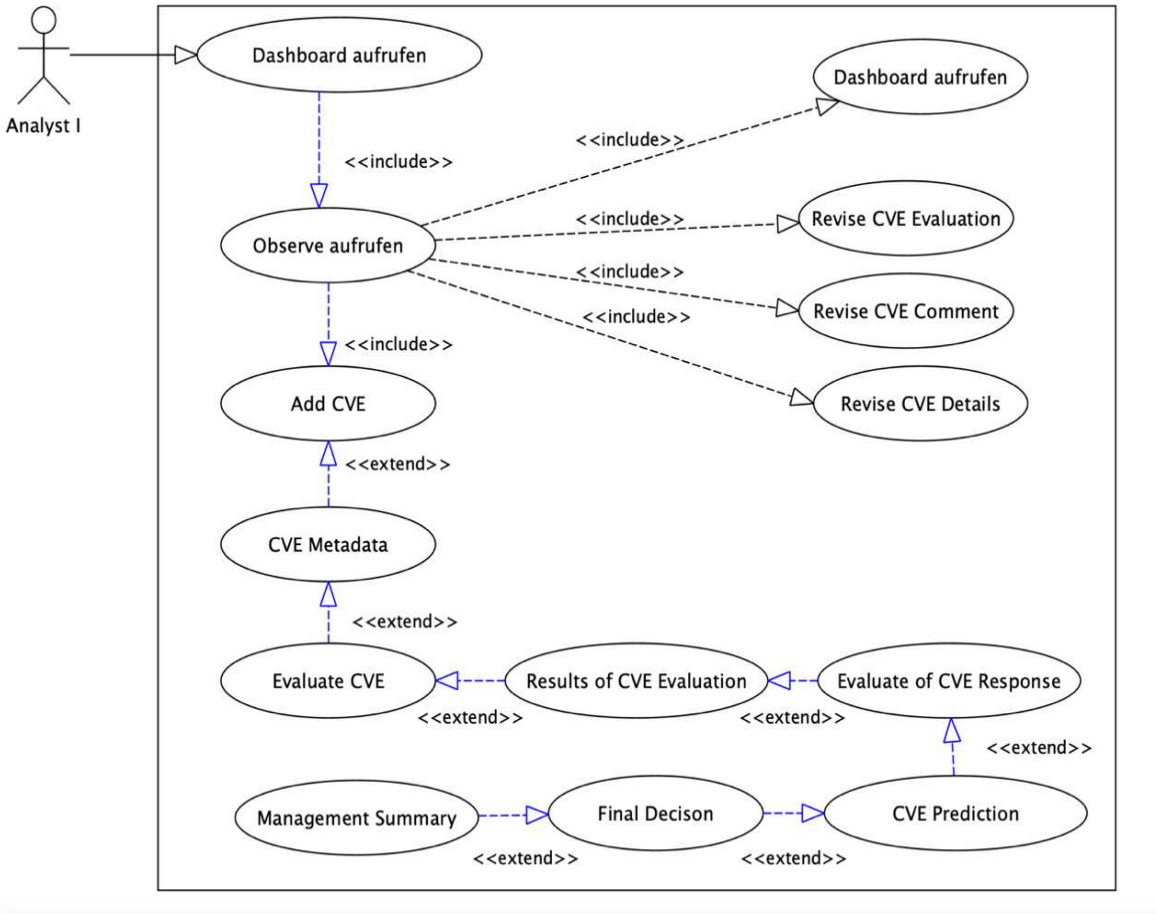


Bild 37: Use Case: Add CVE (Quelle: Eigene Darstellung)

Um die Registrierung einer CVE vorzunehmen, initialisiert der Analyst über das Dialogfenster „Observe“ (siehe Anhang A.2) und über die Schaltfläche „Add CVE“ den Prozess zur Aufnahme der relevanten externen Informationen, die über NIST NVD, MITRE oder über externe CERT-Anbindungen öffentlich zugänglich sind (siehe Anhang A.6). Über die Schaltfläche „Add CVE“ gelangt der Analyst zum Add CVE-Dialogfenster (siehe Anhang A.7), in dem die Base Metrics und die Temporal Metrics einer CVE nun in IRET eingegeben werden können, die dann folgend im Datenblatt „IRET Database“ hinterlegt und gespeichert werden.

Hierbei werden auch die Angaben zu den Subdeterminanten „Exploit Code Maturity (e_4) und Remediation Level (e_5)“ automatisiert in die Berechnungsmethodik eingebettet und zur Berechnung des CVE-Schadensausmaßes der Klasse „Calculate C-Value“ bereitgestellt. Über das Betätigen des „Save and Continue“ Buttons gelangt der Analyst zum Dialogfenster „CVE Metadata“, wo er die weiterführenden Informationen über eine CVE, wie bspw. die CVE-Beschreibung, technische Eigenschaften zur Ausführung der jeweiligen CVE, die verwandte CWE-ID, die Art des betroffenen Produkts, den Hersteller, die Version und Editionen des betroffenen Produktes sowie Informationen zur Quelle der jeweiligen Abhilfemaßnahmen, eingeben und speichern lassen kann (siehe Anhang A.8).

Als nächstes gelangt der Analyst über den Button „Save and Continue“, nachdem er die weiterführenden CVE-Informationen in IRET eingepflegt hat, zum Dialogfenster „Evaluate CVE“, wo er die Möglichkeit bekommt, die integrierte CVE dem betroffenen Port, System und Zone zuzuordnen (siehe Anhang A.9). IRET verwandelt die angegebenen Zuordnungswerte und gibt die Kritikalitätswerte zu f_1, f_2 und f_3 an. Im Anschluss werden alle überlieferten Werte in die C-Berechnungsformel eingebettet und miteinander addiert. So stellt IRET im Hintergrund sicher, dass das Schadensausmaß einer CVE während der Eingabe automatisiert berechnet und ausgegeben wird. In einem vorletzten logischen Schritt leitet IRET den errechneten C-Value (Schadensausmaßwert= $f_1+f_2+f_3+e_1+e_2+e_3+e_4+e_5$) weiter, um diesen den Schadenklassifizierungsstufen der I-Classes zuzuordnen. Nach dem die C-Value- und I-Class-Werte berechnet sind, werden diese zur Visualisierung weitergeleitet, wo der Analyst die Ergebnisse seines bisherigen Bewertungsprozesses entnehmen kann (siehe Anhang A.10).

Bei dem ausgewählten Beispiel mit der CVE-2021-44228 beträgt der Schadensausmaßwert „C-Value“ 21, welcher der I-Class „3“ zugeordnet wird (Tabelle 19, PS 18 und Anhang A.10). Zudem können die Analysten eine Monetarisierung der Ausfallfolgenschäden treffen, indem für jede CVE ein individueller Wert in das Feld „Damage in money“ eingetragen wird. Jede eingetragene CVE in IRET erhält zusätzlich die Möglichkeit die dazugehörigen Beseitigungs- und Abhilfemaßnahmen zu spezifizieren und diese als Dokumentationsgrundlage bei Bedarf zur Weiterbehandlung an die operativen Verteidigungseinheiten weiterzuleiten. Über den Button „Save and Continue“ im Dialogfenster „Result of CVE Evaluation“ gelangt der Analyst zu der nächsten grafischen Oberfläche „Evaluate of CVE Response“. In diesem Dialogfenster können die weiterführenden Informationen zu den Abhilfemaßnahmen sowie den dazugehörigen Beseitigungskosten eingebettet und gespeichert werden (siehe Anhang A.11). Die angegebenen Daten werden später aus dem Datenblatt „IRET Database“ extrahiert und in das Management Summary als informative Grundlage zur Weiterleitung an die operativen Verteidigungseinheiten eingebettet.

Nachdem die weiterführenden Informationen in IRET eingebettet sind, gelangt der Analyst über den Button „Save“ zum nächsten Dialogfenster „CVE Prediction“, indem die Eintrittswahrscheinlichkeit der CVE und die dazugehörige E-Class berechnet und eingegeben werden kann. Im Beispiel mit der CVE-2021-44228 wird der Wert „3“ für die E-Class ausgewählt, da die Eintrittswahrscheinlichkeit der CVE hoch bzw. auf über 61 % postuliert wird. Im Anhang A.12 wird die grafische Visualisierung des Dialogfensters „CVE Prediction“ illustriert.

Als nächstes gelangt der Analyst zu der finalen Entscheidungsfindung, die im Dialogfenster „Final Decision“ angezeigt wird. Um die finale Priorisierungsstrategie bestimmen zu können übergibt die IRET den von den Analysten festgelegten E-Class-Wert weiter. Zudem wird der Wert zur I-Class über die interne IRET-Schnittstelle ebenfalls weitergeleitet, wo die beiden I- und E-Class-Werte miteinander multipliziert werden. IRET errechnet somit den F-Value und die dazugehörige Priorisierungsstrategie im Hintergrund und übermittelt diese Daten an das Dialogfenster Final Decision, wo diese Ergebnisse den Anwendern illustriert werden (siehe Anhang A.13).

Wie bereits in Tabelle 19 mit dem PS 18 dargestellt, wird das Ergebnis für die I-Class und E-Class jeweils dem Wert „3“, für die F-Value dem Wert „9“ und der Priorisierungsstrategie „A“ zugeordnet. Beim Betätigen des Buttons „Save“ gelangt der Analyst zur „Management Summary“, wo er die Möglichkeit erhält seine Expertise in Form von Kommentaren und Empfehlungen hinzuzufügen, um die quantifizierten CVE-Bewertungen zu komplementieren. Das Management Summary erhält darüber hinaus die Möglichkeit Fristen für Abhilfemaßnahmen entsprechend dem Priorisierungsergebnis festzulegen. Das Management Summary kann als PDF gespeichert und an die jeweilige operative Verteidigungseinheit zwecks Umsetzung der Abhilfemaßnahmen weitergeleitet werden (siehe Anhang A.14).

5.5.6 Prozessschritt: „Revise CVE Evaluation” in der Observe-Phase

Ergeben sich Veränderungen in der Netzwerkarchitektur, Netzwerkplanung oder ersetzen neue Softwarekomponenten und Softwaremodule die alten logischen Einheiten, so können sich auch die Anzahl, die Art und die Kritikalitäten der bereits integrierten Ports, Systeme und Zonen verändern. Diese Veränderungen können sowohl zu einer Verschlechterung und damit zu mehr Fragilität oder aber auch zu einer Verbesserung des Sicherheitsniveaus führen. Das impliziert den Grundgedanken des Kohärenzmodells.

Die Art des Software- und Hardwareeinsatzes hat eine signifikante Auswirkung auf die Bewertung von CVE. Eine dieser Veränderung kann sich bspw. auf die mehrfache Integration bzw. das Vorkommen eines Systems oder eines Moduls beziehen. In der Analogie zum mehrfachen Vorkommen des TCP/IP-Ports 455 kann auch eine Applikation für mehrere Systeme gleichzeitig zuständig sein oder diesen zugeordnet werden. Wird angenommen, dass die definierte CVE-2021-44228, das Softwaremodul SPRECON-E IEC 61850 Mapper in den eingesetzten SPRECON Hardwaremodulen innerhalb der Automatisierungstechnik betrifft, kann eine aus der Historie gewachsene falsche Netzwerkkonfiguration zu mehr Verwundbarkeit führen. Das ist bspw. dann der Fall, wenn die Hardwarekomponenten multidimensional in unterschiedlichen Zonen eingesetzt werden. Liegt eine derartige Integrationsarchitektur vor, so können mehrere Systeme und gleichzeitig auch mehrere Zonen von der CVE-2021-44228 betroffen sein (vgl. Sprecher Automation, 2022, o. S.).

Um die Möglichkeit zur Reaktion auf sich verändernde Situationen zu ermöglichen, enthält IRET die Funktion „Revise CVE Evaluation“ um die bereits getroffenen CVE-Auswertungen erneut durchführen zu können. Hierfür wird demzufolge postuliert, dass die SPRECON-Hardware mehrfach in unterschiedlichen Zonen (bspw. Zone 3 und 4) eingesetzt wird. Um die CVE-Evaluation erneut ausführen zu können muss der Analyst, wie dem vorliegenden Anwendungsfall zu entnehmen ist, die IRET-Observe-Funktion aufrufen und den Evaluierungsprozess über die inkludierten Funktionen neu ausführen (Bild 38).

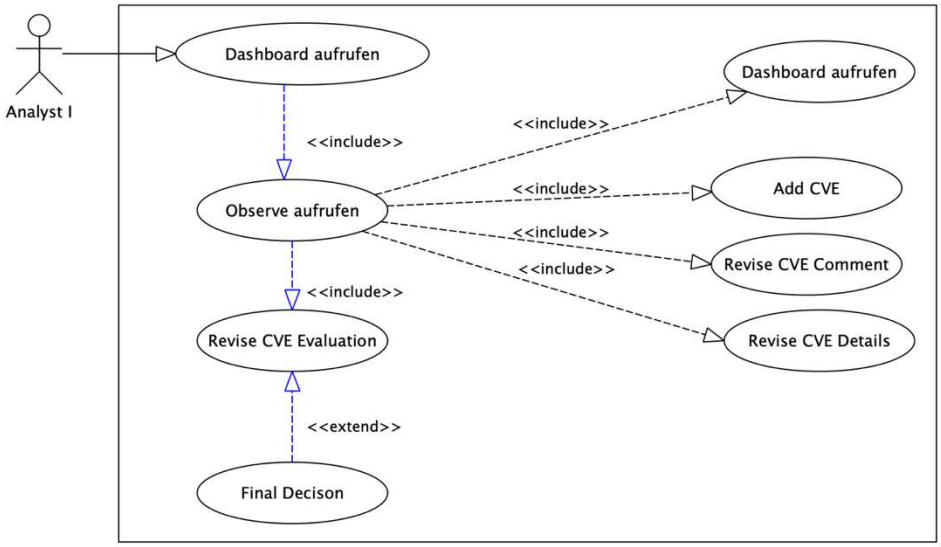


Bild 38: Use Case: Revise CVE Evaluation (Quelle: Eigene Darstellung)

Ruft der Analyst erneut das Observe-Dialogfenster auf (siehe Anhang A.6), so erhält er über den Button „Revise CVE Evaluation“ die Möglichkeit zum gleichnamigen Dialogfenster „Revise CVE Evaluation“ zu gelangen. In diesem Dialogfenster kann der Analyst über die integrierte Suchfunktion die passende CVE ID eintragen, um die dazugehörigen Evaluationsergebnisse aufzurufen (siehe Anhang A.15). In einem nächsten Schritt kann der Analyst in der Analogie zu den ersten CVE-Bewertungen die Zuordnungswerte ändern. So kann gemäß der bereits getroffenen Postulierung das vom CVE betroffene System vom SCADA-Server (MTU) auf „multiple Systeme“ und die von der CVE betroffene Zone von Zone 4 auf „multiple Zonen“ umgeändert werden. Zudem kann der Analyst durch den hohen Schweregrad die monetären Schätzungen zu den Ausfallfolgen von 200.000 € auf z.B. 300.000 € hochkorrigieren und die Response-Informationen neu definieren. Zusätzlich hierzu verändert sich auch die Angriffslage, in der die Stufe der „Exploit Code Maturity“ von POC und auf High hochgestuft wird, da nun ausführbare Angriffscodes öffentlich zugänglich sind. Nach den Ausführungen der Änderungen bzgl. der Zuordnungswerte kann der Analyst mit Hilfe des „Save-Buttons“ die Eingaben speichern und die Änderungen bestätigen. IRET übernimmt die neuen Angaben und führt auf Grundlage der neuen Zuordnungswerte die Berechnungen im Hintergrund durch (siehe Anhang A.16)

5.5.7 Prozessschritt „Decide“

Um die neuen CVE-Berechnungswerte zu betrachten und diese über eine neue Management Summary zu dokumentieren, muss der Analyst über einen neuen Anwendungsfall das Decide-Dialogfenster aufzurufen, um die modifizierten Ergebnisse und Änderungen in den Berechnungen durchführen zu können (Bild 39). Über das Dialogfenster „Decide“ erhält der Analyst die Möglichkeit die isolierte CVE-Schadensausmaßberechnung („CVE Results“), Response-Informationen („Response Results“) und die finale Entscheidung („Final Decision“) aufzurufen (siehe Anhang A.17). Das Dialogfenster „CVE Evaluation Results“ zeigt die veränderten Werte der Subdeterminanten und führt den C-Value und die dazugehörige I-Class auf (siehe Anhang A.18).

Über das Dialogfenster „CVE Response Evaluation Results“ können die Ergebnisse der Response-Informationen visualisiert werden (siehe Anhang A.19), während das Dialogfenster „CVE Final Results“ die modifizierte finale Priorisierung darstellt (siehe Anhang A.20).

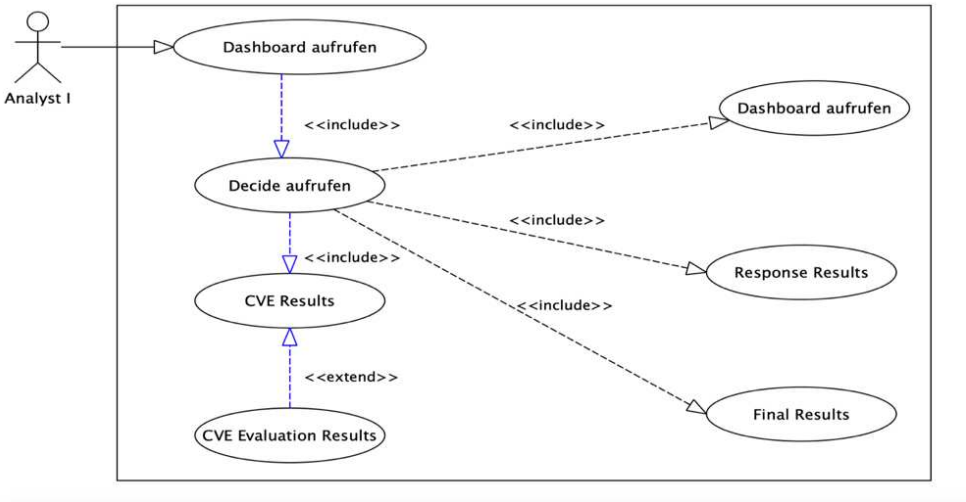


Bild 39: Use Case: Decide (Quelle: Eigene Darstellung)

Bei den aufgeführten Modifikationen wird ersichtlich, dass sich durch die mehrfache Betroffenheit der Zonen sowie durch Veränderungen des Niveaus der „Exploit Code Maturity“ der C-Value von 21 auf 24 erhöhen lässt (siehe Anhang A.18). Die Priorisierungsstrategie bleibt jedoch trotz des veränderten C-Values gleich und wird als „A-Prio“ ausgegeben, da die dazugehörige Zuordnung zur I-Class nach wie vor der dritten Stufe zugeordnet wird.

5.5.8 Prozessschritt „Monitoring“

Zur Überwachung der Evaluationsprozesse implementiert IRET eine Monitoringsfunktion, wodurch die operativen Daten zur CVE-Bewertung und -Priorisierung extrahiert und in Form von KPIs konsolidiert werden. Der Anwendungsfall zeigt, wie die zwei Monitoringberichte in IRET generiert werden können (Bild 40)

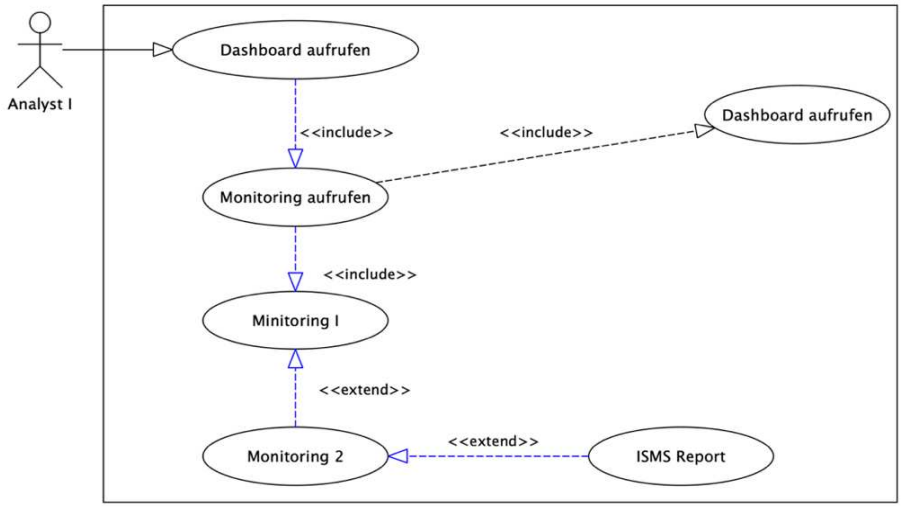


Bild 40: Use Case: Monitoring (Quelle: Eigene Darstellung)

Ruft der Analyst das Dialogfenster „Monitoring“ auf, so kann er in einer festgelegten Reihenfolge die zwei implementierten Monitoringberichte aufrufen. Der erste Monitoringbericht enthält Kennzahlen über den CVE-Evaluationsstatus und zeigt auf, wie viele CVE bereits erfolgreich abgeschlossen und wie viele noch zu evaluieren sind. Der Evaluationsstatus einer CVE ist dann als abgeschlossen, also „DONE“, zu betrachten, wenn der Analyst eine CVE vollständig eingebettet, die CVE-Zuordnungswerte und die Eintrittswahrscheinlichkeit festgelegt hat, sodass die erforderliche C-Value, I-Class, E-Class und F-Value sowie die dazugehörige Priorisierungsstrategie berechnet werden kann. Andernfalls wird der Evaluationsstatus als WIP ausgegeben. Zur Visualisierung des CVE-Evaluationsstatus werden sowohl die absoluten Zahlen in tabellarischer Form als auch die prozentualen Zahlen in einem Kreisdiagramm dargestellt. Neben dem Evaluationsstatus einer CVE wird auch der Status des CVE-Berichtes innerhalb von IRET fortlaufend dokumentiert und überwacht. Der CVE-Reportstatus gibt an, ob die im Management Summary konsolidierten Informationen auch tatsächlich an die zuständigen operativen Verteidigungseinheiten berichtet wurden. Die Evaluierung einer CVE ist somit dann fachlich und organisatorisch vollständig abgeschlossen, wenn sowohl der CVE-Evaluationsstatus als auch der CVE-Reportstatus beide abgeschlossen sind.

Zur Visualisierung des CVE-Reportstatus werden die absoluten Zahlen in tabellarischer Form und die prozentualen Zahlen in einem Balkendiagramm dargestellt. Zusätzlich zu den zwei generierten KPIs werden die bereits erreichten Priorisierungsergebnisse konsolidiert. So können Kennzahlen entwickelt werden, aus denen ersichtlich wird, wie die CVE in der Gesamtheit priorisiert wurden. Dabei wird die absolute Zahl der eingebetteten CVE zum Verhältnis der jeweiligen Priorisierungsstrategien in tabellarischer Form und in einem Balkendiagramm visualisiert. So kann den Kennzahlen entnommen werden, wie viele CVE als TN und wie viele als TP mit welcher zeitlichen Kritikalität priorisiert wurden. Diese Kennzahlen werden im Anhang A.21 illustriert. Die Monitoringberichte enthalten weitere Funktionen, um die KPIs zu aktualisieren „Refresh“, diese als PDF-Datei generieren zu lassen „Create PDF“, um den Bericht als Anhang dem ISMS-Report hinzufügen zu können. Betätigt der Analyst den Button „Continue with Monitoring 2“ gelangt er zum zweiten Monitoringbericht, welcher strategische Kennzahlen zu den definierten Behandlungsstrategien sowie aggregierte Kennzahlen zu anfallenden Kosten darstellt.

Die Übersicht der Kennzahlen über die CVE-Behandlungsstrategie führt auf, wie oft die Reduzierungsstrategie zur Minimierung bzw. Beseitigung der CVE ausgeführt wurde. Zusätzlich hierzu werden auch die beiden Kostenposten gegenübergestellt. Dabei kann aufgezeigt werden, wie viel monetären Schaden die eingebetteten CVE kumulativ verursachen können. Als Vergleichswert wird auch der kumulative Betrag aufgeführt, der durch die operative Ausführung der Beseitigungsmaßnahmen anfällt.

Durch die Gegenüberstellung dieser beiden Kostenposten kann der monetäre Vorteil ermittelt werden („Estimated monetary value added by response to eliminate vulnerability“), der sich durch das Subtrahieren der anfallenden kumulativen Kosten zur Beseitigung der CVE („Total estimated response costs“) von anfallenden kumulativen CVE-Ausfallfolgenkosten („Total estimated downtime costs“) berechnet ((Total estimated downtime costs)-(Total estimated response costs)).

Die aufgelisteten Kennzahlen werden sowohl in tabellarischer Form als auch in Form von Balkendiagrammen visualisiert (siehe Anhang A.22). Beide Monitoringberichte lassen sich mit Hilfe der Funktion „Create PDF“ dem ISMS-Report als Anhänge hinzufügen. Betätigt der Analyst den Button „Continue“ im Dialogfenster „Monitoring: CVE-Key Performance Indicators II“ so gelangt er zu der grafischen Oberfläche des ISMS-Reports. Im Dialogfenster „ISMS-Report“ können der Berichtzeitraum sowie weitere Anmerkungen herangezogen werden.

Der ISMS-Report hängt die beiden zuvor generierten Monitoringberichte an und kann als periodischer oder jährlicher Bericht an den Informationssicherheitsbeauftragten weitergeleitet werden. Der Fokus des ISMS-Reports adressiert die Maßnahmen aus der DIN EN ISO/IEC 27001 A. 16 (A. 16.1.3, A. 16.1.4, A. 16.1.5 und A. 16.1.6), welche sich im Bereich des IRM und VM, u.a. mit den technischen und organisatorischen Prozessen zur Schwachstellenerkennung, Schwachstellenbewertung und den Abhilfemaßnahmen befassen (siehe Anhang A.23).

In den nächsten Kapitelabschnitten werden weitere Modifikationen simuliert, die im Detail

- Änderungen der Eintrittswahrscheinlichkeit der CVE-2021-44228,
- Änderungen der CVE-Zuordnungswerte und die Eintrittswahrscheinlichkeit der CVE-2021-44228,
- Hinzufügen einer neuen CVE (CVE-2021-26855, Schwachstelle in Microsoft Exchange) mit neuen Kritikalitätswerten innerhalb eines Netzwerkes eines WVUs ohne ausreichende Netzwerksegmentierung zwischen dem Büro- und ICS-Netzwerk und
- die Betrachtung derselben CVE innerhalb eines Netzwerkes eines WVUs mit ausreichender Netzwerktrennung und Netzwerkzonen zwischen dem Büro- und ICS-Netzwerk

betreffen, um das Systemverhalten und die daraus folgenden Modifikationen des Kohärenzmodells zur Bewertung und Priorisierung der CVE aufzeigen zu können.

5.5.9 Prozessschritt bei Änderung der CVE-Eintrittswahrscheinlichkeit

In diesem Kapitelabschnitt wird das Systemverhalten bezugnehmend auf Veränderungen der Eintrittswahrscheinlichkeiten thematisiert. Erfolgt die Betrachtung der Auswirkungen der CVE-2021-44228 hinsichtlich des von der CVE verursachten Schadensausmaßes, so können Modifikationen zu Temporal Metrics, darunter auch Änderungen am Exploit Code Maturity und an der CVE-Eintrittswahrscheinlichkeit, der Priorisierungsstrategie und damit auch die erreichten C-Value, I-Class, E-Class und F-Value verändert werden. Um diesen Vorgang simulativ darstellen zu können, wird zunächst angenommen, dass die CVE-2021-44228 nach wie vor den TCP/IP-Port 389, den SCADA-Server (MTU) und die Zone 4, mit dem Remediation Level „Workaround (W)“ sowie die bereits definierten Kritikalitäten betrifft. Während jedoch die Erstbewertung der CVE-2021-44228 eine „Exploit Code Maturity“ mit der (POC)-Deklaration (siehe Anhang A.7) hat, wird in diesem Beispiel der Wert auf „Functional (F) umgeändert. Das bedeutet, dass der CVE-Angriffsvektor nun durch einen lauffähigen und freizugänglichen Code sowie dazugehörigen Toolkits von jedem ausgeführt werden kann. Während der Angriffsvektor sich verschlechtert, verbessert sich die CVE-Eintrittswahrscheinlichkeit.

Hierbei wird der ursprüngliche Eintrittswahrscheinlichkeitswert von 3 auf 1 reduziert. Wird dieses Gedankenspiel weiter ausgeführt, muss sich der entsprechende F-Value, der sich aus der Zusammenführung der I-Class und E-Class zusammensetzt, verändern. Gemäß der Berechnungsmethodik des Kohärenzmodells wird erwartet, dass sich der Schadensausmaßwert „C-Value“ verschlechtert (C-Value > 21), wobei der neu errechnete Wert nach wie vor der I-Class „3“ zugeordnet werden kann. Während der neu zugewiesene Wert der I-Class „3“ zugeordnet wird und konstant bleibt, muss der E-Class-Wert von 3 zu 1 verändert werden, was auch gleichzeitig eine Auswirkung auf den F-Value mit sich bringt. Der Berechnungsmethodik des Portfolios zufolge ergibt sich aus der Multiplikation der I-Class mit der E-Class der F-Value, der durch die Neuberechnung vom ursprünglichen Wert „9“ (siehe Anhang A.13) auf 3 reduziert wird und somit der CVE-Priorisierungsstrategie „C“ zugeordnet wird. In den Anhängen A.24, A.25 und A.26 werden die bereits beschriebenen Änderungen und das zu erwartende Systemverhalten dargestellt.

Der neuen Berechnung zufolge handelt es sich bei dieser Betrachtung, ableitend aus den veränderten externen Informationen um eine CVE, die zwar ein hohes Schadensausmaß verursachen kann, aber in der freien Wildbahn kaum ausgenutzt wird. Die C-Priorisierungsstrategie spiegelt diese Tatsache wider, in der eine zeitliche Reihenfolge zur Beseitigung dieser CVE definiert wird. Allerdings müssen die erreichten Priorisierungsstrategien in Abhängigkeit der personellen und fachlichen Ressourcen und in Abhängigkeit zu anderen Priorisierungsstrategien verstanden werden. In diesem Fall und sofern keine weiteren höher eingestuften Priorisierungsstrategien definiert sind (z. B. A oder B), kann die Empfehlung erfolgen, dass die CVE unverzüglich mit Abhilfemaßnahmen beseitigt werden muss. Stehen höhere Priorisierungsergebnisse an, so müssen diese von der zeitlichen Reihenfolge vor der CVE-2021-44228 behoben und beseitigt werden. Hierdurch können die begrenzten personellen Kapazitäten besser und zielgerechter geplant und eingesetzt werden. Gleichwohl, wie die Eigeninterpretation der einzelnen Priorisierungsstufen ausfallen, erhalten die Entscheidungsträger eine objektive und nach Faktenlage basierte Priorisierungsstrategie, nach der sie ihre Abhilfemaßnahmen definieren und koordinieren können.

5.5.10 Prozessschritt bei Änderung der CVE-Zuordnungswerte

Wie verhält sich das Kohärenzmodell, wenn bspw. die Ursache der Verwundbarkeit und somit der Einsatz der Softwaremodule und Hardwaremodule im Zuge der Behebungsmaßnahmen vollständig eliminiert werden? Dies kann gelingen, wenn die Softwaremodule deinstalliert oder die Hardwaremodule durch andere vergleichbare Hardwaremodule anderer Hersteller ersetzt werden. Technisch betrachtet können auch andere Mechanismen eingesetzt werden, um die Gefahrenquellen vollständig zu eliminieren. Gleichwohl welche Mechanismen zur Eliminierung der Gefahrenquellen eingesetzt werden, führt dieser Umstand zu einem anderen Ergebnis der CVE-Priorisierung. Gemäß dieser Prämisse muss IRET bei Nichtvorhandensein der Gefahrenquelle die CVE-2021-44228 zurückstellen, da die Eigenschaften dieser CVE nicht mehr auf das ICS-Netzwerk zutreffen und somit keine Schäden mehr verursachen können. Für diese Postulierung wird die Exploit Code Maturity als High eingestuft. Führt der Analyst die Bewertung nun aufgrund der neuen Konfigurationseigenschaften sowie der neuen Software- und Hardwareintegration erneut durch, so kann er die neuen CVE-Zuordnungswerte mit „kein Port ist betroffen“, „kein System ist betroffen“ und „keine Zone ist betroffen“ deklarieren.

Trifft eine CVE nicht auf die ICS-Netzwerkkomponenten zu, so kann die CVE-Eintrittswahrscheinlichkeit als vernachlässigbare Größe betrachtet werden, dessen Wert durch den Analysten manuell auf 1 gesetzt wird (siehe Anhang A.27 E-Class). Durch das Eingeben der neuen CVE-Zuordnungswerte und des CVE-Eintrittswahrscheinlichkeitswerts errechnet IRET das Schadensausmaß, den C-Value, die I-Class und die E-Class neu und ermittelt auf Basis der neuen Berechnung eine neue Priorisierungsstrategie. Die IRET-Berechnungswerte untermauern die erwarteten Ergebnisse und stellen die CVE-2021-44228 auf Grund der neuen Orientierungsmerkmale zurück, was im System als „Deprioritize“ deklariert wird (siehe Anhänge A.28 und A.29).

5.5.11 Prozessschritt bei Hinzufügung neuer Kritikalitäten und CVE

In diesem Kapitelabschnitt wird eine neue Bewertungsgrundlage postuliert, die sich an den spezifischen Eigenschaften eines mittelständischen WVUs ohne ausreichende Netzwerksegmentierung orientiert. Diese spezielle Netzwerklandschaft zeigt eine logische und physische Verschmelzung der beiden Welten miteinander, in der keine Netzwerktrennung zwischen dem Büro- und ICS-Netzwerk vorhanden ist.

Mit anderen Worten vernachlässigen die Systemverantwortlichen das Prinzip „Defense in Depth“, indem sie ihre Soft- und Hardwarekomponenten nicht nach ihrem erforderlichen Schutzbedarf separieren. Hierdurch entsteht die Gefahr, dass die CVE, die nur die Büro-Netzwerke kompromittieren, auch eine Gefahr für die ICS-Komponenten darstellen. So lässt sich der Auswirkungsgrad eines erfolgreichen Angriffs nicht nur isoliert in einem gesonderten Segment, sondern in allen Bereichen entfalten, sodass es zu einer Infiltrierung der versorgungsrelevanten technischen Komponenten kommen kann.

Um dieses Szenario simulieren zu können, wird die CVE-2021-26855 herangezogen, die eine bestimmte Schwachstelle in der Microsoft Exchange-Umgebung ausnutzt, um eine Infiltrierung durchführen zu können. Zur Evaluierung dieser CVE müssen allerdings die Orient-Stammdaten abhängig der zu betrachtenden Netzwerkarchitektur und Konfigurationsprofile neu vergeben werden. Die CVE-2021-26855 betrifft den TCP/IP-Port 443, den Exchange-Server, der aufgrund des Nichtvorhandenseins ausreichender Netzwerkzonen und -segmenten der Zone 1 zugeordnet werden kann. Hierdurch muss die Zone 1 beim Setzen der Kritikalität auf Grund der bestehenden Architektur dem Wert „3“ zugeordnet werden. Zudem kann die Kritikalität des TCP/IP-Ports 443 der Stufe „2“ zugeordnet werden. Diese Angaben können über die „Set Criticality“-Funktion in IRET eingebettet werden. Die weiteren Angaben zu den Redundanzkritikalitäten müssen auch entsprechend der Netzwerkeigenschaften bestimmt werden. Hierbei werden die Einträge zu „nur Systeme des Büronetzwerkes sind betroffen“, „betroffene Systeme sind nur innerhalb des ICS-Netzwerkes“ sowie „multiple Systeme sind betroffen“ alle auf Grund der fehlenden physischen Netzwerksegmentierung und den Redundanzen ebenfalls auf 3 hochgestuft (siehe Anhang A.30).

Diese Art der Klassifizierung kann auf die Vererbungsstrategie zurückgeführt werden, in der die Kritikalität aller Systeme im Sinne des Maximalprinzips als kritisch eingestuft werden muss, da diese sich unabhängig ihrer Anwendung oder des Schutzbedarfes in einer einzigen Zone befinden und sich somit die Kritikalität dieser Zone auf alle Systeme übertragen lässt.

Ferner wird postuliert, dass die Systeme keine Redundanzen besitzen und somit als SPOF eingestuft werden können, was die Identifizierung und Einstufung der einzelnen Systeme überflüssig macht. Die Aufnahme der CVE erfolgt über die „Add CVE“-Funktion (siehe Anhang A.31), in der der Wert zum „Exploit Maturity Code (e_4)“ mit „Functional (F)“ und der Wert zum „Remediation Level (e_5)“ mit „Official Fix (O) deklariert wird. Durch die IRET-Umrechnungsfunktion wird der Wert „3“ der Subdeterminante e_4 und der Wert „1“ der Subdeterminante e_5 zugerechnet. Als nächstes können die Zuordnungswerte über das Dialogfenster „Evaluate CVE“ eingetragen werden, indem die betroffene TCP/IP „433“, „nur die Systeme des Büronetzwerkes sind betroffen“ und die „Zone 1“ ausgewählt werden (siehe Anhang A.32).

Im nächsten Schritt rechnet IRET im Hintergrund alle Werte der Subdeterminanten, den C-Value und weist den C-Value der passenden I-Class zu. So wird das CVE-Schadensausmaß mit dem C-Value auf „20“ berechnet und der I-Class „3“ zugeordnet (siehe Anhang A.33). Nach Evaluierung der Abhilfemaßnahmen erfolgt im vorletzten Schritt die Bestimmung der CVE-Eintrittswahrscheinlichkeit bzw. die E-Class, die mit dem Wert „3“ festgelegt wird (siehe Anhang A.34).

Die endgültige Priorisierungsstrategie wird im Dialogfenster „Final Decision“ auf Grundlage der eingegebenen Werte und der Berechnungsmethodik des Kohärenzmodells berechnet (siehe Anhang A.35). Die Auswertung verdeutlicht, wie die spezifischen Netzwerkeigenschaften eines Betreibers technischer Basisinfrastrukturen als objektive Grundlage einer CVE herangezogen werden können und kann zudem im erweiterten Sinne durch die Aufführung des nachfolgenden Gegenbeispiels untermauert werden.

5.5.12 Prozessschritt bei Änderungen der Kritikalitäten

Um die Kritikalität der einzusetzenden ICS-Netzwerkkomponenten zu verringern, wird die ICS-Netzwerklandschaft des zuvor betrachteten WVUs in mehrere Zonen und Segmenten nach dem jeweiligen Schutzbedarf separiert. Hierfür wird eine explizite logische und physische Netzwerktrennung zwischen dem Büronetzwerk und dem ICS-Netzwerk implementiert, um den Auswirkungsgrad eines Angriffes auf die einzelnen Netzwerke stark einzugrenzen. Zudem werden die Systeme physisch in separaten Brandabschnitten redundant ausgelegt.

Nach dem Prinzip der strikten Netzwerktrennung und den Redundanzauslegungen kann nun postuliert werden, dass die Kritikalität der Orient-Stammdaten nun anders ausfallen könnte. Diese Änderung bzw. die Überarbeitung der bereits getroffenen Kritikalität stellt für sich einen eigenen Anwendungsfall dar, der im nachfolgenden Bild 41 dargestellt wird:

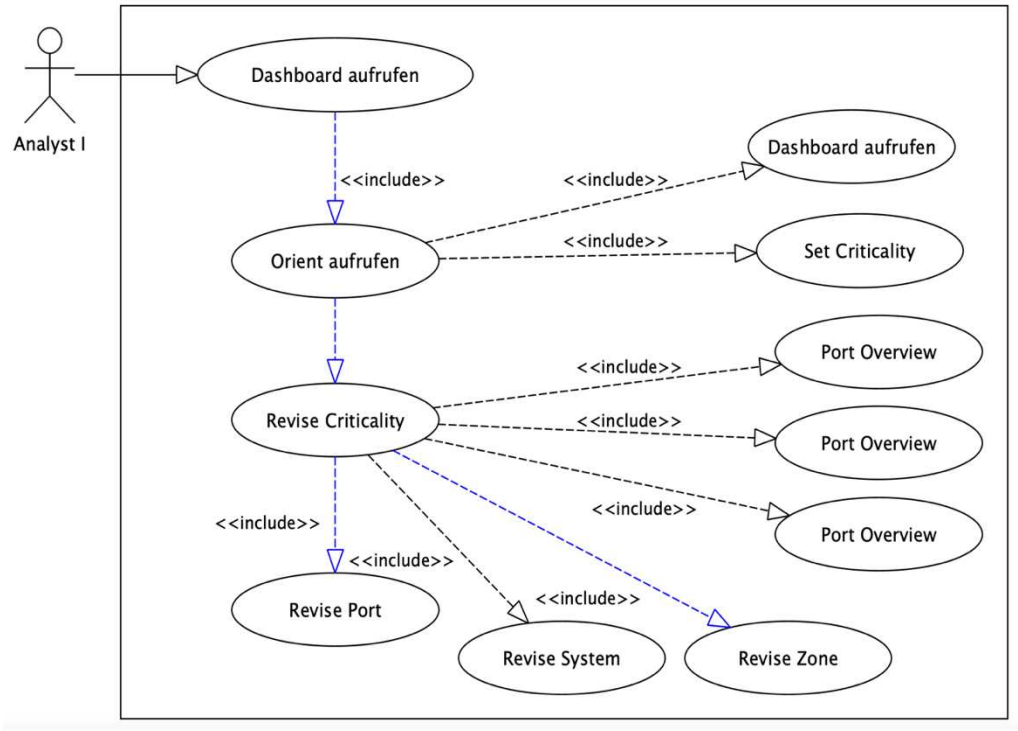


Bild 41: Use Case: Revise Criticality (Quelle: Eigene Darstellung)

Die Modifikation der betroffenen Kritikalitäten erfolgt über das Dialogfenster „Revise Criticality“ innerhalb der Orient-Funktionen (siehe Anhang A.36). So können zunächst mehrere Zonen hinzugefügt und die entsprechenden Kritikalitäten klassifiziert werden. Dabei wird der Kritikalitätswert der Zone 1 mit Hilfe der Such- und Überschreibungsfunktion von „3“ auf „1“ heruntergestuft (siehe Anhang A.37). Insgesamt werden fünf Zonen definiert, um die Netzwerke des Büro- und ICS-Netzwerkes ausreichend voneinander separieren zu können (siehe Anhang A.38). Die weiteren angegebenen Stammdaten können über die dazugehörigen Datenblätter überprüft und besichtigt werden (siehe Anhänge A.39 und A.40).

Um die CVE-2021-26855 nach den neuen Systembegebenheiten zu evaluieren kann die Funktion „Revise CVE Evaluation“ aufgerufen werden, in der die CVE-Zuordnungswerte neu berechnet werden können. Hierbei werden dieselben Zuordnungswerte eingetragen, die auch in der vorherigen CVE-Auswertung eingetragen wurden. Durch die veränderten Kritikalitätswerte rechnet IRET das CVE-Schadensausmaß neu (siehe Anhang A.41). Die Ergebnisse der Neuevaluierung der CVE-2021-26855 werden in den beiden Dialogfenstern „CVE Evaluation Results“ und „CVE Final Decision“ aufgeführt, in der der C-Value als CVE-Schadensausmaß mit dem Wert „8“, die dazugehörige I-Class mit dem Wert „1“ und die I-Class als Eintrittswahrscheinlichkeitswert mit „3“ ausgegeben werden (siehe Anhang A.42). Im Dialogfenster „CVE Final Evaluation“ werden nun die I-Class und die E-Class zusammengeführt und der Priorisierungsklasse „F“ zugeordnet (siehe Anhang A.43). So kann nun ersichtlich werden, wie die Veränderungen der Systembegebenheiten, sowie Mängel oder Vorhandensein von sicherheitstechnischen Mechanismen einen direkten Einfluss auf die CVE-Bewertungs- und -Priorisierungsstrategien haben.

So kann in Anbetracht der ausgeführten Netzwerksegmentierungen und der Auslegung von Redundanzen das Schadensausmaß derselben CVE maßgeblich beeinflusst werden und zur Bestimmung einer anderen Priorisierungsstrategie führen, in der dieselbe CVE in zeitlicher Reihenfolge anders eingestuft werden kann. Auch hier ergibt sich nun die Möglichkeit die erreichte CVE-Priorisierungsstrategie mit qualitativen Kommentaren und Empfehlungen zu komplementieren und die Abhilfemaßnahmen bei Bedarf präziser zu definieren. Werden bspw. die ICS-Netzwerkkomponenten nur von zugewiesenen Verteidigungseinheiten des ICS-Netzwerkes überwacht und administriert, während die Büro-Netzwerkkomponenten vom IT-Personal des Büro-Netzwerkes administriert werden, so können die für das ICS-Netzwerk zuständigen Analysten die CVE-2021-26855 trotz der F-Priorisierung gänzlich zurückstellen, da diese Abhilfemaßnahmen nicht von den operativen Verteidigungseinheiten des ICS-Netzwerkes ausgeführt werden und die CVE-2021-26855 durch die strikte Netzwerksegmentierung keinen Einfluss auf die ICS-Komponenten hat. Will der Analyst diesen Umstand durch IRET darstellen, so kann die CVE-Eintrittswahrscheinlichkeit bei einer erneuten CVE-Evaluation auf 1 zurückgesetzt werden, um die CVE nach den IRET-Regeln zurückstellen zu können. Die aufgeführten Beispiele zeigen, wie das Kohärenzmodell und IRET als Anwendungstool auf verschiedene Begebenheiten und verschiedene CVE reagieren. Allerdings stellen diese Beispiele eine Simulation dar, deren Machbarkeit, Plausibilität, Validität und Effizienz in einem industriellen Umfeld getestet und anhand von realen Anwendungsfällen evaluiert werden müssen. Zu diesem Zweck wurde das Kohärenzmodell und IRET für ein Jahr nach den gemeinsamen Entwicklungsphasen mit den Cybersicherheitsingenieuren und Netzwerkanalysten in einem industriellen Umfeld getestet.

6. Evaluierungsergebnisse

In den nachfolgenden Kapiteln werden die Evaluierungsergebnisse, Erkenntnisse und die Auswertung der Erfolgsevaluierung aufgeführt und anschließend kritisch diskutiert.

6.1 Technische und organisatorische Eigenschaften des Evaluierungsfeldes

Der Anwendungsbereich, in dem IRET zur industriellen Erfolgsevaluierung eingesetzt wird, befindet sich in der OT-Umgebung. Hier erfolgen Prozesse zur Anlagenüberwachung und -Steuerung im Bereich der Kohleförderung, der konventionellen Energieerzeugung (d. h. konventioneller fossilbasierter Kraftwerksbetrieb), des Betriebs von elektrischen Erzeugungsanlagen auf Basis der erneuerbaren Energien, bzw. regenerativen Energien, sowie Kopplungsprozesse zur Einspeisung und Weiterleitung der erzeugten elektrischen Energie in das Verteilnetz.

Die informationstechnische Netzwerkarchitektur ist durch logische OT-Zonen bzw. ICS-Zonen mit der entsprechenden Netzwerkplanung in fünf differenzierte Zonen separiert. Die Separierung erfolgt unter Berücksichtigung des jeweiligen Schutzbedarfs und betrifft Segmentierungsmechanismen wie Firewalls, DMZ, Sicherheitsgateways, Paketfiltering oder P-A-P-Strukturen.

Neben der restriktiven Separierung der OT-Zonen, wird das OT-Netzwerk durch weitere Firewalls von den Büronetzwerken (IT-Netzwerke) im ERP-Bereich logisch und physisch getrennt. Innerhalb der OT-Netzwerke werden informationstechnische und elektrotechnische ICS und Cyber-physische Systeme wie Sensorik, Aktorik, SPS, DCS und SCADA-Systeme eingesetzt.

Das OT-Netzwerk zählt zudem nach der verbindlichen Deklaration des § 11 Abs. 1 b des EnWG und § 8 a BSIG sowie gemäß der Deklaration der Anlagenkategorien und der dazugehörigen Schwellenwerte in der BSI-KritisV als eine KRITIS. Hierfür greift das OT-Netzwerk auf den holistischen präventiven Ansatz der Triangulation der Informationssicherheit (vgl. Koza/Öztürk, 2022a, S. 99 | Koza, 2022a, S. 2859 | Koza/Öztürk, 2021, S. 49-69 | Koza, 2022b, 49 f.) zurück. Betreiber dieser KRITIS müssen demnach ein ISMS nach DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27002 und DIN EN ISO/IEC 27019 einführen, das präventiv, korrektiv, reaktiv und detektierend zur Sicherstellung der Informationssicherheit vorrangig im Bereich der Energieerzeugung zur Erfüllung der verbindlichen Anforderung des IT-Sicherheitskataloges der BNetzA nach § 11 Abs. 1 b des EnWG eingesetzt wird.

Zur Erfüllung der Anforderungen aus dem Control A. 16 „Handhabung von Informationssicherheitsvorfällen“ der DIN EN ISO/IEC 27001, das Maßnahmen zur Detektion und Früherkennung von Schwachstellen, Beurteilung und Priorisierung und sowie zur Entwicklung und Koordinierung von Mitigation- und Behebungsmaßnahmen beschreibt, wird in der OT ein zentrales IRT mit sieben Cybersicherheitsingenieuren und Sicherheitsanalysten eingesetzt (vgl. DIN EN ISO/IEC 27001, 2017, S. 28).

Die Akteure leiten ihre Analyseentscheidungen an jeweils weitere dezentrale operative Verteidigungseinheiten in den jeweiligen OT-Abteilungen weiter, die die operative Umsetzung der Abhilfemaßnahmen und Beseitigungsmaßnahmen (Responses) oder Patchs ausführen.

6.2 Ergebnisse der industriellen Erfolgsevaluierung

6.2.1 Erkenntnisse während der Konzeptualisierungs- und Entwicklungszeit

Im Verlauf der zwei-jährigen Konzeptualisierungs- und Entwicklungsphase wurden insgesamt zehn interne Funktionstests mit hierfür extrahierten anonymisierten fiktiven Orient-Datensätzen (d. h. Ports, OT-Systeme und logische Zonen) aus OT-Netzwerken durchgeführt. Die Evaluierung der Logik des Kohärenzmodells sowie des Prototyps „IRET“ wurde in diesem Zusammenhang innerhalb eines iterativen Prozesses während der Gesamtlaufzeit der Entwicklungsprozesse als Begleitungsschritt ausgeführt. In der primären Betrachtung stand die Evaluierung der Logik, die Funktionstüchtigkeit, Reaktionsvielfalt sowie Entscheidungsqualität des Kohärenzmodells und IRET. Bei der Plausibilitätsprüfung der ersten vier Phasen sollte demzufolge als Erstes überprüft werden, ob die Logik von IRET und die von IRET berechneten Ergebnisse und Priorisierungsstrategien von den Cybersicherheitsingenieuren und Sicherheitsanalysten Expertenergebnisse reproduziert werden können. Hierbei sollte die Überdeckungsgleichheit der Expertenergebnisse mit den automatisierten IRET-Ergebnissen abgeglichen werden.

Als Zweites sollte im Detail überprüft werden, ob die Plausibilität der IRET-Ergebnisse auch mit den individuellen Sicherheitserkenntnissen der Cybersicherheitsingenieure deckungsgleich ist. Dabei wurde der Frage nachgegangen, ob die Orient-Stammdaten (Kritikalitätsbestimmung der Ports, der Systeme und jeweiliger Redundanzen und Zonenkritikalitäten) und die erweiterten Subdeterminanten wie Exploit Code Maturity, Remediation Level, und die Einbettung der CVE-Eintrittswahrscheinlichkeit sich tatsächlich als objektive Entscheidungsgrundlagen zur CVE-Bewertung eignen würden. Die daraus resultierenden Erkenntnisse, die als Rückkopplungsschleife zur Optimierung von IRET und des Kohärenzmodells eingearbeitet wurden, lassen sich in der nachfolgenden Auflistung präzisieren:

- **Vorkonfiguration der Standard-Subdeterminanten Teil I:** Um die CVE bzw. Schwachstellen, die das OT-Netzwerk nicht betreffen und somit explizit auf die vorhandenen Schwachstellen in den Büronetzwerken zurückzuführen sind, wie bspw. Zero Day Exploits im Exchange-Server, erfolgreich filtern zu können, wurden folgende Vorkonfigurationen der Orient-Stammdaten hinzugefügt:

    1. Vorkonfiguration der Portskritikalitäten:
        a. „No port is affected“
    2. Vorkonfiguration der Redundanzkritikalitäten:
        a. „No system is affected“
        b. „Only systems in the office network are affected“
    3. Vorkonfiguration der Zonenkritikalität:
        a. „No OT zone is affected“

- **Vorkonfiguration der Standard-Subdeterminanten Teil II:** Um die CVE bzw. Schwachstellen, die das OT-Netzwerk mehrmals betreffen und somit einen Einfluss auf unterschiedliche Zonen und Systeme darstellen, erfolgreich selektieren zu können, wurden folgende Vorkonfigurationen der Orient-Stammdaten hinzugefügt:

    1. Vorkonfiguration der Redundanzkritikalitäten:
        a. „Multiple system are affected“
    2. Vorkonfiguration der Zonenkritikalität:
        a. „Multiple OT zones are affected“

- **Vorkonfiguration der Standard-Subdeterminanten Teil III:** Um die CVE bzw. Schwachstellen, die das OT-Netzwerk nicht direkt über eine bestimmte TCP/IP Portanbindung betreffen aber dennoch als netzwerkbasierte Angriffe ausgeführt werden können (z.B. abgelegte Dateiviren auf Netzwerken, Mailviren, versteckte maliziöse Schadcodes durch Phishingangriffe als Makroviren) erfolgreich selektieren zu können, wurde folgende Vorkonfigurationen der Orient-Stammdaten hinzugefügt:

    1. Vorkonfiguration der Redundanzkritikalitäten:
        a. „Multifold distribution“

- **Vorkonfiguration der Standard-Subdeterminanten Teil IV:** Um die CVE bzw. Schwachstellen, die das OT-Netzwerk nicht direkt über eine bestimmte TCP/IP Portanbindung bzw. netzwerkbasierten Vektor betreffen aber als sogenannte Insider Threats als physischer Angriffsvektor ausgeführt werden können, erfolgreich selektieren zu können, wurden folgende Vorkonfigurationen der Orient-Stammdaten hinzugefügt:

1. Vorkonfiguration der Portskritikalitäten:
   a. „Insider Threats“

- **Vorbewertung der Vorkonfigurationswerte:** Zur globalen Quantifizierung der Vorkonfigurationswerte wurde eine 0-Wertung als neutrale Bewertung zur Trennung der IT-spezifischen CVE von den OT-spezifischen CVE hinzugefügt. Nachfolgend wird die Zuordnung der Wertungen zu den Vorkonfigurationswerten aufgelistet:

Tabelle 22: Vorkonfigurationen in IRET (Quelle: Eigene Darstellung)

Vorkonfiguration	Wertung
No port is affected	**0**
No system is affected	**0**
Only systems in the office network are affected	**0**
No OT zone is affected	**0**
Multiple systems are affected	**3**
Multiple OT zones are affected	**3**
Multifold distribution	**3**
Insider Threats	**3**

- **Debugging**: Die Lokalisierung und Behebung von einzelnen Laufzeitfehlern, logischen Fehlern aus denen die Notwendigkeit zur Generierung und Präzisierung von Default-Feldern und Pflichtfeldern abgeleitet und nachtragend in IRET eingebettet wurde.

6.2.2 Evaluierungsergebnisse aus der ein-jährigen industriellen Erfolgsevaluierung

In der letzten Forschungsphase wurde IRET für eine ein-jährige industrielle Nutzung freigegeben. Nachfolgend werden die einzelnen Ergebnisse aus der fünften Forschungsphase aufgeführt. Insgesamt wurden 60 CVE über einen Evaluierungszeitraum von 12 Monaten durch zwei Experten des IRT in einem Parallelverfahren wie folgt ausgewertet: Im ersten Durchlauf haben die Analysten in einem manuellen Verfahren 60 CVE ausgewertet. Die manuelle Auswertung basiert auf die Erfahrungsexpertise und die subjektiven Erfahrungswerte der Analysten und wird innerhalb von Expertenrunden operationalisiert. Die Terminierung, Koordinierung sowie die Dokumentation der Entscheidungen bzgl. der CVE-Auswertungs- und Priorisierungsprozesse wurden in einem Ticketsystem realisiert.

Beide Analysten besitzen die notwendigen akademischen Qualifikationen und domänenspezifisches Fachwissen sowie langjährige praktische Expertisen als OT-Netzwerkanalytiker und Cyber Security Ingenieure im Bereich der OT-Energieerzeugung und OT-Energieverteilung, was letztlich ein explizites Domänenwissen sowohl im Bereich der Erzeugung der elektrischen Energie als auch der Kopplung sowie der Verteilung dieser in das Verteilnetz beinhaltet. Mit dem Einsatz dieser beiden Experten kann in einem simultanen Verfahren eine effiziente Begutachtung durchgeführt werden, da beide wesentliche kritische Bereiche zur Energieerzeugung und -verteilung gleichzeitig evaluiert werden können.

Die 60 eingebetteten CVE (Tabelle 23) werden über ein externes Selektionsverfahren durch das dCERT vorbestimmt. Hierfür nutzen die Analysten die technischen Möglichkeiten des dCERTs, indem sie mit Hilfe eines Zuordnungsverfahrens zunächst ihre ICS und OT-Software- und Hardwarekomponenten mit den dazugehörigen Herstellern, Editionen und Versionen festlegen, die für den sicheren Betrieb der OT-Netzwerke eine signifikante Rolle spielen. Die dCERT-Applikation übernimmt die eingegebenen Daten und ordnet die weltweit identifizierten CVE automatisiert zu den betroffenen ICS-Komponenten. Hierdurch entsteht die Möglichkeit zunächst nur die CVE in die Auswertungs- und Priorisierungsanalyse einzubetten, die die eingesetzte ICS tatsächlich betreffen.

Als grundlegende Vorselektion werden alle CVE in die Analyse eingebettet, die einen CVSS-Score von 4,0 aufweisen. Um Rückschlüsse auf die kritischen und analysierten CVE-Daten zu verhindern, werden die CVE-IDs im Anhang B.1 tabellarisch und pseudonymisiert aufgeführt.

In einem Parallelverfahren haben die Analysten exakt dieselben 60 CVE zwecks automatisierter Analyse und Priorisierung in IRET eingebettet und ihre Analyse- und Priorisierungsprozesse auf Basis der bereits definierten und festgelegten Orient-Stammdaten operationalisiert. Die Festlegung der Orient-Stammdaten wird als erster Prozessschritt zur Bestimmung der vorhandenen objektiven Ports-, Redundanz- und Zonenkritikalitäten in einer Expertenrunde ausgeführt. Der Grund dafür ist der methodisch-logische Ansatz von IRET, da die beiden Analysten in der Orientierungsphase zunächst in einer gemeinsamen Runde ihre system- und netzwerkspezifischen Umgebungen einheitlich, nach Faktenlage und der internen Systemeigenschaften bewerten müssen.

Damit wird sichergestellt, dass die CVE-Bewertungsgrundlage für die beiden Analysten und auch für weitere Analysten objektiv gleichbleibt. Die gemeinsamen Orient-Stammdaten dienen somit als Bewertungsgrundlage und erlauben es den Analysten, die CVE-Priorisierungsstrategien unabhängig des Entscheidungsträgers zu konstruieren. Die im Anhang B.2 definierten Metadaten stellen die Entscheidungen der beiden eingesetzten Verfahren (Expertenbewertung und IRET-Bewertung) gegenüber.

Um die Zeiteffizienz der beiden Verfahren miteinander vergleichbar zu machen, wurde die Zeit zur Initialisierung und Durchführung der beiden Verfahren zur Expertenbewertung und IRET-Bewertung gemessen. Die im Anhang B.3 aufgeführte Tabelle stellt die gemessene Zeit pro CVE dar.

6.3 Auswertung der Ergebnisse der industriellen Erfolgsevaluierung

Um die Auswertung von IRET und des Kohärenzmodells vollziehen zu können, werden die in den anfänglichen Forschungsphasen definierten Zielsetzungen (Bild 20) herangezogen und nacheinander bewertet.

6.3.1 Effizienter Entscheidungsprozess zur Reduzierung der FP- und FN-Rate

Die erste Zielsetzung kann anhand der Gegenüberstellung der quantifizierten Trefferquote der FP und FN der Expertenbewertung gegenüber der quantifizierten Trefferquote der TP und TN der IRET-Bewertung errechnet werden. Hierbei gilt der folgende Grundsatz: Die Expertenbewertung basiert im Detail auf der selektiven Wahrnehmung des Entscheidungsträgers und kann infolgedessen auf seine individuelle Fachexpertise, Knowhow und Salienz zurückgeführt werden und stellt eine menschenabhängige Entscheidung dar. Im Gegensatz hierzu stellt IRET die Grundlage für eine objektive Entscheidung dar, da die Entscheidungskriterien zum einen aus den reellen System- Konfigurations- und ICS-Netzwerkeigenschaften extrahiert und zum anderen auf Basis von transparenten fachlichen Kritikalitäten eingestuft werden. Aus diesem Grund wird der Vergleichswert durch die Gegenüberstellung der einzelnen Ergebnisse der beiden Verfahren nach dem mathematischen Prinzip „Abdeckungsgrad und Effizienz“ neutral definiert.

Die Expertenbewertung lässt sich in der kumulativen Betrachtung auf 35 TPs (58 %) sowie auf 25 TNs (42 %) aufteilen (Bild 42).

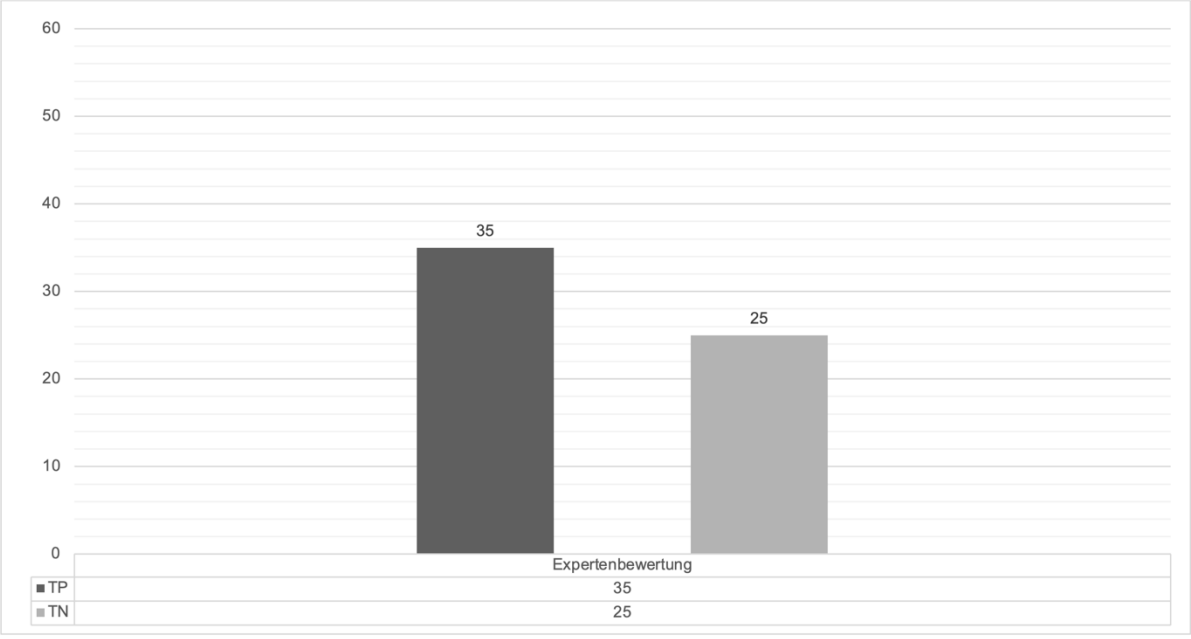


Bild 42: Übersicht der Expertenbewertung nach TP und TN (Quelle: Eigene Darstellung)

Die IRET-Bewertung lässt sich hingegen in der kumulativen Betrachtung auf 45 TPs (75 %) und 15 TNs (25 %) aufteilen (Bild 43).

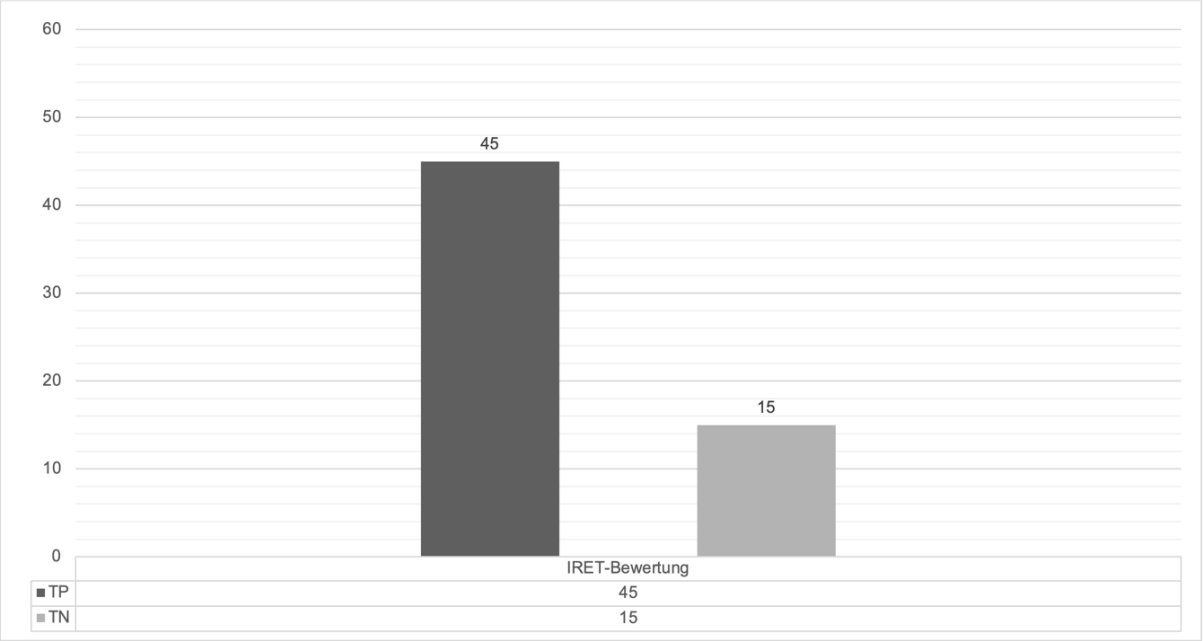


Bild 43: Übersicht der IRET-Bewertung nach TP und TN (Quelle: Eigene Darstellung)

Bei der ersten Betrachtung steht die Annahme, dass die Expertenbewertung insgesamt 10 CVE mehr als TN gegenüber der IRET-Bewertung klassifiziert hat. In der logischen Schlussfolgerung kann zunächst die Aussage getroffen werden, dass die Experten in der Gesamtheit ihrer Bewertung möglicherweise 10 CVE, die nach objektiver Grundlage als TP hätten bewertet werden müssen, fälschlicherweise als TN und damit als FN bewertet haben. Aus der sicherheitstechnischen Sicht bedeutet das, dass möglicherweise 10 wesentliche CVE nicht beseitigt und behandelt werden, da die Entscheidungsträger diese Schwachstellen auf „Zurückstellen“ depriorisiert haben. Um jedoch die aufgeführte Annahme zu verifizieren bzw. präzisieren zu können, müssen die einzelnen CVE-Bewertungsergebnisse zunächst gegenübereinander aufgestellt werden. Die Aufführung und der Vergleich der einzelnen Bewertungsergebnisse dienen der Ermittlung von Unstimmigkeiten, die sich in zwei grundsätzliche Bereiche teilen. Die erste Ausdifferenzierung betrifft die (TP<>TN-) Konstellation. Diese Konstellation tritt dann auf, wenn die CVE-Expertenbewertung auf TP und die CVE-IRET-Bewertung auf TN ausgelegt wird. Die zweite Ausdifferenzierung betrifft die (TN<>TP-) Konstellation. Diese Konstellation entsteht, wenn die CVE-Expertenbewertung auf TN und die CVE-IRET-Bewertung auf TP ausgelegt wird. Zusätzlich hierzu können auch Entscheidungsübereinstimmungen ermittelt werden, wenn die (TP<>TP-) Konstellation oder (TN<>TN-) Konstellation im direkten Verglich zu erkennen sind. Hieraus lassen sich sogenannte Treffer („Match“) und Nichttreffer („Mismatch“) deklarieren, um die Unstimmigkeiten bestimmen und kennzeichnen zu können. Das nachfolgende Diagramm (Bild 44) visualisiert die zwei Kurvenverläufe (gelb: IRET-Bewertung) (schwarz: Expertenbewertung), welche sich aus der Zusammenführung der einzelnen TP- und TN-Bewertungen der beiden Bewertungsverfahren ergeben und die Einzelbewertungen aus der im Anhang B.4 aufgeführten Tabelle illustrieren.

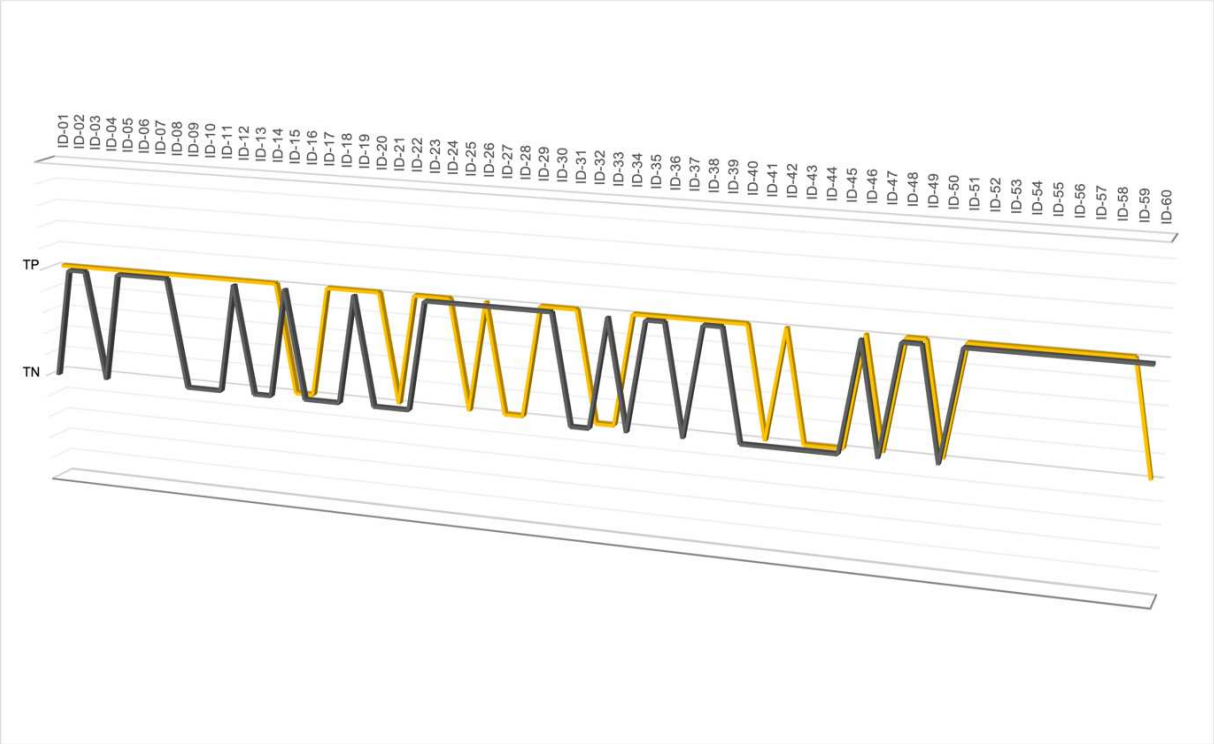


Bild 44: Gegenüberstellung der beiden Bewertungsverfahren (Quelle: Eigene Darstellung)

Den beiden visualisierten Kurvenverläufen und der im Anhang B.4 aufgeführten Tabelle (Spalte „Gegenüberstellung“) entnommen, existieren sowohl Übereinstimmungen als auch Unstimmigkeiten innerhalb der Entscheidungsfindung der beiden Bewertungsverfahren. Bei der Extrahierung der Kurvenverläufe nach Entscheidungsübereinstimmungen der beiden Verfahren können **38 Matches** definiert werden, die auf 9 (TN<>TN-) Konstellationen und auf 29 (TP<>TP-) Konstellationen zurückgeführt werden können (Bild 45 und Anhang B.5).

Bei einer weiteren Extrahierung der Kurvenverläufe nach unstimmigen Entscheidungen der beiden Verfahren können jedoch **22 Mismatches** definiert werden, die im Detail auf 16 (TN<>TP-) Konstellationen und damit als FN und auf 6 (TP<>TN-) Konstellationen als FP zurückgeführt werden können (Bild 46 und Anhang B.6).

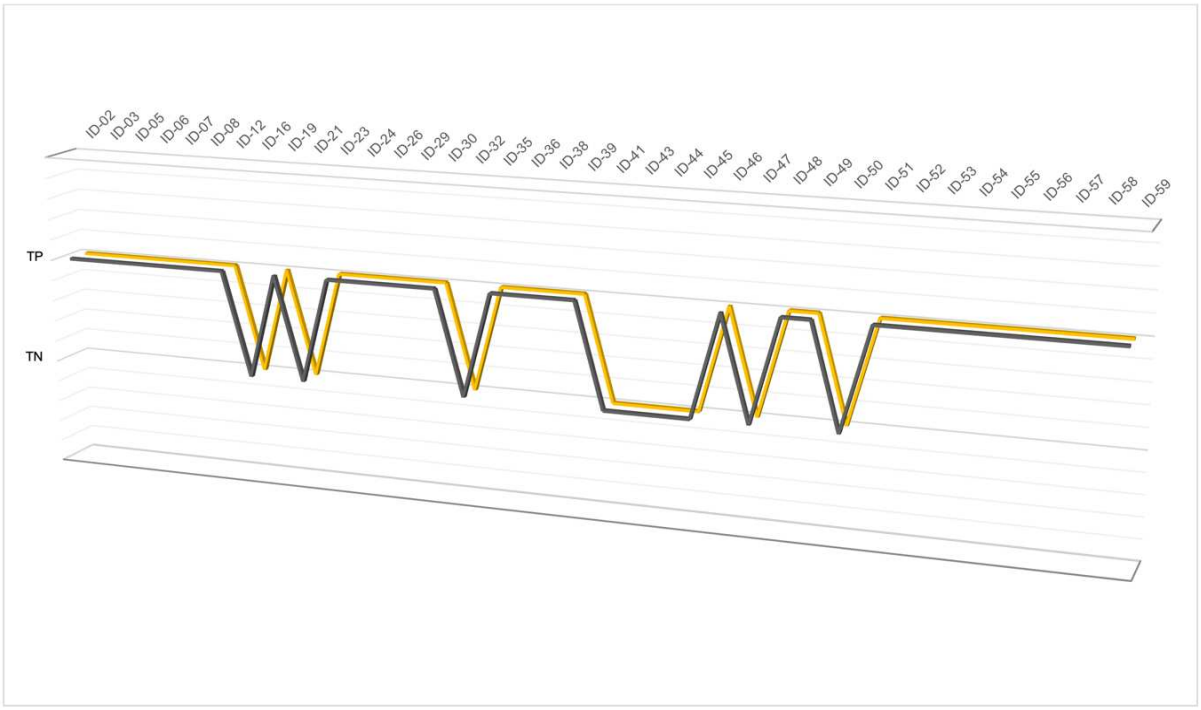


Bild 45: Übereinstimmungen der CVE-Bewertungen der beiden Bewertungsverfahren (Quelle: Eigene Darstellung)

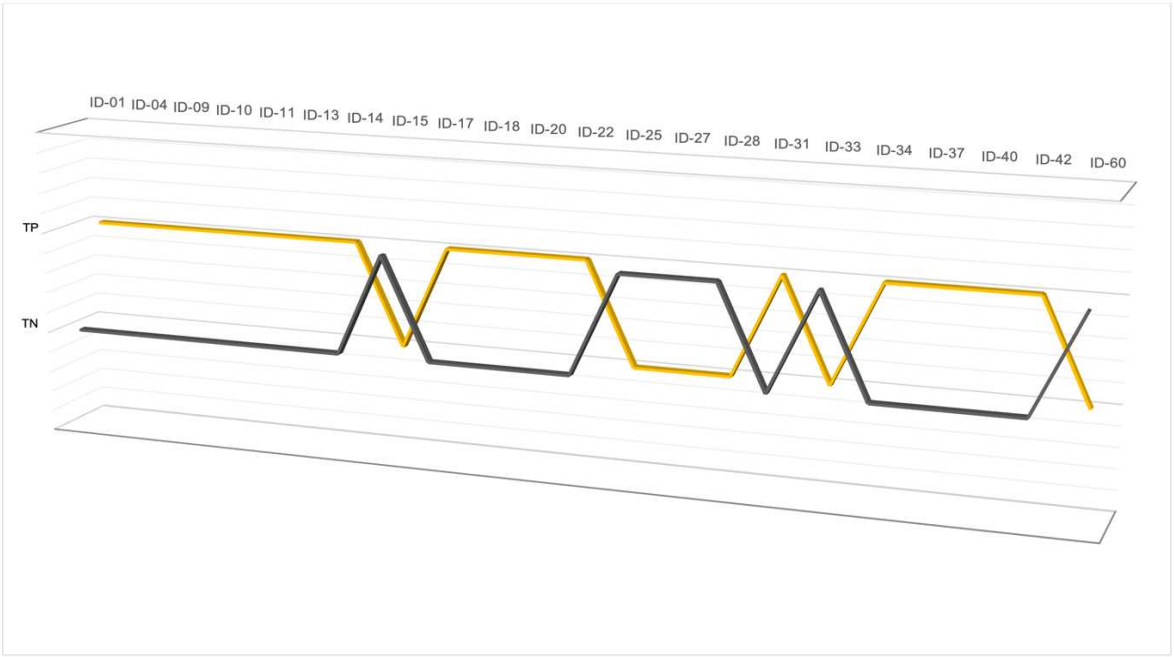


Bild 46: Unstimmigkeiten der CVE-Bewertungen der beiden Bewertungsverfahren (Quelle: Eigene Darstellung)

Aus der obigen Extrahierung kann bezugnehmend zu der oben aufgeführten Annahme geschlussfolgert werden, dass in der Expertenbewertung in der Summe **6** CVE (ID-15, ID-25, ID-27, ID-28, ID-33, ID-60 im Anhang B.6) als **TP** ausgewertet wurden, welche jedoch auf Grundlage von objektiven Entscheidungskriterien auf Basis des anfallenden Schadensausmaßes sowie der Angriffsvorhersage von IRET als **TN** klassifiziert wurden. Zusätzlich hierzu wurden auch weitere **16** CVE (ID-1, ID-4, ID-9, ID-10, ID-11, ID-13, ID-14, ID-17, ID-18, ID-20, ID-22, ID-31, ID-34, ID-37, ID-40, ID-42 im Anhang B.6) bei der Expertenbewertung als **TN** klassifiziert, die jedoch nach IRET als **TP** zu definieren und infolgedessen behandelt werden müssen. In der Gesamtbewertung führten die Expertenentscheidungen zu insgesamt 16 **FN** und 6 **FP.**

Die Folgen derartiger subjektiver Expertenentscheidungen können jedoch aus der sicherheitstechnischen Kausalitätsbetrachtung dazu führen, dass die den OT-Netzwerken zur Verfügung stehenden personellen und finanziellen Ressourcen im Sinne einer effizienten Ressourcenallokation nicht zielgerichtet und somit nicht sachdienlich eingesetzt werden. Diese Interpretation ergibt sich aus der Tatsache, dass bei einer subjektiven Entscheidungsfindung in der Summe sechs CVE zur sofortigen Behebung hätten veranlasst werden sollen, die aus der objektiven Betrachtung bezugnehmend zum anfallenden Schadensausmaß und zur Eintrittswahrscheinlichkeit hätten nicht behandelt werden müssen, da diese in der freien Wildbahn so gut wie nicht ausgenutzt werden. Allerdings beschränken sich die Folgen nicht nur auf die ineffiziente Ressourcenallokation, was auch eine monetäre Fragestellung darstellt. Die Folgen einer falschen Entscheidung können auch zu einer steigenden Fragilität und Vulnerabilität der OT-Systeme beitragen, da hierbei in der Summe bspw. 16 CVE, die nach IRET als TP priorisiert und behoben werden müssten, durch die Experten als TN klassifiziert wurden.

Dies bedeutet im Detail, dass 16 CVE, die aus objektiver Sicht hätten behoben werden müssen, weiterhin offenbleiben, da IRET diese aufgrund des errechneten kritischen Schadensausmaßes und der Angriffsvorhersage als TP priorisiert hätte. Wird die IRET-Entscheidung als Grundlage zur objektiven Entscheidungsfindung eingesetzt, so kann die nachfolgende Berechnung zur Effizienz und Abdeckung der beiden Verfahren herangezogen werden:

Tabelle 23: Berechnung der Effizienz und Abdeckung beider Verfahren (Quelle: Eigene Darstellung)

IRET-TP	***45 / 60***
IRET-TN	***15 / 60***
Effizienz der IRET-Bewertung (TP/ (TP+FP)) * 100	*(45 / (45+0)) x 100 =* ***100 %***
Abdeckung der IRET-Bewertung (TP/ (TP+FN)) * 100	*(45 / (45+0)) x 100 =* ***100 %***
Anzahl der identifizierten FP	***0***
Anzahl der identifizierten FN	***0***
Expertenbewertung TP	***35 / 60***
Expertenbewertung TN	***25 / 60***

Effizienz der Expertenbewertung (TP/ (TP+FP)) * 100	*(35 / (35+6)) x 100 =* ***85 %***
Abdeckung der Expertenbewertung (TP/ (TP+FN)) * 100	*(35 / (35+16)) x 100 =* ***69 %***
Anzahl der identifizierten FP	***6***
Anzahl der identifizierten FN	***16***

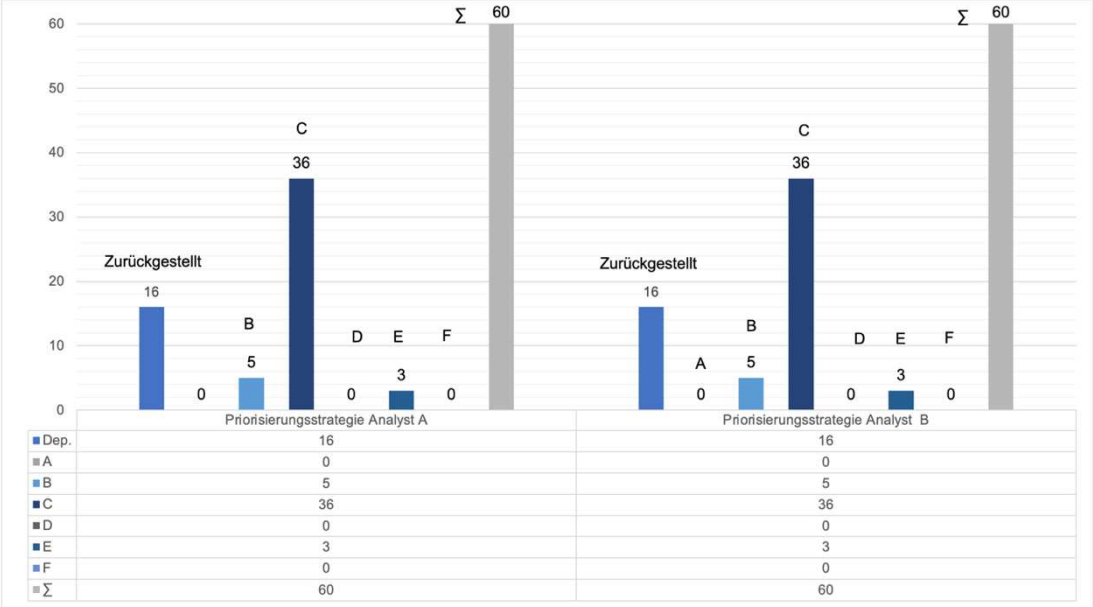
Durch die Gegenüberstellung der Effizienz und der Abdeckung der beiden Verfahren kann nun geschlussfolgert werden, dass IRET in der Summe 15% effizienter gegenüber Expertenentscheidungen agiert. Dies bedeutet, dass der IRET-Effizienzgrad nach den vorliegenden Datensätzen im Durchschnitt **15 %** höher liegt als der Effizienzgrad der Expertenentscheidung, was folglich zu einer besseren Ressourcenallokation und zu einer effizienteren Behebung der Schwachstellen führt. Zusätzlich hierzu erreicht IRET **31 %** mehr Abdeckungsrate gegenüber Expertenentscheidungen (69 %), da hierbei die Anzahl der Schwachstellen, die behoben werden müssen (TP), stetig steigt, während die Anzahl der FN kontinuierlich gegen null tendiert.

6.3.2 Definition objektiver und reproduzierbarer Entscheidungskriterien

IRET ermöglicht eine objektive Priorisierungsstrategie, indem es die für die Entscheidungsfindung relevanten Subdeterminanten des Kohärenzmodells nach Faktenlage identifiziert und nach einem einheitlichen Klassifizierungsschema zur Quantifizierung und Priorisierung der CVE in das Entscheidungsverfahren einbettet. Um die Objektivität und Reproduzierbarkeit der Ergebnisse entgegen prüfen zu können, wurden alle 60 CVE von zwei unterschiedlichen Personen in IRET eingebettet und durch die IRET-Logik automatisiert ausgewertet.

In den zwei unabhängigen Durchläufen wurde die Machbarkeit in unterschiedlichen Systemumgebungen (Systeme zur Kohleförderung, DCS und SCADA in der Energieerzeugung etc.) mit zwei unterschiedlichen Analysten getestet. Das Ziel war es, festzustellen, ob a) die Determinanten bzw. Subdeterminanten transportabel sind und somit auf unterschiedliche Systemumgebungen reagieren und b) ob andere Analysten ebenfalls in der Lage sind, die Methodik von IRET zur Bewertung der CVE zu a) anzuwenden. Es wurde festgestellt, dass die Metamodellierung von IRET einen wesentlichen Vorteil aufweist. Die Standard-Determinanten sind transportabel. Allerdings wurde auch festgestellt, dass die arithmetischen Klassifikationen in Systemumgebungen mit starker Netzsegmentierung angepasst werden müssen. Solche individuellen arithmetischen Anpassungen könnten dann durch die Metadefinition des Kohärenzmodells leicht vorgenommen werden (z. B. Konfiguration von Nullwerten). Ein Beispiel hierfür sind die CVE (CVE-2021-26855/26857/26858/27065), die Schwachstellen in den jeweiligen Microsoft Exchange Servern betreffen. Bestimmte CVE betreffen z. B. nur Büronetzwerke und haben aufgrund restriktiver Segmentierungen keinen Einfluss auf OT-Netzwerke. Durch die Integration einer Null-Wertung kann der Einfluss der Determinanten f_1, f_2, f_3, e_1, e_2 und e_3 (systemabhängige interne Determinanten) gleich Null gesetzt werden. Aufgrund der flexiblen Anpassungsfähigkeit von IRET (Änderungen im Rechenmodell, wobei die Logik des Rechenmodells erhalten bleibt) konnten die Analysten IRET für eine effiziente Bewertung von CVE operationalisieren.

Zudem kamen beide Analysten in den unabhängigen Testdurchläufen zu demselben Ergebnis bzw. den gleichen Priorisierungsstrategien und konnten die IRET-Ergebnisse somit unabhängig des Anwenders und der Entscheidungsträger reproduzieren (Bild 47). Der Grund dafür ist der methodisch-logische OODA-Ansatz von IRET, da die beiden Analysten in der Orientierungsphase zunächst in einer gemeinsamen Runde ihre system- und netzspezifischen Umgebungen evaluieren und somit auf Basis von faktischen und systemnahen Eigenschaften sowie einem einheitlichen Klassifizierungsschema die Bewertungsgrundlage für alle CVE global vordefiniert haben. Damit wurde sichergestellt, dass die Bewertungsgrundlage für beide Analysten und alle von ihnen integrierten CVE zu jederzeit gleich definiert ist.



	Priorisierungsstrategie Analyst A	Priorisierungsstrategie Analyst B
Dep.	16	16
A	0	0
B	5	5
C	36	36
D	0	0
E	3	3
F	0	0
Σ	60	60

Bild 47: Reproduzierbarkeit der Priorisierungsstrategien zwei unabhängiger Analysten (Quelle: Eigene Darstellung)

6.3.3 Zeitaufwandsminimierung durch IRET

Neben der bisherigen Evaluierung wurde auch der Zeitaufwand für die Erfassung, Bewertung und Dokumentation einer CVE in der Analogie zu den oben aufgeführten Testverläufen in zwei separaten Abläufen gemessen. Hierfür wurden zwei parallele Aktivitäten durchgeführt – der traditionelle Ansatz der Expertenbewertung und die IRET-Bewertung. Die im Anhang B.3 dargestellte Tabelle zeigt die einzelnen Messungen, die während der Evaluierungsphasen erfolgt sind.

Bild 48 zeigt die beiden Kurvenverläufe (Schwarz: Expertenbewertung, Gelb: IRET-Bewertung), welche die aufgeführten Messeinheiten pro CVE illustrieren.

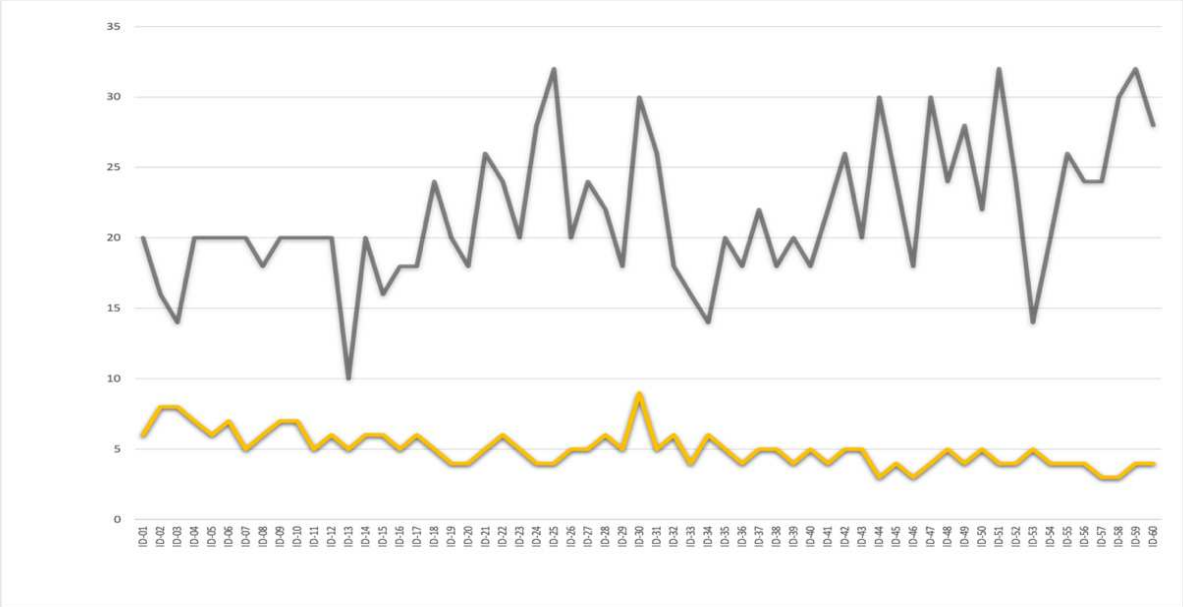


Bild 48: Messergebnisse der beiden Verfahren pro CVE (Quelle: Eigene Darstellung)

In der Gesamtheit zeigen die Messungen auf, dass der Zeitaufwand für die Bewertung der 60 integrierten CVE durch die Nutzung von IRET um **77 %**, d.h., von 21 Stunden und 44 Minuten auf 5 Stunden und drei Minuten reduziert werden kann. Wird die maximal benötigte Zeit für eine Expertenbewertung von 32 Minuten gegenüber der maximal benötigten Zeit für eine IRET-Bewertung betrachtet, liegt die Zeiteffizienz bei **71 %.** Wird jedoch der direkte Vergleichswert (siehe ID-59) herangezogen, so kann eine Zeiteffizienz von **87,5 %** erreicht werden, da der Zeitaufwand der Expertenbewertung von **32 Minuten** auf **4 Minuten** reduziert werden konnte.

Durch die implementierte IRET-Logik müssen demzufolge nur noch die CVE-Grundinformationen in das IRET eingebettet werden (Dialogfenster *Add CVE*, *Evaluate CVE*, und *Attack Prediction*). Im Hintergrund läuft die Bewertung und Priorisierung der CVE automatisch ab. Darüber hinaus wird der Zeitaufwand nicht nur für die Bewertung, sondern auch für die Dokumentation und das Reporting der CVE deutlich reduziert. Zudem integriert IRET die Möglichkeit, Kommentare und Empfehlungen als komplementäre qualitative Merkmale zur Vervollständigung der quantifizierten Priorisierungsstrategie abzugeben. So kann trotz des standardisierten Verfahrens der Bewertung einer CVE eine gewisse Flexibilität eingeräumt werden, um das subjektive Fachwissen und die Erfahrungswerte der Analysten für die Bewertung einer CVE in die Dokumentation und Bewertung einzubeziehen.

Einer der unerwarteten Vorteile ist, dass die Priorisierung von Maßnahmen zur Behebung einer CVE im Laufe der Zeit die Erstellung eines dynamischen internen Sanierungsplans ermöglicht hat. IRET klassifiziert das Ausmaß des Schadens an einer CVE, bestimmt jedoch gleichzeitig, welche zeitliche Priorisierung der Behandlung einer CVE zugewiesen werden kann. Darüber hinaus können CVE-Berichte in Form von Management-Summaries mit den notwendigen Informationen für die CVE-Bewertungen und -Reaktionen identifiziert, dokumentiert und zur Behebung an die zuständige Abteilung weitergeleitet werden.

7. Diskussion und Ausblick

Die Antwort auf das definierte Forschungsdefizit, wie eine objektive Priorisierungsstrategie im Wesentlichen zur Effizienzsteigerung und Erhöhung der Resilienz der Systeme beitragen kann, ist das Kohärenzmodell. Das dazugehörige Anwendungstool IRET dient in diesem Zusammenhang als Werkzeug zur Ausführung des Kohärenzmodells, das eine elementare Lücke im Priorisierungs- und Evaluierungssystem der Schwachstellenbewertung und -behebung der KRITIS schließt.

Mit der Deklaration des BSI IT-Grundschutz-Kompendiums, der DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27019, dem NIST CSF sowie weiteren spezifischen informativen Standards wie der ISO/IEC 27035 oder NIST SP 800-53 steht den Fachanwendern eine Vielzahl an intersektoralen und ICS-sektorspezifischen Standards und Normen zur Verfügung, welche eine Reihe von organisatorischen, technischen und soziologischen Sicherheitsanforderungen zur nachhaltigen und effektiven Sicherstellung und Aufrechterhaltung der Informationssicherheit darstellt. Das Grundgerüst der einzelnen Deklarationen fußt hierbei auf die Triangulation der Informationssicherheit und stellt den holistischen Ansatz dar (vgl. Koza/Öztürk, 2022a, S. 99 | Koza, 2022a, S. 2859 | Koza/Öztürk, 2021, S. 49-69 | Koza, 2022b, 49 f.).

Aus dieser Betrachtung kann nun geschlussfolgert werden, dass die Effektivität durch die Deklaration der Normen, Standards, Empfehlungen etc. bereits sichergestellt wird. Die wesentliche Fragestellung gilt also nicht der Erstellung von weiteren Sicherheitsparadigmen, denn insbesondere aus der detektierenden und präventiven Sichtweise existiert bereits eine Vielzahl an zielführenden Sicherheitsanforderungen im Bereich des IRM, VM und der Handhabung von Informationssicherheitsvorfällen. Vielmehr gilt es neue intelligente Modelle und Werkzeuge zu entwickeln, die den Fachanwendern die Fähigkeit verleihen, die bereits vorhandenen Sicherheitsanforderungen und Deklarationen effizient, zielführend, schlank und ökonomisch nachhaltig umsetzen zu können. Wie wichtig derartige praxisbasierte Lösungsansätze sind, zeigt die kürzliche Anerkennung des BSI gegenüber den vom Verfasser entwickelten IDS-NWA-Modells, welches mit dem „Best Student Award“ honoriert wurde (vgl. Koza/Öztürk, 2022b, S. 203-217).

Dabei geht es grundsätzlich darum, den Fokus der Forschung auf eine Bedürfnisbefriedigung der Fachanwender zu legen, um mit Hilfe von gestaltungsorientierter angewandter Forschung industrielle Problemstellungen zu identifizieren und diese mit geeigneten Lösungsansätzen zu lösen. Das entwickelte Kohärenzmodell fußt ebenfalls auf diesen Gedankengang und dient als Entscheidungsunterstützungsmodell zur Optimierung der Priorisierungsstrategie von anfallenden Schwachstellen und CVE in OT-Netzwerken. Die wesentlichen und erprobten Vorteile des Kohärenzmodells und IRET basieren auf der Ermöglichung einer automatisierten, objektiven, reproduzierbaren und schlanken Priorisierungsstrategie, welche unabhängig des Entscheidungsträgers bestimmt werden kann.

Die in Kapitel 4 formulierte Forschungsleitlinie FL1 diente dazu, die für die Überprüfung der Forschungshypothesen notwendigen objektiven Entscheidungskriterien abzuleiten. Bild 31 fasst diese Kriterien zusammen.

Bezogen auf die Forschungshypothese konnte validiert werden, dass die Integration objektiver Entscheidungskriterien zur Bewertung und Priorisierung von CVE in dem Kohärenzmodell für wirksame und effiziente Handlungsoptionen nach der Kritikalität von Zeit, der Ausfallfolgen und des erforderlichen Aufwands sorgt. Dies konnte durch die Evaluierung der Experten aus der Industrie bestätigt werden.

Dabei können die Cybersicherheitsingenieure eine wichtige Optimierung ihrer Entscheidungsqualität erreichen, indem sie durch Anwendung des Kohärenzmodells die Anzahl der inkorrekten Priorisierungen bezugnehmend zu FP und FN reduzieren und gleichzeitig zur Erhöhung der Effizienz- und Abdeckungsrate ihrer Entscheidungen beitragen.

Neben der Steigerung der Entscheidungsqualität sind die Cybersicherheitsingenieure auch in der Lage, ein einheitliches Verständnis für die CVE-Evaluierungsprozesse zu entwickeln und reproduzierbare und personenunabhängige Entscheidungen abzuleiten, die von allen Mitarbeitenden getragen werden können.

In der Summe kann durch den Einsatz des Kohärenzmodells in IRET eine Reduzierung des Zeitaufwandes zwischen 71 % bis 87,5 % gegenüber von manuellen Expertenentscheidungen erreicht werden. Durch die implementierten Dokumentationselemente wie die Management Summaries, Monitoringberichte I und II sowie ISMS-Reports, können die Cybersicherheitsingenieuren ihre Evaluierungsprozesse visualisieren und die Berichte bspw. als Nachweiserbringung für interne und externe Auditprozesse an andere Organisationseinheiten weiterleiten. In der Gesamtheit der empirischen Betrachtung konnte daher zusammengetragen werden, dass das Kohärenzmodell in der Lage ist, die gestellten Anforderungen und Ziele zu erfüllen und somit zu einer zeitlichen und fachlichen Effizienzsteigerung der CVE-Priorisierungsstrategien beizutragen.

Die wesentlichen kritischen Merkmale, die IRET und das Kohärenzmodell betreffen, thematisieren zunächst die Art der statischen VBA-Implementierung und die fehlende Dynamik. Zur Beseitigung dieser Problematiken soll im Verlauf der weiteren Forschungseinheiten wie folgt vorgegangen werden: Durch die Übertragung der Logik des Kohärenzmodells und von IRET auf eine dynamische Entwicklungsumgebung entsteht die Möglichkeit, IRET als eine Webanwendung zu realisieren und über bestimmte technische Schnittstellen direkt an CERT-Einheiten oder auch an die NIST NVD anzubinden. Über diese Anbindung kann IRET alle weltweit generierten CVE automatisiert in das Bewertungsverfahren einfügen und die Bewertung automatisiert durchführen. Durch die Integration und Implementierung von Alarmfunktionen können dann, ähnlich wie bei einem IDS, nur die CVE gemeldet werden, die gemäß der individuell festgelegten Orient-Stammdaten und Klassifizierungsstufen eine TP, somit eine Gefahr für OT-Netzwerke darstellen. Allerdings stellt ein derartiges Forschungsvorhaben ein komplexes Feld dar, das nur durch die Integration mehrerer internationaler Partner und ausreichenden Forschungsgeldern realisiert werden kann.

Ein weiterer kritischer Punkt betrifft die Transformationsfähigkeit des Kohärenzmodells auf nichtverwandte industrielle Bereiche, wie bspw. innerhalb des Rechenzentrumbetriebs oder der Medizintechnik.

Auch dieser Aspekt sollte in den zukünftigen Forschungsaktivitäten aufgegriffen werden, um die Vielfältigkeit der Einsatzfelder von IRET anhand empirischer Daten zu verifizieren oder ggf. mit Hilfe der Metamodellierung des Kohärenzmodells Anpassungen vorzunehmen, die den reellen Einsatz von IRET in nichtverwandten Gebieten zulässt.

Literaturverzeichnis

Ahmad, A., Maynard, S. B., Desouza, K. C., Kosias, J., Whitty, M. T., Baskerville, R. L. (2021): How can organizations develop situation awareness for incident response: A case study of management practice. In: Computers & Society, Vol. 101.

Allodi, L., Massacci, F. (2014): Comparing vulnerability severity and exploits using case-control studies. In: ACM Transactions on Information and System Security, Vol. 17, Nr. 1, S. 1-20.

Almukaynizi, M., Nunes, E., Dharaiya, K., Sennguttuvan, M., Shakarian, J., Shakarian, P. (2017): Proactive identification of exploits in the wild through vulnerability mentions online. In: IEEE 2017: Proceedings of CyCon U.S., United States, S. 82-88.

Alperin, K. B., Wollaberm A. B., Gomez, S. R. (2020): Improving Interpretability for Cyber Vulnerability Assessment Using Focus and Context Visualizations. In: Proceedings of the Symposium on Visualization for Cyber Security (ViZSec), Salt Lake City, UT, USA, S. 30-39.

Anderson, R., Moore, T. (2006): The Economics of Information Security. In: Science, American Association for the Advancement of Science, Vol. 314, No. 5799, S. 610-613.

Babar, A., Islam, C., Nepal, S. (2019): An Ontology-Driven Approach to Automating the Process of Integrating Security Software Systems. In: Proceedings of the IEEE/ACM International Conference on Software and System Processes (ICSSP), Montreal QC, Canada, S. 54-63.

Baggio, J. A., Brown, K., Hellebrandt, D. (2015): Boundary object or bridging concept? A citation network

Baur, A., Fritsch, P., Hoch, W., Merkl, G., Rautenberg, J., Weiß, M., Wricke, B. (2019): Wassergewinnung. In: Mutschmann/Stimmelmayr Taschenbuch der Wasserversorgung. Springer Vieweg, Wiesbaden, 2019.

BBK (o. J.): Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: KRITIS-Gefahren, unter: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/KRITIS-Gefahrenlagen/kritis-gefahrenlagen_node.html (Zugriff am: 27.02.2023).

Bildstein, A., Seidelmann, J. (2014): Industrie 4.0-Readiness: Migration zur Industrie 4.0-Fertigung. In: Industrie 4.0 in Produktion, Automatisierung und Logistik, Bauernhansl, T.; Hompel, M. und Vogel-Heuser, B. (Hrsg.), Wiesbaden, Springer Vieweg, S. 581-597.

BMI (2009): Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS – Strategie), Bonifatius GmbH, Paderborn, Stand: 17. Juni 2009.

BNetzA (2018): Bundesnetzagentur: IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz, Stand: Dezember 2018.

BNetzA (2015): Bundesnetzagentur: IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, Stand: August 2015.

Bolívar, H., Parada, H. D. J., Roa, O. I, Velandia, J. (2019): Multi-criteria Decision Making Model for Vulnerabilities Assessment in Cloud Computing regarding Common Vulnerability Scoring System. In: IEEE 2019: Proceedings of CONIITI, Bogota, Colombia S. 1-6.

Boyd, J. zitiert nach Hammond, G. T. (2018): A Discourse on winning and losing. John R. Boyd, Air University Press, März 2018, Maxwell, S. 1-400.

Boyd, J. zitiert nach Richards, C., Spinney, C. (2012, original 1996): The Essence of Winning and Losing, September 2012, Bluffton, South Carolina, S. 1-6.

Boyd, J. (1976): Destruction and Creation, S. 1-8.

Bozorgi, M., Saul, L. K., Savage, S., Voelker, G. M. (2010): Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits. In: Proceedings of the 16th ACM Conference on Knowledge Discovery and Data Mining (KDD-2010), S. 105-113.

BSI (2021c): Net.1: Netze. NET1.1: Netzarchitektur- und design, Stand Februar 2021, S. 1-10.

BSI (2021b): Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Medienhaus Plump GmbH, Rheinbreitbach, Stand: Februar 2021.

BSI (2021a): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2020, Appel & Klinger Druck und Medien GmbH, Schneckenlohe, Stand: September 2021.

BSI (2020b): Bundesamt für Sicherheit in der Informationstechnik: Cyber-Angriff auf Uniklinik Düsseldorf: BSI warnt vor akuter Ausnutzung bekannter Schwachstelle, unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html (Zugriff am 18.10.2020).

BSI (2020a): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2020, Appel & Klinger Druck und Medien GmbH, Schneckenlohe, Stand: September 2020.

BSI (2019b): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2019, Appel & Klinger Druck und Medien GmbH, Schneckenlohe, Stand: Oktober 2019.

BSI (2019a): Bundesamt für Sicherheit in der Informationstechnik: Empfehlung: IT in der Produktion. Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen 2019.

BSI (2018): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2018, Appel & Klinger Druck und Medien GmbH, Schneckenlohe, Stand: September 2018.

BSI (2017b): Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2. IT-Grundschutz-Methodik, Version 1.0, Stand: März 2017.

BSI (2017a): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2017, Druck- und Verlagshaus Zarbock Frankfurt am Main, Stand: August 2017.

BSI (2016): Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2016, Druck- und Verlagshaus Zarbock Frankfurt am Main, Stand: Oktober 2016.

BSI (2015b): Bundesamt für Sicherheit in der Informationstechnik: KRITIS-Sektorstudie. Energie, Bonn, Revisionsstand 05. Februar 2015.

BSI (2015a): Bundesamt für Sicherheit in der Informationstechnik: KRITIS-Sektorstudie. Ernährung und Wasser, Bonn, Revisionsstand 16. März 2015.

BSI (2013): Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium, Bonn, Version 1.23.

BSI (o. J.): Bundesamt für Sicherheit in der Informationstechnik: Industrielle Steuerungs- und Automatisierungssysteme (ICS), unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/industrielle-steuerungs-automatisierungssysteme_node.html (Zugriff am: 04.04.2021).

Bürkner, H. J. (2010): Vulnerabilität und Resilienz: Forschungsstand und sozialwissenschaftliche Untersuchungsperspektiven, Working Paper, Nr. 43, Leibniz-Institut für Regionalentwicklung und Strukturplanung (IRS), Erkner.

Cullen, A., Armitage, L. (2018): A Human Vulnerability Assessment Methodology. In: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, S. 1-2.

CVE (o. J. c): History, unter: https://cve.mitre.org/cve/identifiers/syntaxchange.html (Zugriff am: 03.05.2022).

CVE (o. J. b): CVE and NVD Relationship, unter: https://cve.mitre.org/about/cve_and_nvd_relationship.html (Zugriff am: 03.06.2022).

CVE (o. J. a): History, unter: https://www.cve.org/About/History (Zugriff am: 05.04.2022).

dCERT (o. J.): Häufig gestellte Fragen, unter: https://www.dcert.de/faq.html (Zugriff am 04.06.2022).

Dena (2020): Deutsche Energie-Agentur GmbH: dena-Studie. Systemsicherheit 2050. Systemdienstleistungen und Aspekte der Stabilität im zukünftigen Stromnetz, Stand: April, 2020.

Dey, D. Lahiri, A., Zhang, G. (2015): Optimal Policies for Security Patch Management. In: INFORMS Journal on Computing, Vol. 27, Nr. 3, S. 462-477.

DHS (2009): Department of Homeland Security: Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, Stand: Oktober 2009.

Dierich, A., Bösche, U., Wurbs, S. (2020): Analyse von Interdependenzen zwischen KRITIS. Empfehlungen für Praxisakteure aus Versorgungsunternehmen und kommunalen Behörden, 2. aktualisierte Auflage, Berlin, Stand: Februar 2020.

DiMasse, D., Collier, Z. A., Chandy, J., Cohen, B. S., D'Anna, G., Dunlap, H., Hallman, J., Mandelbaum, J., Ritchie, J., Vessels, L. (2020): A Holistic Approach to Cyber Physical Systems Security and Resilience. In: IEEE, Proceedings of SSS, Crystal City, VA, USA, S. 1-8.

DIN EN ISO/IEC 27019:2020-08, Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08).

DIN EN ISO/IEC 27000:2020-06, Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018).

DIN EN ISO/IEC 27002:2017-06, Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015).

DIN EN ISO/IEC 27001:2017:06 Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015).

DIN EN 62264-1:2014-07, Integration von Unternehmensführungs- und Leitsystemen – Teil 1: Modelle und Terminologie (IEC 62264-1:2013).

Doynikova, E., Kotenko I. (2018): CVSS-based Prohabilistic Risk Assessment for Cyber Situational Awareness and Countermeasure Selection. In Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), St. Petersburg, Russia, S. 346-353.

Döring, N., Bortz, J. (2016): Forschungsmethoden und Evaluation in den Sozial und Humanwissenschaften. Unter Mitarbeit von Sandra Pöschl. 5. vollständig überarbeitete, aktualisierte und erweiterte Auflage, Springer-Verlag Berlin Heidelberg.

DVGW (2006): Deutscher Verein des Gas- und Wasserfaches: Technische Regel. Arbeitsblatt W 645-3. Überwachungs-, Mess-, Steuer- und Regeleinrichtungen in Wasserversorgungsanlagen – Teil 3: Prozessleittechnik, Bonn, Stand: Februar 2006.

Ernst, A. (2020): Polizei ermittelt nach Hacker-Angriff in einem Todesfall. In: Süddeutsche, 17.09.2020, unter: https://www.sueddeutsche.de/panorama/duesseldorf-uniklinikum-erpressung-hacker-angriff-1.5035140 (Zugriff am: 04.01.2023).

Faria, M. R., Figueiredo, G., Cordeiro, K. d. G., Cavalcanti, M. C., Campos, M. (2019): Applying Multi-Level Theory to an Information Security Incident Domain Ontology. In: ONTOBRAS.

FIRST (2005): Common Vulnerability Scoring System v1 Archive, unter: https://www.first.org/cvss/v1/ (Zugriff am 07.06.2022).

FIRST (o. J. c): Common Vulnerability Scoring System v3.0: Specification Document (v1.9), unter: https://www.first.org/cvss/v3.0/specification-document (Zugriff am: 04.07.2022).

FIRST (o. J. b): The EPSS Model, unter: https://www.first.org/epss/model (Zugriff am 05.05.2021).

FIRST (o. J. a): Common Vulnerability Scoring System version 3.1. Specification Document, Revision 1.

Gianini, G., Cremonini, M. Rainini, A., Cota, G. L., Fossi, L. G. (2015): A game theoretic approach to vulnerability patching. In: International Conference on Information and Communication Technology Research (ICTRC), Abu Dhabi, United Arab Emirates, S. 88-91.

Haacke, F., Endreß, C. (2022): Risiko Blackout. Krisenvorsorge für Wirtschaft, Behörden und Kommunen, Richard Boorberg Verlag GmbH & Co KG, Stuttgart.

Hellström, T. (2007): Critical infrastructure and systemic vulnerability: Towards a planning framework. In: Safety Science 45 (3), S. 415-430.

Ibers, T., Hey, A. (2005): Risikomanagement, Merkur Rinteln Verlag.

IEC 62443-3-3:2013-08, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

IEC 62443-2-1:2010-11, Industrial communication network – Network and system security – Part 2-1: Establishing an industrial automation and control security program.

IEC/TS 62443-1-1:2009-09, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models.

ISO/IEC 27035-3:2020-09, Information technology – Security techniques – Information security incident management, Part 3: Guidelines for ICT incident response operations.

ISO/IEC 27035-2:2016-01, Information technology – Security techniques – Information security incident management, Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035:2011-09).

ISO/IEC 27035-1:2016-11, Information technology – Security techniques – Information security incident management, Part 1: Principles of incident management (ISO/IEC 27035:2011-09).

ISO/IEC 27005:2011-06-01, Information technology – Security techniques – Information security risk management.

Jacobs, J., Romanosky, S., Adjerid, I., Baker, W. (2020): Improving vulnerability remediation through better exploit prediction. In: The Journal of Cybersecurity, S. 1-12.

Jalali, M. S., Siegel, M., Madnick, S. (2019): Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. In: The Journal of Strategic Information Systems, Cambridge, United States, Vol. 28, Heft 1, S. 66-82.

Kebande, V. R., Kigwana, I., Venter, H. S., Karie, N. M., Wario, R. D. (2018): CVSS Metric-Based Analysis, Classification and Assessment of Computer Network Threats and Vulnerabilities. In: icABCD, South Africa, S. 1-10.

Kiesel, R., Heutmann, T., Dering, J., Kies, A., Vollmer, T., Schmitt, R. H. (2020): Cybersecurity in der vernetzten Produktion Whitepaper Fraunhofer IPT, S. 1-22.

Koza, E., Öztürk, A. (2022b): Entwicklung eines adaptiven Anforderungsanalyse-Tools zur bedarfsgerechten Ermittlung von CERT und IDS-Dienstleistungen für die Akteure in der Energiewirtschaft. In: Cyber-Sicherheit ist Chefinnen- und Chefsache! Tagungsband zum 18. Deutschen IT-Sicherheitskongress, S. 203-217.

Koza, E., Öztürk, A. (2022a): A Coherence Model to Outline Obstacles and Success Factors for Information Security from the CISO's Point of View. In: Proceedings of the 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022), Human Factors in Cybersecurity, Vol. 53, New York, USA, S. 92-101.

Koza, E., Beese, Y., Denker, K., Gabel, F., Korte, B., Opper, J., Schließer, L., Schminder, Seitz, J., Zill, M. (2022): SiFo innovativ. Positionspaper des Graduierten-Netzwerks Zivile Sicherheit für das Rahmenprogramm Forschung für die zivile Sicherheit 2024-2030, Stand: 19.09.2022.

Koza, E. (2023): An Assessment Model for Prioritizing CVEs in Critical Infrastructures in the Context of Time and Fault Criticality. In: Hämmerli, B., Helmbrecht, U., Hommel, W., Kunczik, L., Pickl, S. (eds) Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723. Springer, Cham. In Proceedings of the 17th International Conference on Critical Infrastructures Security (CRITIS 2022), Springer Lecture Notes in Computer Science, Deutschland, München.

Koza, E. (2022c): Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security. In: Medicon Engineering Themes, Vol. 2, Issue 3, S. 26-39.

Koza, E. (2022b): Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security? In: Proceedings of the 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022), Human Factors in Cybersecurity, Vol. 53, New York, USA, S. 49-57.

Koza, E. (2022a): OODA Loop as a Decision Support Model to Continuous and Dynamic Vulnerability Management and Incident Response Management of Critical Infrastructures. In: Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022). Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson. Research Publishing, Singapore, S. 2859-2866.

Koza, E., Treibert, R., Öztürk, A. (2021): Gutachten für den Deutschen Bundestag. Präventive Informationssicherheit in der Wasserwirtschaft: Stand und Herausforderung (unveröffentlicht).

Koza, E., Öztürk, A. (2021): A Literature Review to Analyze the State of the Art of Virtual Power Plants in Context of Information Security. In: Wohlgemuth, V., Naumann, S., Behrens, G., Arndt, HK. (eds) Advances and New Trends in Environmental Informatics. ENVIROINFO 2021. Progress in IS. Springer, S. 49-69.

Koza, E. (2021): Eine empirische Kontentanalyse zur Ermittlung von praxisorientieren Optimierungsfeldern zur Resilienz-Erhöhung der IT-Systeme im Sinne der ganzheitlichen Betrachtung der Informationssicherheit. Hemmnisse und Erfolgsfaktoren eines nachhaltigen und effizienten Informationssicherheitsmanagementsystems. In: Informatik 2021 Computer Science & Sustainability, Gesellschaft für Informatik, Lecture Notes in Informatics, S. 819-831.

Krempl, S. (2022): Viasat: Wiper-Malware hat Ausfall des Satellitennetzwerks KA-Sat verursacht. In: Heise online, 02.04.2022, unter: https://www.heise.de/news/Viasat-Wiper-Malware-hat-Ausfall-des-Satellitennetzwerks-KA-Sat-verursacht-6661499.html (Zugriff am 23.11.2022).

Kuckartz, U. (2016): Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, Beltz Verlag, Weinheim Basel, 3. überarbeitete Auflage.

Laskowski, N. (2013): Netflix uses the OODA loop to stay ahead of the competition, unter: https://www.techtarget.com/searchcio/news/2240203084/Netflix-uses-the-OODA-loop-to-stay-ahead-of-the-competition (Zugriff am 06.07.2021).

Lewis, L. P., Petit, F. (2019): Critical Infrastructure Interdependency Analysis: Operationalising Resilience Strategies, Global Assessment Report on Disaster Risk Reduction of the United Nations Office for Disaster Risk Reduction, Contributing Paper, S. 1-33.

Lewis, R. (2016): Becoming a Cognitive Enterprise – the OODA Approach, Herausgeber: Dell Technologies, unter: https://www.dell.com/en-us/blog/becoming-a-cognitive-enterprise-the-ooda-approach/ (Zugriff am 07.08.2021).

Luiijf, E. (2014): Chapter 3. In: Akhgar, B., Staniforth, A., Bosco, F., Cyber Crime and Cyber Terrorism Investigator's Handbook, S. 24-29.

Mann, D. E., Christey, S. M. (1999): Towards a Common Enumeration of Vulnerabilities. The MITRE Corporation.

Meilinger, P. S. (2017): Time in War. In: Joint Forces Quarterly, Vol. 87, Nr. 4, S. 93-94.

Mock, R. (2003): Risiko, Sicherheit und Zuverlässigkeit. Analysemethoden in der "Information and Communication Technology"? In: Informatik Spektrum 26, S. 167-172.

Mundie, D., Ruefle, R., Dorofee, A., McCloud, J., Collins, M. (2014): An Incident Management Ontology, Software Engineering Institute.

NAS (2012): National Academy of Sciences: Disaster Resilience. A National Imperative, National Academies Press, Washington, D.C., United States of America.

Neller, M., Bolzen, S., Doll, N., Heuzeroth, T., Smirnova, J. (2017): Es ist kein Zufall, dass auch die Deutsche Bahn getroffen wurde. In: WELT, 13.05.2027, unter: https://www.welt.de/wirtschaft/article164541556/Es-ist-kein-Zufall-dass-auch-die-Deutsche-Bahn-getroffen-wurde.html (Zugriff am: 12.12.2022).

NERC CIP (2019): North American Electric Reliability Corporation Critical Infrastructure Protection, Cyber Security – Incident Reporting and Response Planning. Implementation Guidance for CIP-008-06.

NERC CIP (2006): North American Electric Reliability Corporation Critical Infrastructure Protection, Cyber Security – Recovery Plans for Critical Cyber Assets.

NIAC (2009): National Infrastructure Advisory Council: Critical Infrastructure Resilience Final Report and Recommendations, Stand: 8. September 2009.

NIAC (2005): National Infrastructure Advisory Council: Meeting Agenda Tuesday, April 12, 2005, unter: https://www.cisa.gov/sites/default/files/publications/niac-qbm-minutes-04-12-05-508.pdf, (Zugriff am: 04.05.2022).

NIST (2020): National Institute of Standards and Technology: Security and Privacy Controls for Information Systems and Organizations, (U.S. Department of Commerce, Washington, D.C.), NIST Series (NIST Special Publication 800-53) Rev. 4, September 2020.

NIST (2018): National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Stand: 16. April 2018.

NIST (2015): National Institute of Standards and Technology: Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), (U.S. Department of Commerce, Washington, D.C.), NIST Series (NIST Special Publication 800-82) Rev. 2, May 2015.

NIST (2012): National Institute of Standards and Technology: Computer Security Handling Guide. Recommendations of the National Institute of Standards and Technology, (U.S. Department of Commerce, Washington, D.C.), NIST Series (NIST Special Publication 800-61) Rev. 2, August 2012.

NIST (o. J. b): National Vulnerability Database, unter: https://nvd.nist.gov (Zugriff am 02.07.2022).

NIST (o. J. a): NIST Cybersecurity Framework, unter: https://www.nist.gov/cyberframework (Zugriff am 02.12.2022).

NSA (o. J.): National Security Agency: Defense of Depth, unter: https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf (Zugriff am: 05.07.2022).

Osinga, F. (2007): Science, Strategy and War, The Strategic Theory of John Boyd, London, Routledge.

Pfitzmann, A. (2000): Datensicherheit und Kryptographie, Skript aus dem WS2000/2021, TU Dresden.

Pham, V., Dang, T. (2018): CVExplorer: Multi-dimensional Visualization for Common Vulnerabilities and Exposures. In IEEE 2018, Seattle, WA, USA, S. 1296-1301.

Qiong, Q. (2017): A Brief Introduction to Perception. In: Studies in Literature and Language, Vol. 15, Nr. 4, S. 18-28.

Rannenberg, K., Pfitzmann, A., Müller, G. (1996): Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: it-Information Technology, Vol. 38, Nr. 4, S. 7-10.

Rinaldi, S. M, Peerenboom J. P., Kelly, T. K. (2001): Identifying, Understanding, and Analyzing. Critical Infrastructure Interdependencies. In: IEEE Control Systems Magazine, Bd. 21, Nr. 6, S. 11-25.

Sabottke, C., Suciu, O., Dumitras, T. (2015): Vulnerability Disclosure in The Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. In: USENIX Security Symposium, S. 1041-1056.

Shepherd, C., Akram, R. N., Petitcolas, F. A. P., Markantonakis, K. (2017): An Exploratory Analysis of the Security Risks of the Internet of Things in Finance. In: Lopez, J., Fischer-Hübner, S., Lambrinoudakis, C. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2017. Lecture Notes in Computer Science, Springer, Cham, Vol. 10442, S. 1-16.

Siepmann, D. (2016): Industrie 4.0 - Technologische Komponenten. In: Einführung und Umsetzung von Industrie 4.0, Roth, A. (Hrsg.), Berlin Heidelberg, Springer Gabler Verlag, S. 47-72.

Skopik, F., Wurzenberger, M., Settani, G., Fiedler, R. (2015): Establishing national cyber situational awareness through incident information clustering. In: Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), London, UK, S. 1-8.

Sprecher Automation GmbH (2022): Security Alerts, unter: https://www.sprecher-automation.com/it-sicherheit/security-alerts (Zugriff am: 08.10.2022).

Tianfield, H. (2016): Cyber Security Situational Awareness. In: Proceedings of the International of the IEEE International Conference on Internet oof Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber Physical and Social Computing (CPSCom) and IEEE Smart Data (Smart Data), S. 782-787.

Tredgold, T. 1818. On the transverse strength of timber. Philosophical Magazine: Journal of Theoretical, Experimental and Applied Science Volume XXXXVII. Taylor and Francis, London, UK.

Tremblay, M. P. D. Jr. (2015): Shaping and Adapting. Unlocking the power of Colonel John Boyd's OODA Loop, Marine Corps Combat, Development Command Quantico, United States, Virginia.

UKD (2020): Universitätsklinik Düsseldorf: IT-Ausfall an der Uniklinik Düsseldorf, unter: https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/it-ausfall-an-der-uniklinik-duesseldorf (Zugriff am: 23.11.2022).

UP KRITIS (2014): Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen. Grundlagen und Ziele, Druck- und Verlagshaus Zarbock Frankfurt am Main, Stand: Februar 2014.

Vanamala, M., Yuan, X., Roy, K. (2020): Modeling And Classification Of Common Vulnerabilities And Exposures Database. In: icABCD, Durban, South Africa, S. 1-5.

Wang, H., Chen, Z., Zhao, J., Di, X., Liu, D. (2018): A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow. In: IEEE Access, Vol. 6, S. 8599-8609.

Wang, J. A., Guo, M., Wang, H., Xia, M., Zhou, L. (2009): Environmental Metrics for Software Security Based on a Vulnerability Ontology. In: IEEE 2009: Proceedings of the International Conference on Secure Software Integration and Reliability Improvement, China, 2009, S. 159-168.

Wendzel, S. (2021): IT-Sicherheit für TCP/IP- und IoT-Netzwerke. Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg, 2. aktualisierte und erweiterte Auflage.

Zhu, L., Zhang Z., Xia, G., Jiang, C. (2019): Research on Vulnerability Ontology Model. In: Proceedings of the 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, S. 657-661.

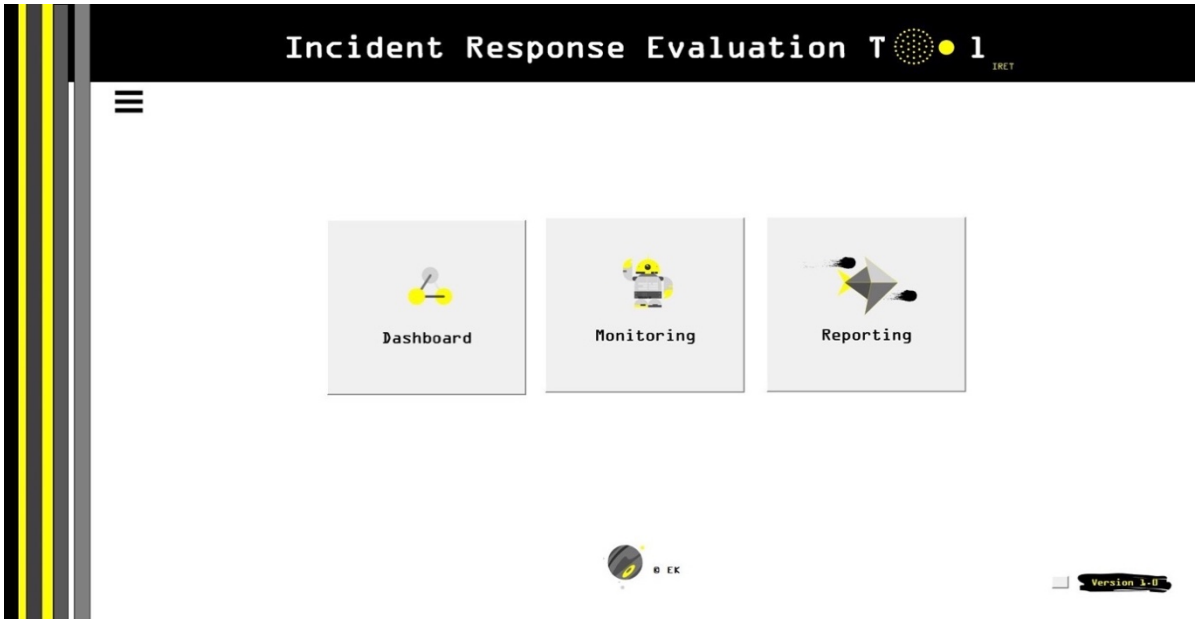
Bilderverzeichnis

Tabellenverzeichnis

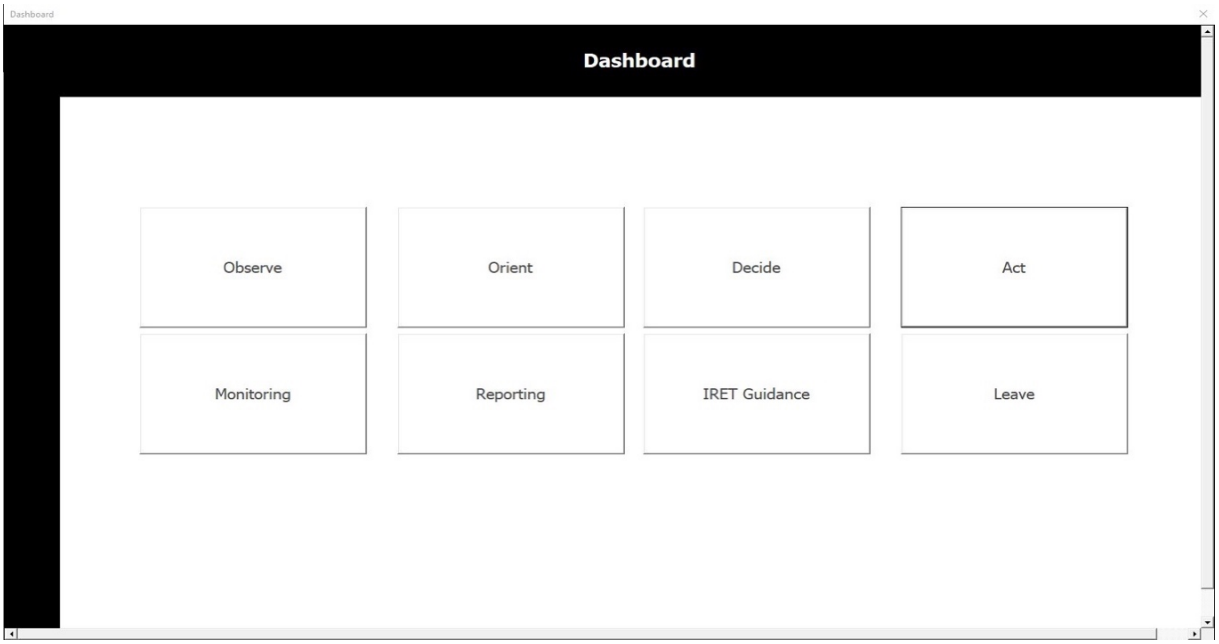
Anhang

A. In den Anhängen A.1 bis A.43 der Arbeit werden die Funktionen des IRET vorgestellt, die in Kapitel 5.5 der Dissertation ausführlich beschrieben werden und eine Visualisierung des Kohärenzmodells darstellen. IRET dient als Ausführungstool, um die Machbarkeit und Validierung des Kohärenzmodells in der Praxis zu testen. Die Bilder stellen die Systemeingaben durch die Fachanwender schrittweise dar.

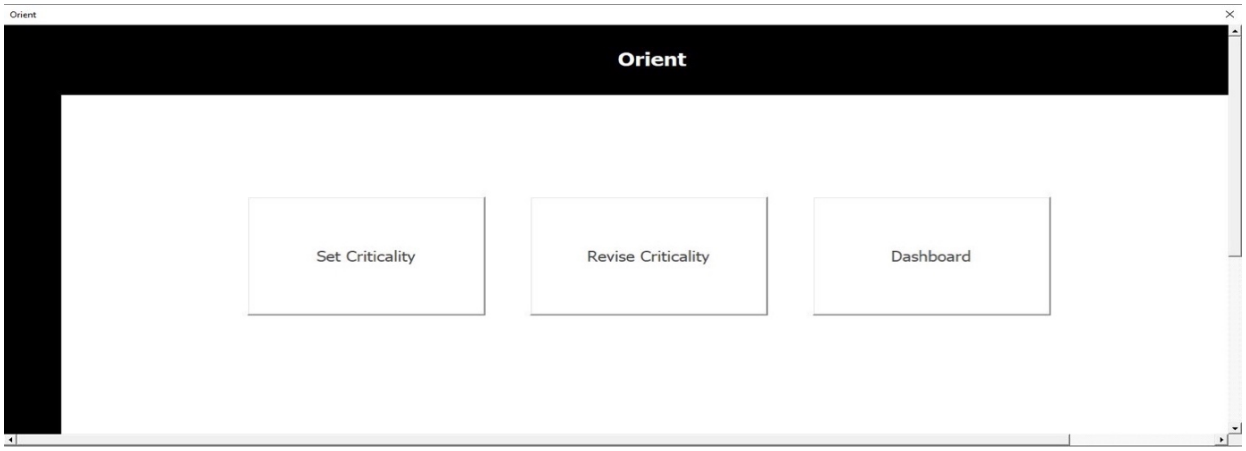
A.1: IRET-Dialogfenster: Startseite (Quelle: In Anlehnung an Koza, 2023, S. 112)



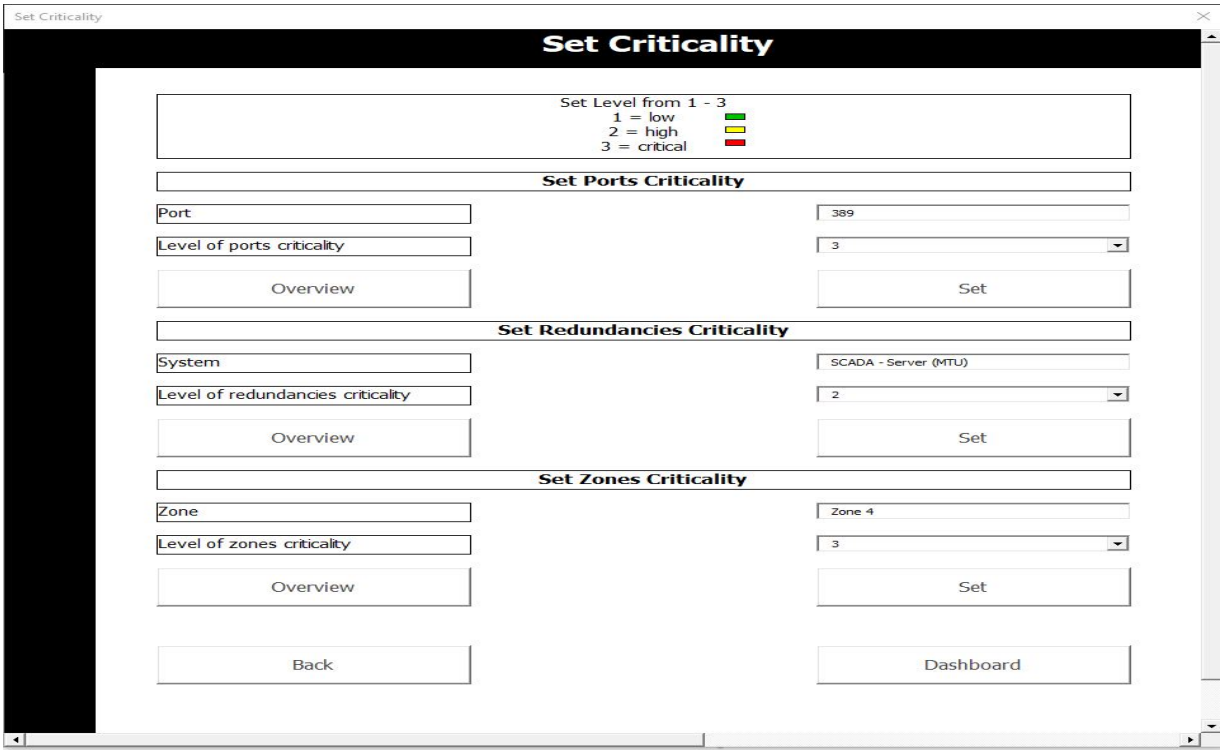
A.2: *IRET-Dialogfenster: Dashboard (Quelle: In Anlehnung an Koza, 2023, S. 112)*



A.3: *IRET-Dialogfenster: Orient (Quelle: Eigene Darstellung)*



A.4: *IRET-Dialogfenster: Set Criticality (Quelle: In Anlehnung an Koza, 2023, S. 112)*



A.5: *IRET-Datenblätter zu f_1, f_2 und f_3 (Quelle: Eigene Darstellung)*

Do not change data from here (use arrow to change)

F1 _ Ports-Criticality

ID	Port	Value	Criticality
0	No port is affected	0	low
1	Insider threats	3	critical
2	389	3	critical

Do not change data from here (use arrow to change)

F 2 _ Redundancy - Criticality

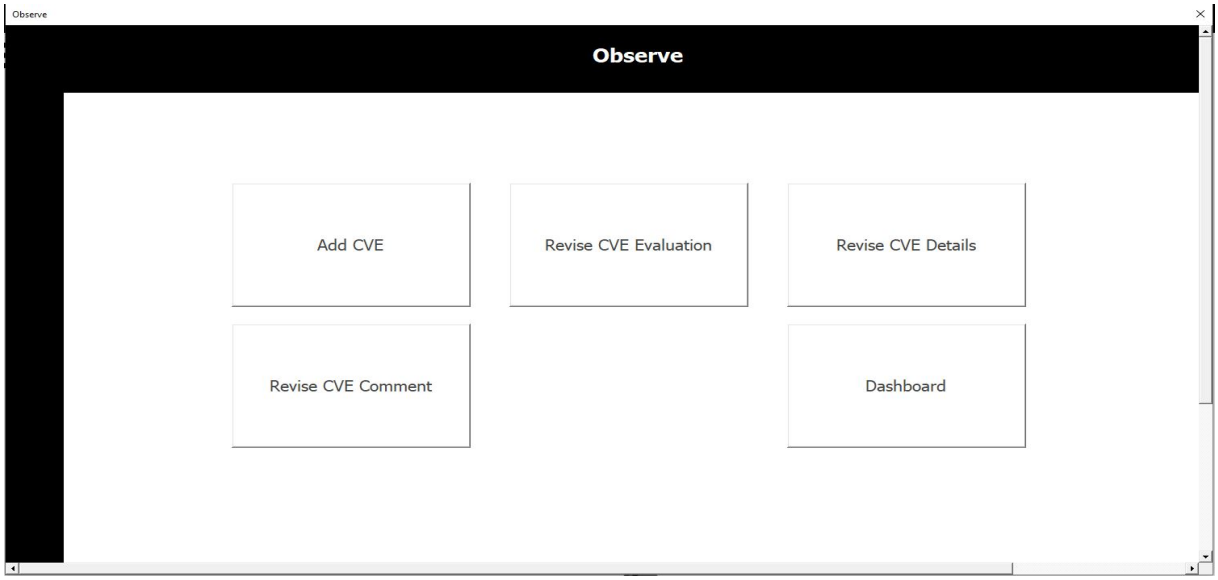
ID	System	Value	Criticality
0	No system is affected	0	none
1	Only systems on the office network are affected	0	none
2	Affected systems are outside the ICS network	0	none
3	Multiple systems are affected	3	critical
4	SCADA-Server (MTU)	2	high

Do not change data from here (use arrow to change)

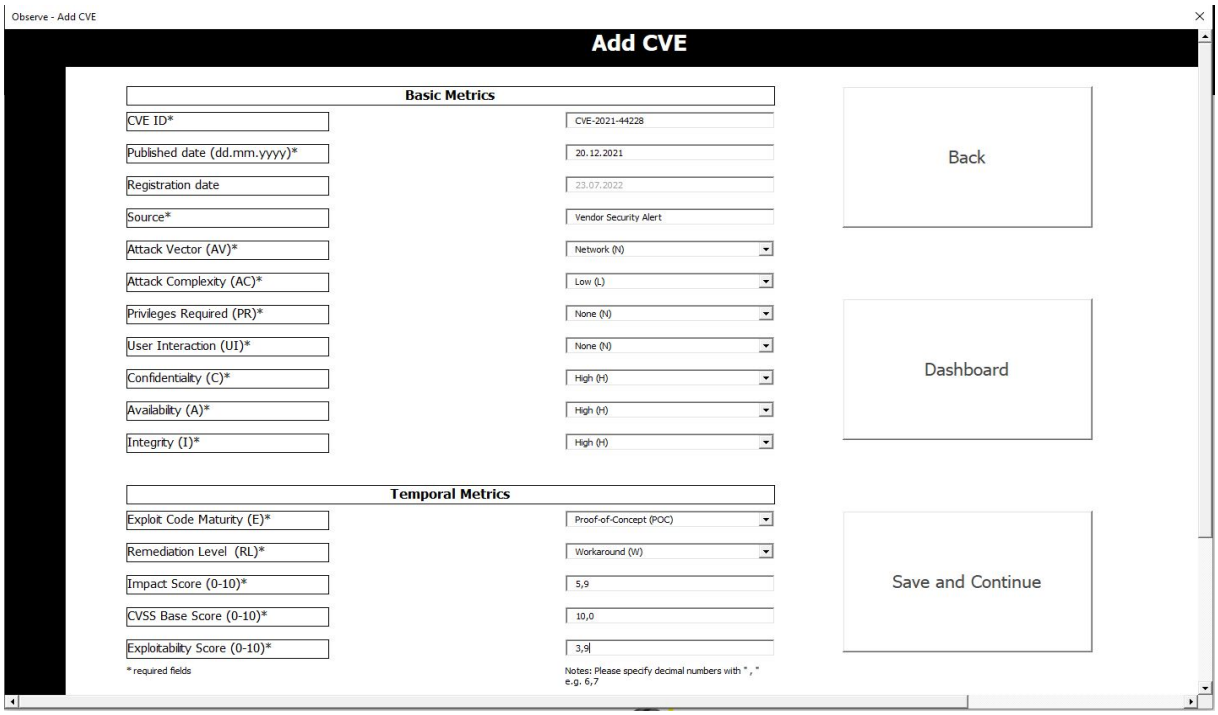
F 3_ Zone Criticality

ID	Zone	Value	Criticality
0	No OT zone is affected	0	none
1	Multiple zones are affected	3	critical
2	Zone 4	3	critical

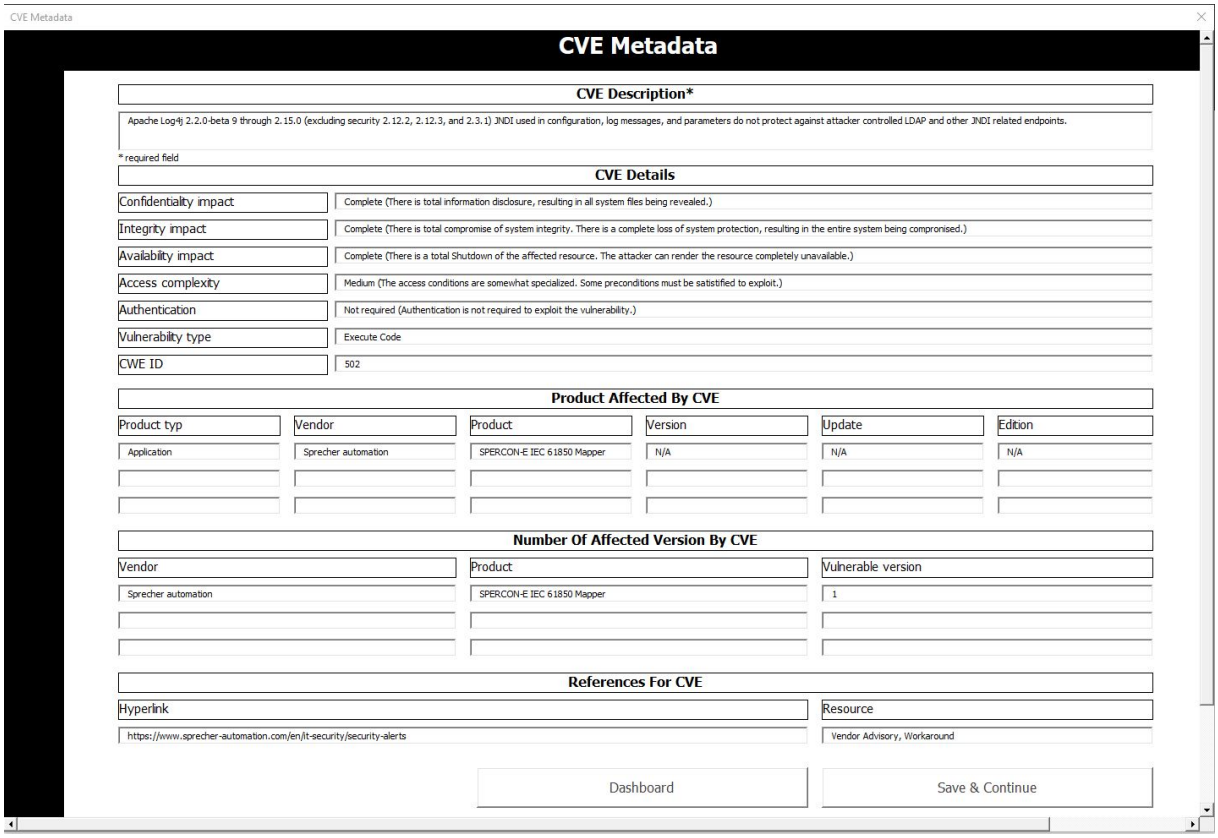
A.6: *IRET-Observe Dialogfenster (Quelle: In Anlehnung an Koza, 2023, S. 112)*



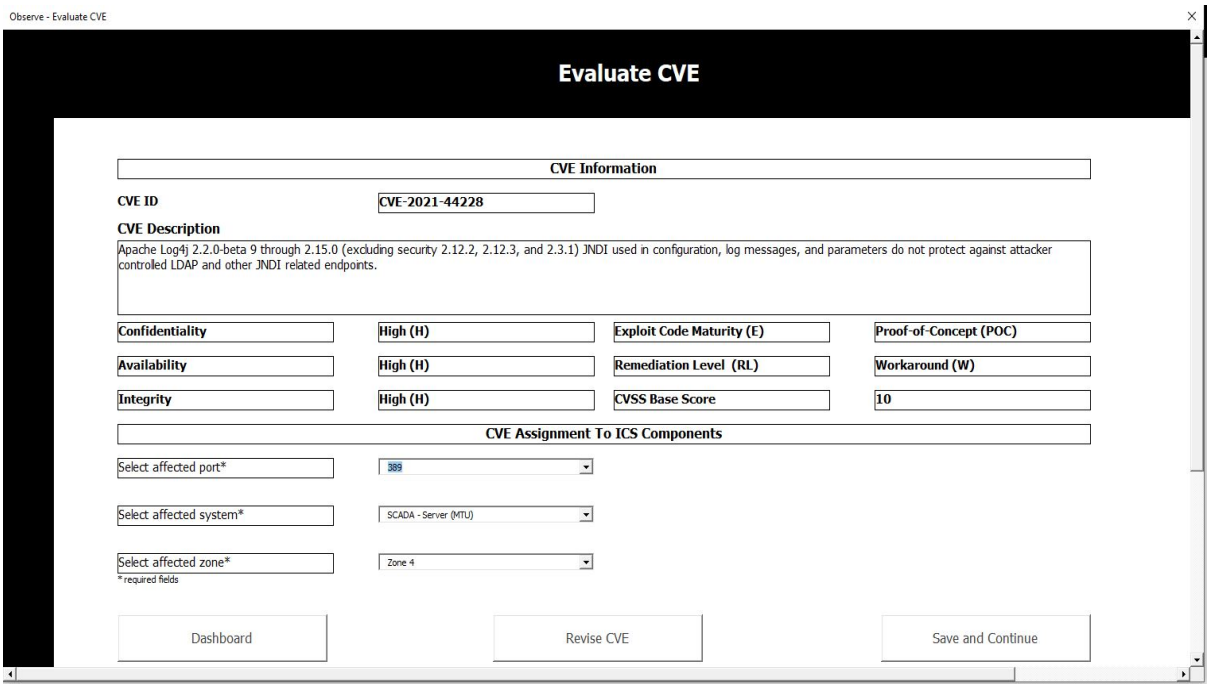
A.7: *IRET-Add CVE Dialogfenster (Quelle: In Anlehnung an Koza, 2023, S. 113)*



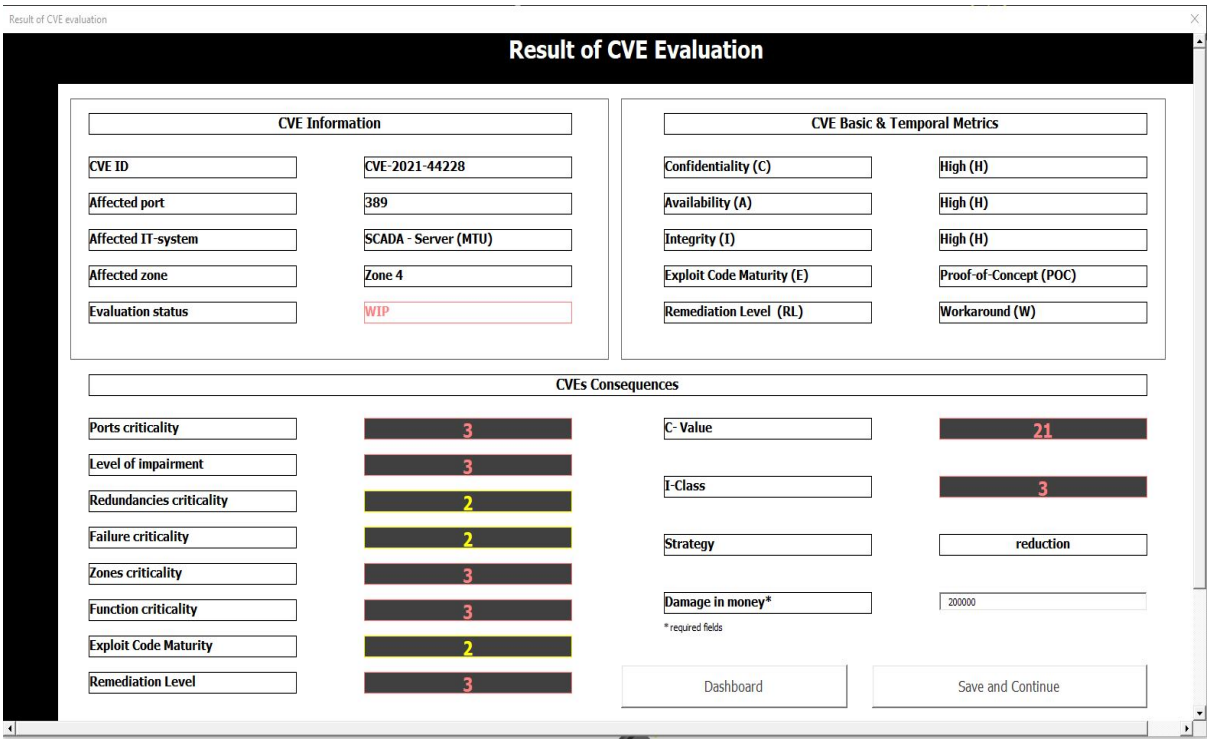
A.8: *IRET-Add CVE Metadata (Quelle: Eigene Darstellung)*



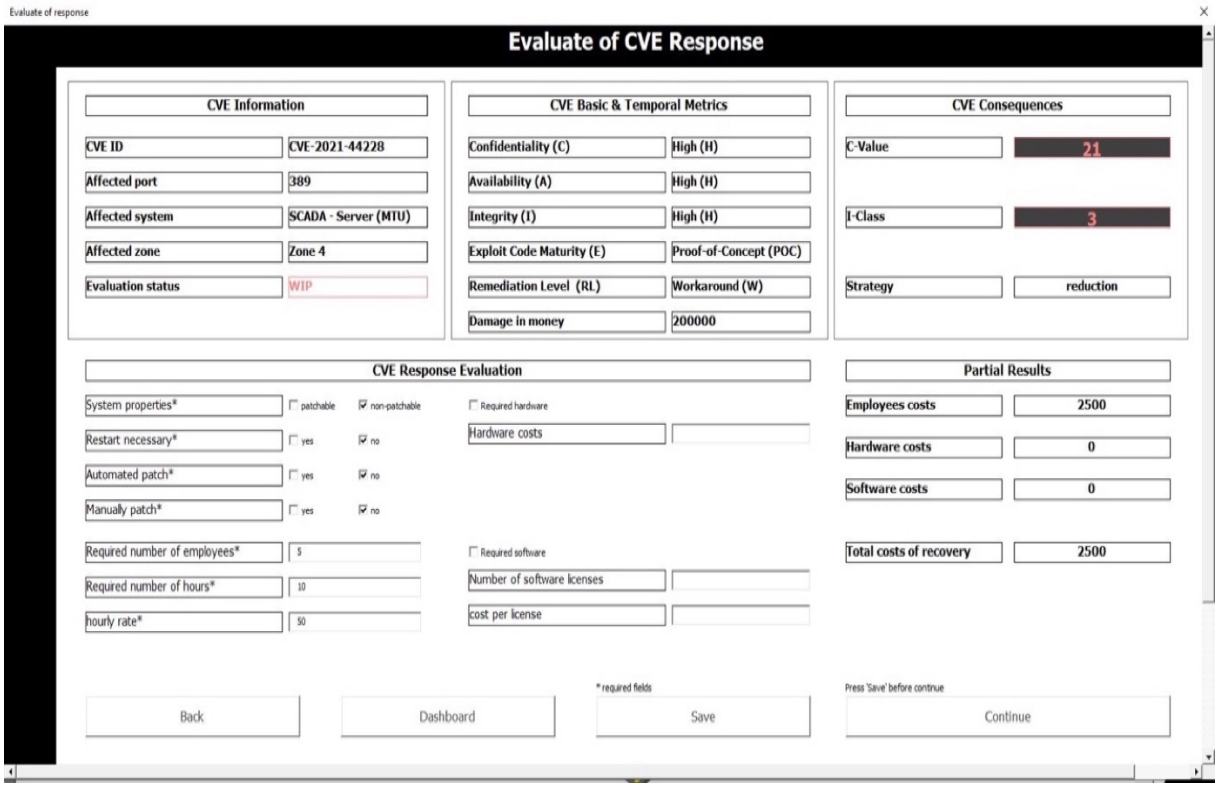
A.9: IRET-*Evalute CVE (Quelle: Eigene Darstellung)*



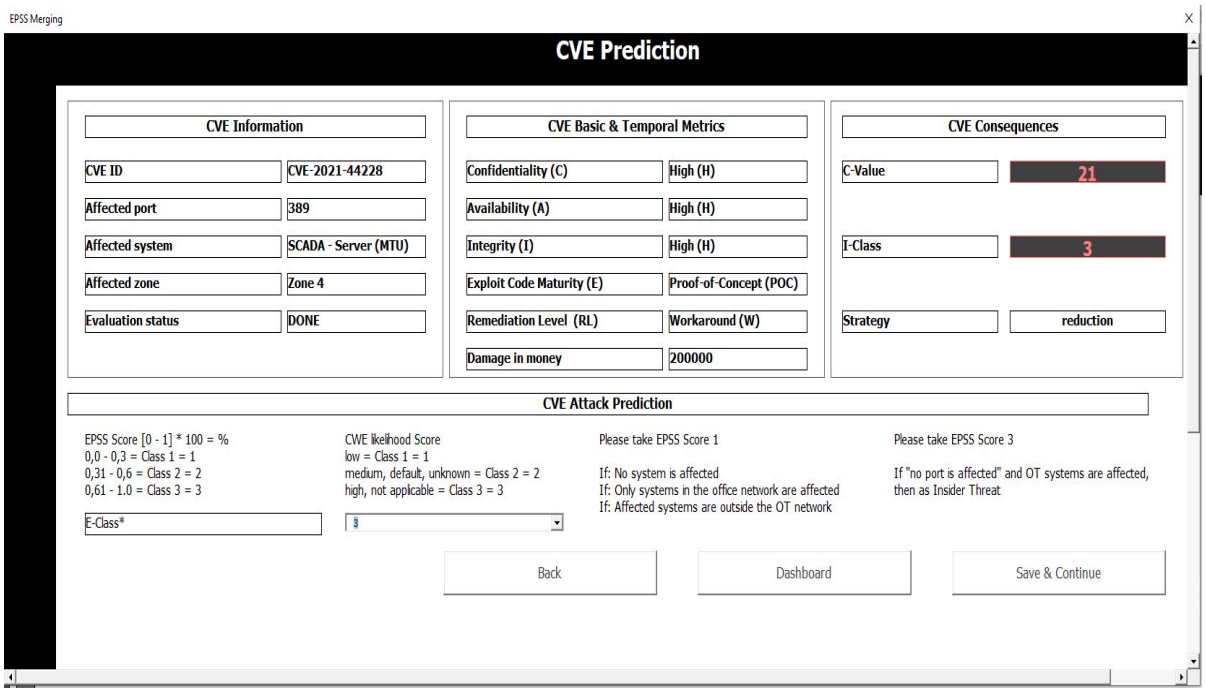
A.10: IRET-*Result of CVE Evaluation (Quelle: In Anlehnung an Koza, 2023, S. 114)*



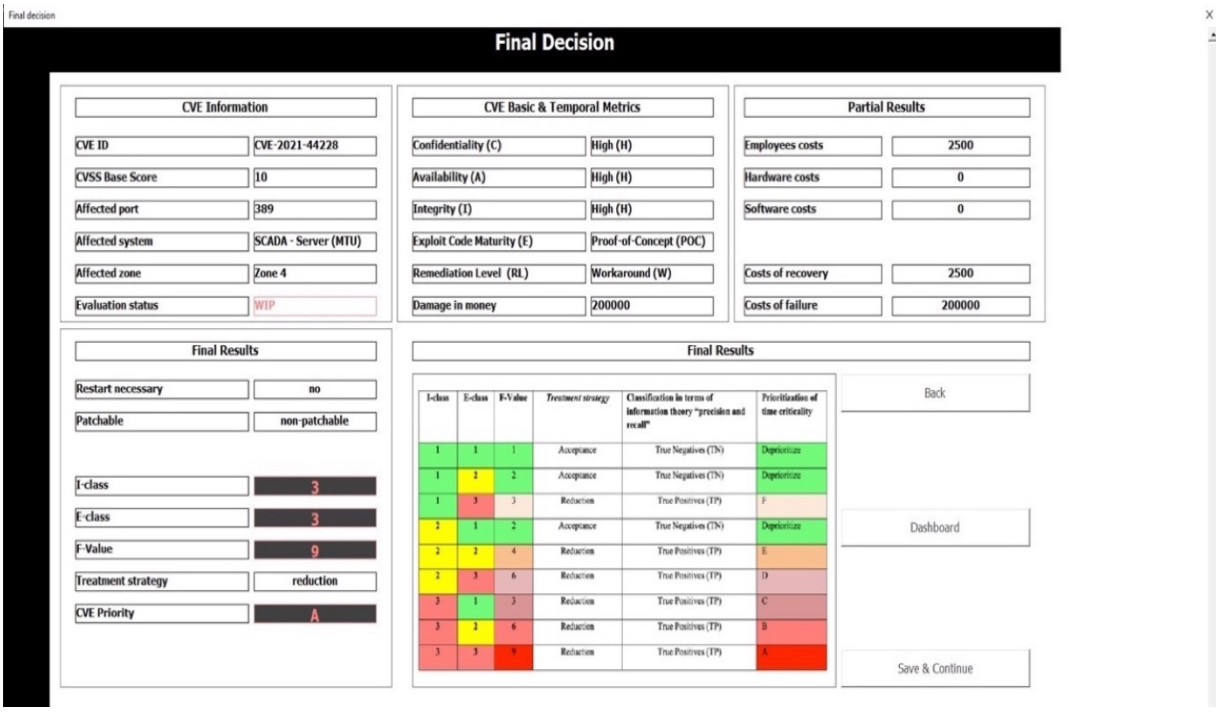
A.11: IRET-*Evaluate of CVE-Response (Quelle: In Anlehnung an Koza, 2023, S. 115)*



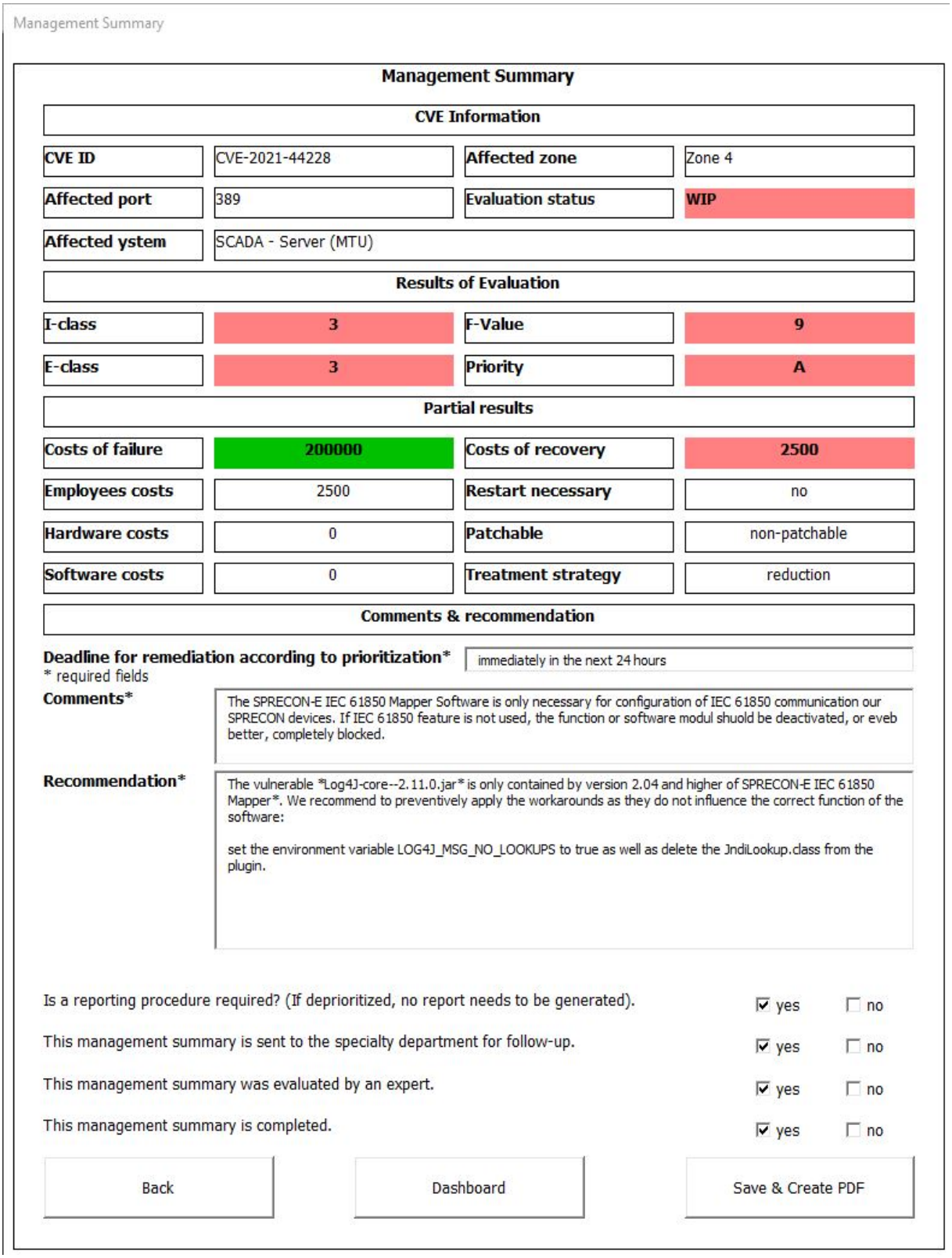
A.12: *IRET CVE Prediction (Quelle: Eigene Darstellung)*



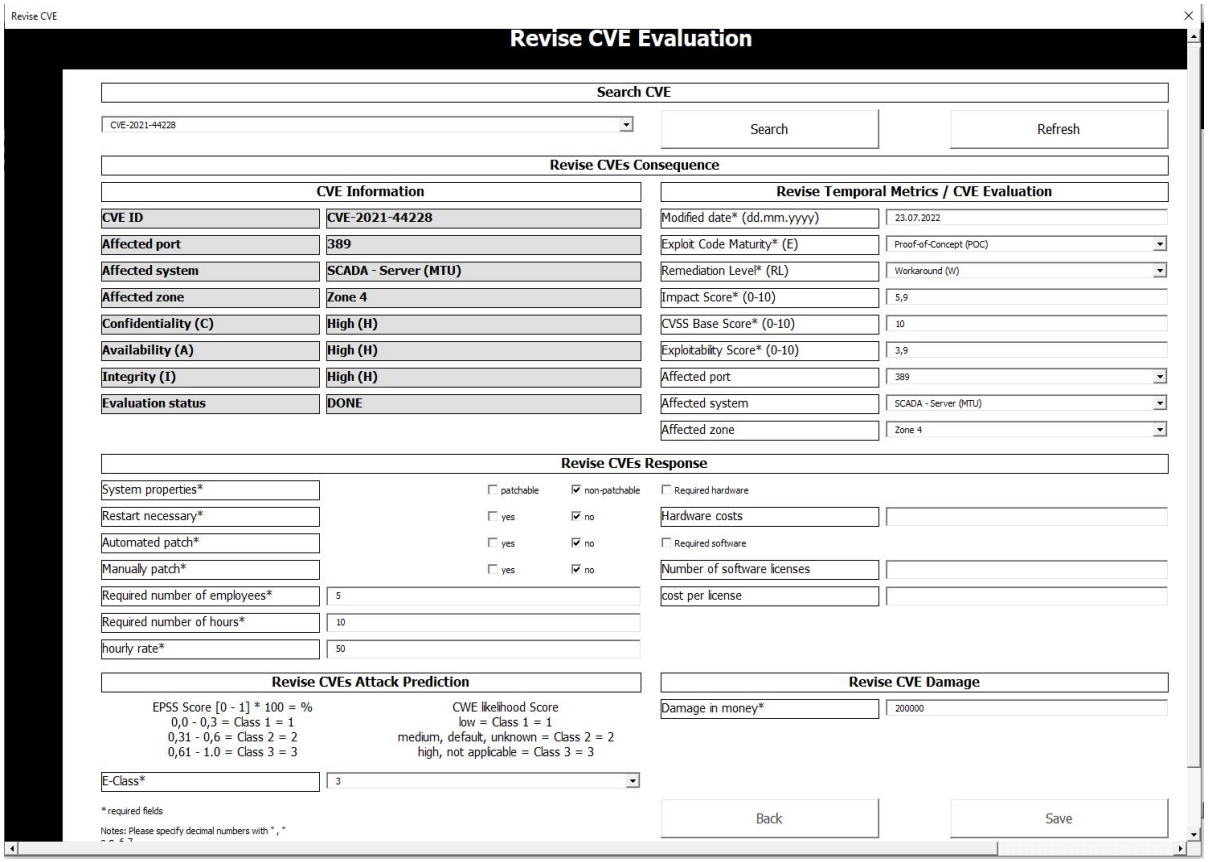
A.13: *IRET-Final Decision (Quelle: In Anlehnung an Koza, 2023, S. 115)*



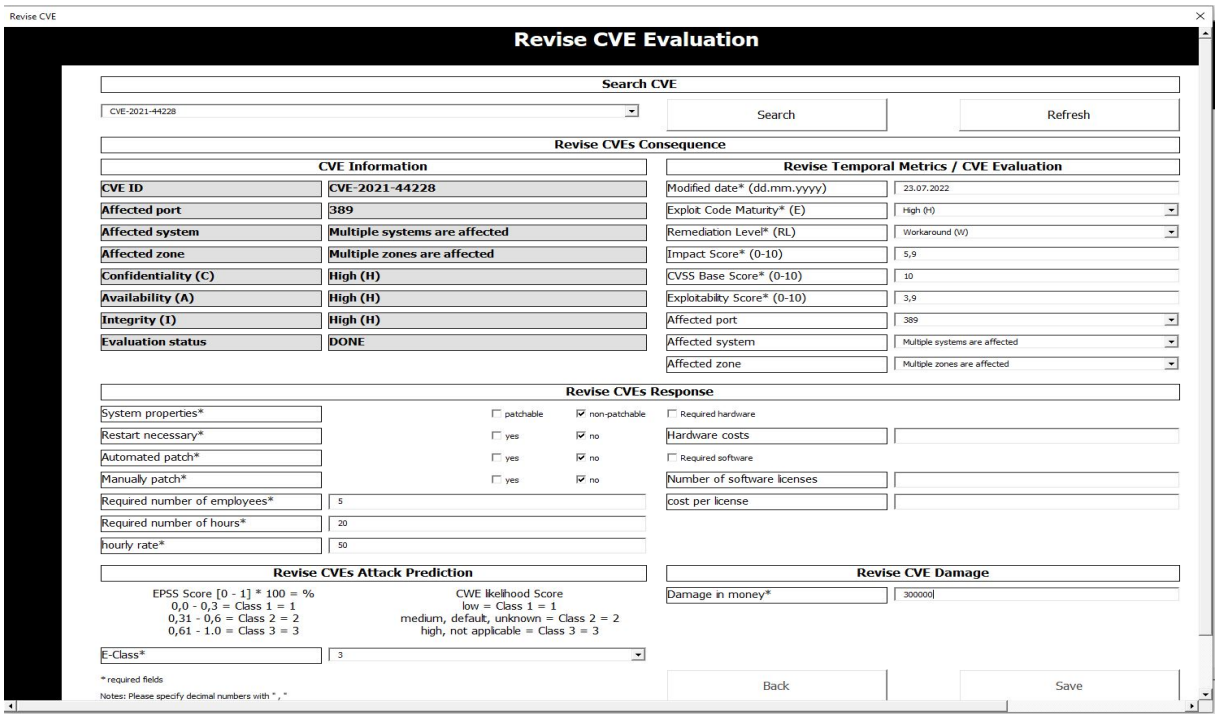
A.14: *IRET-Management Summary (Quelle: In Anlehnung an Koza, 2023, S. 115)*



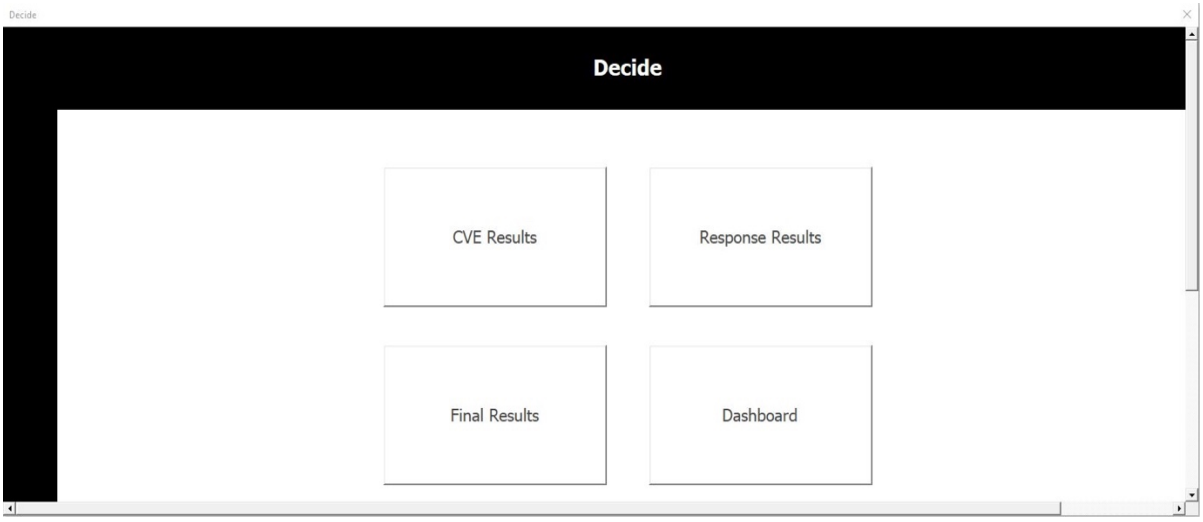
A.15: *IRET-Revise CVE-Evaluation mit der Suchfunktion (Quelle: Eigene Darstellung)*



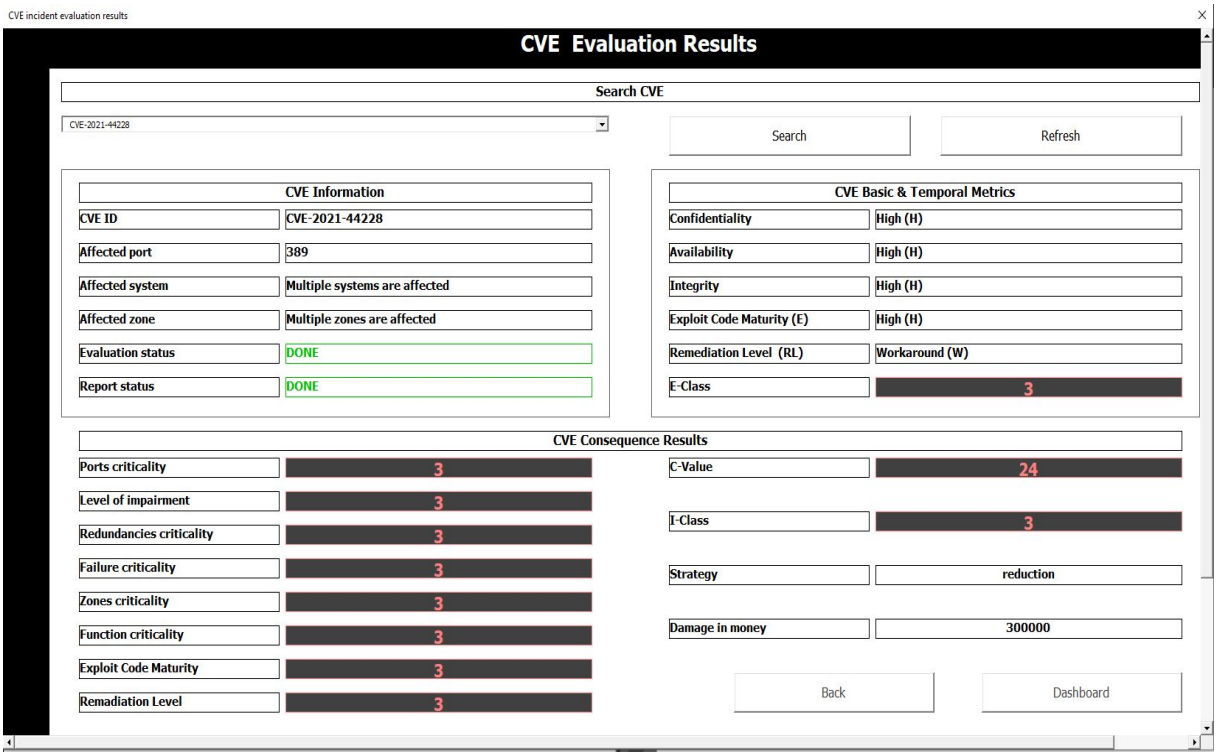
A.16: *IRET-Revise CVE-Evaluation mit der Revidierfunktion (Quelle: Eigene Darstellung)*



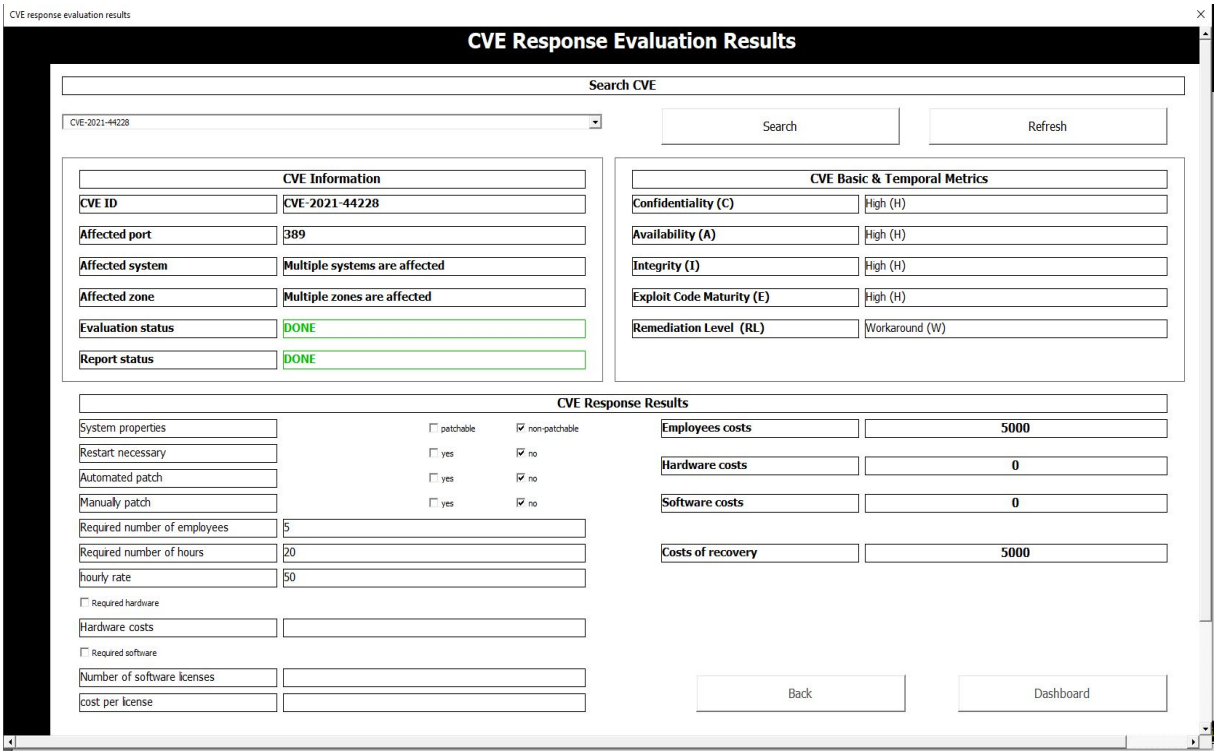
A.17: *Dialogfenster: Decide (Quelle: Eigene Darstellung)*



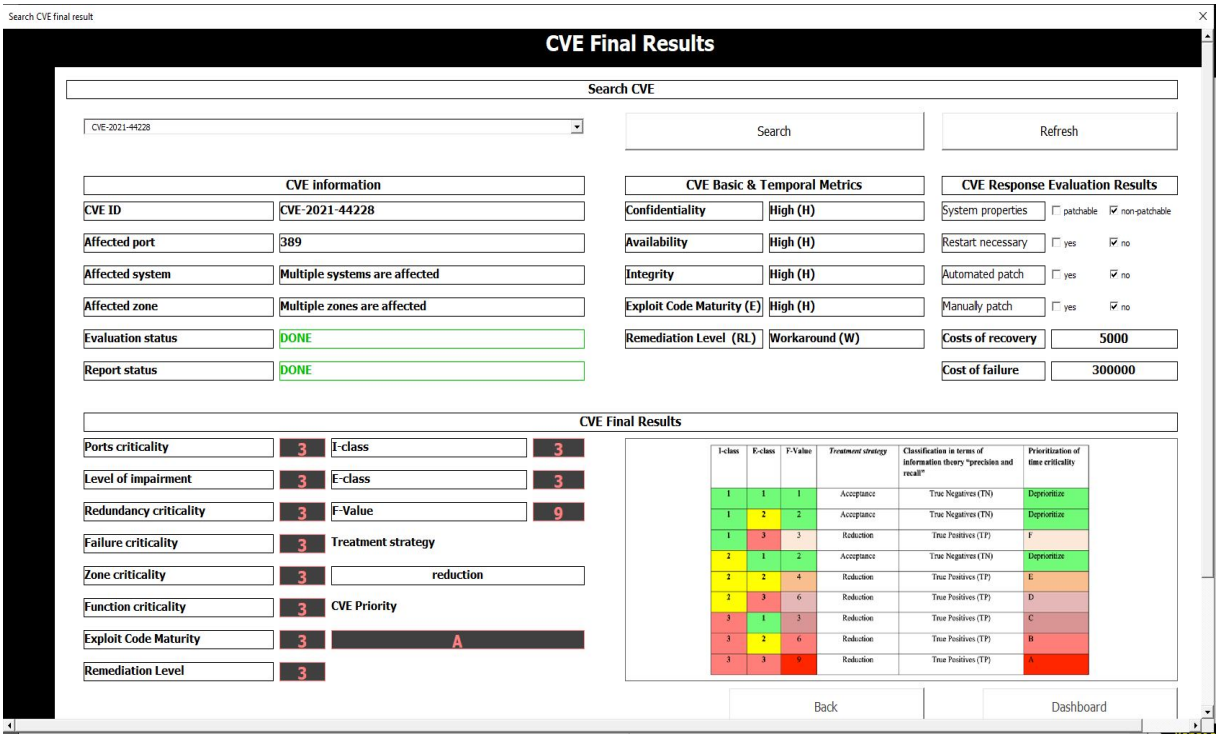
A.18: *Dialogfenster: CVE-Evaluation Results (Quelle: Eigene Darstellung)*



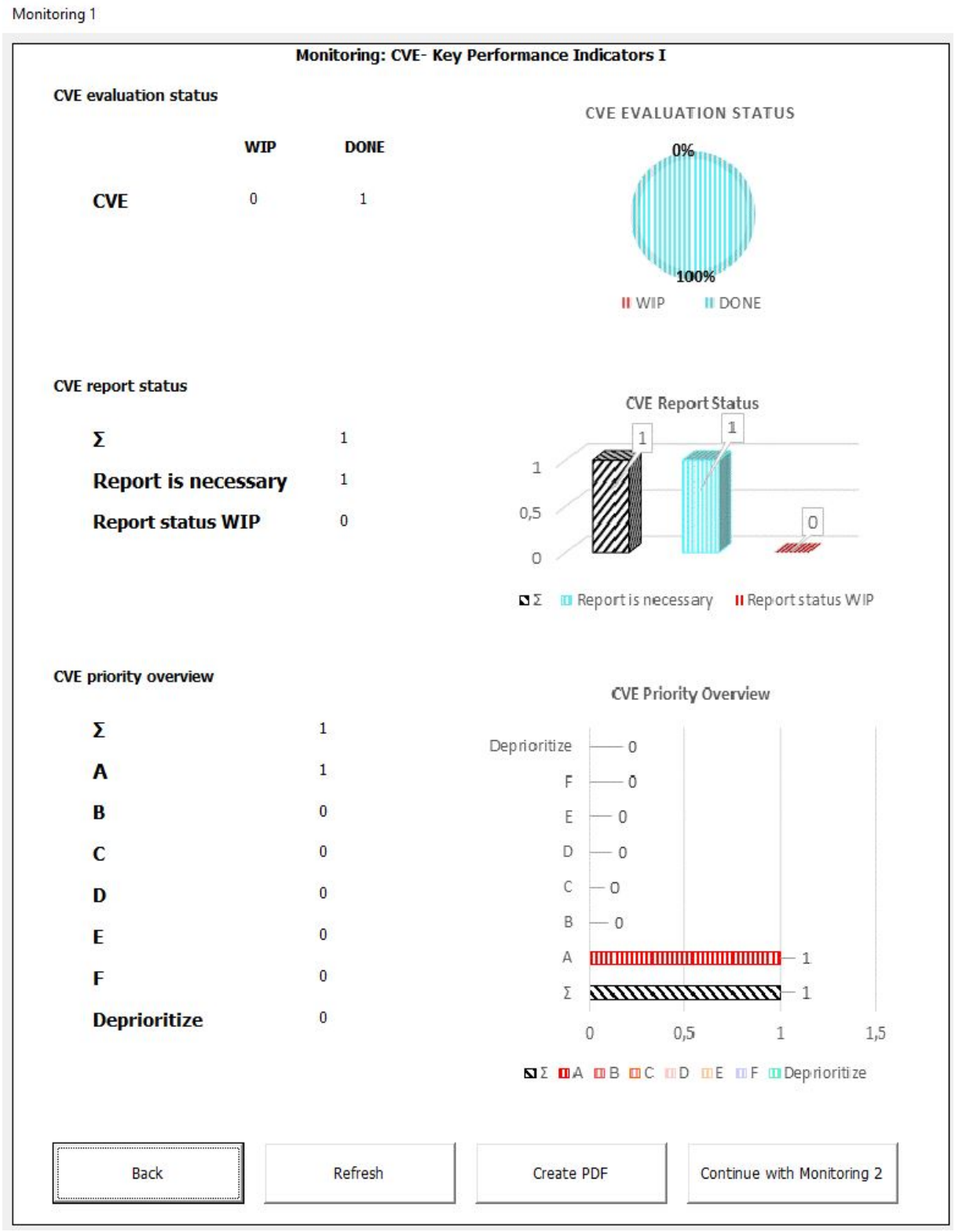
A.19: *Dialogfenster: CVE-Response Evaluation Results (Quelle: Eigene Darstellung)*



A.20: *Dialogfenster: CVE Final Results (Quelle: Eigene Darstellung)*



A.21: *IRET-Monitoringbericht (Quelle: Eigene Darstellung)*



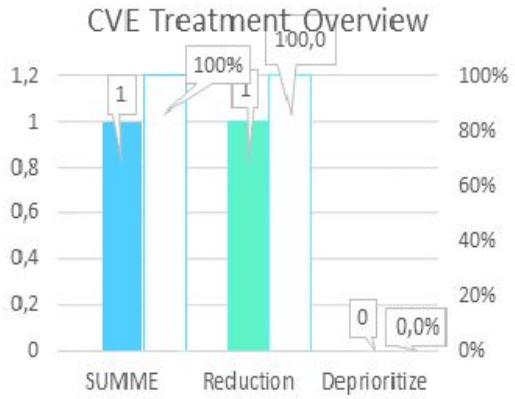
A.22: *IRET-Monitoringbericht II (Quelle: Eigene Darstellung)*

Monitoring 2

Monitoring: CVE - Key Performance Indicators II

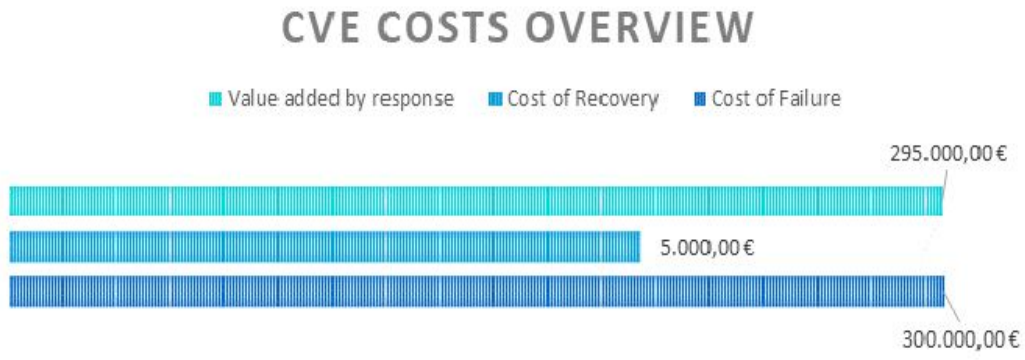
CVE treatment overview

	Numerics	%
Σ	1	100,0 %
Reduction	1	100,0 %
Acceptance	0	0,0 %



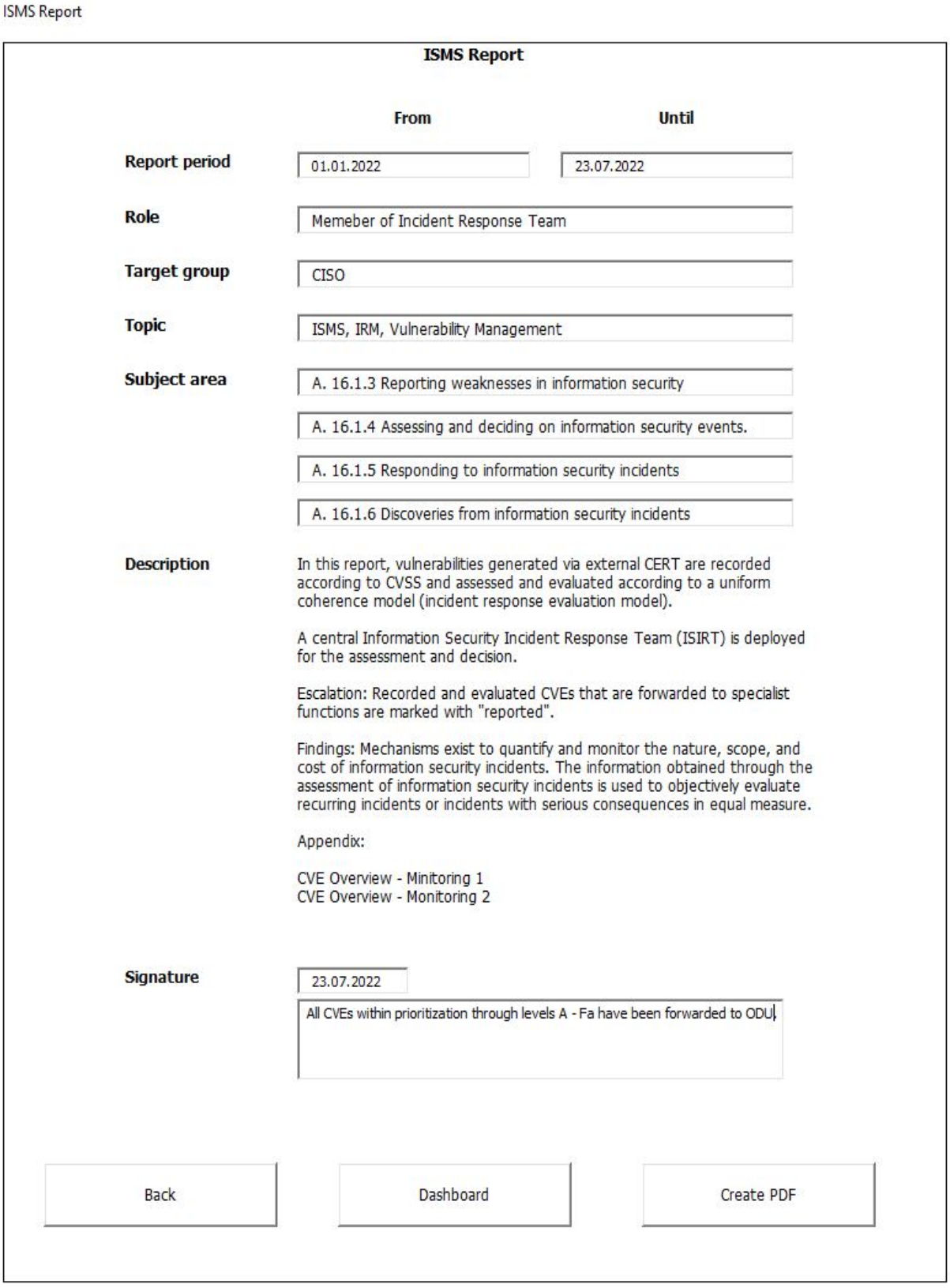
Costs overview

	€
Total estimated downtime costs (estimated costs due to incidents)	300000 €
Total estimated response costs	5000 €
Estimated monetary value added by response to eliminate vulenrability	295000 €

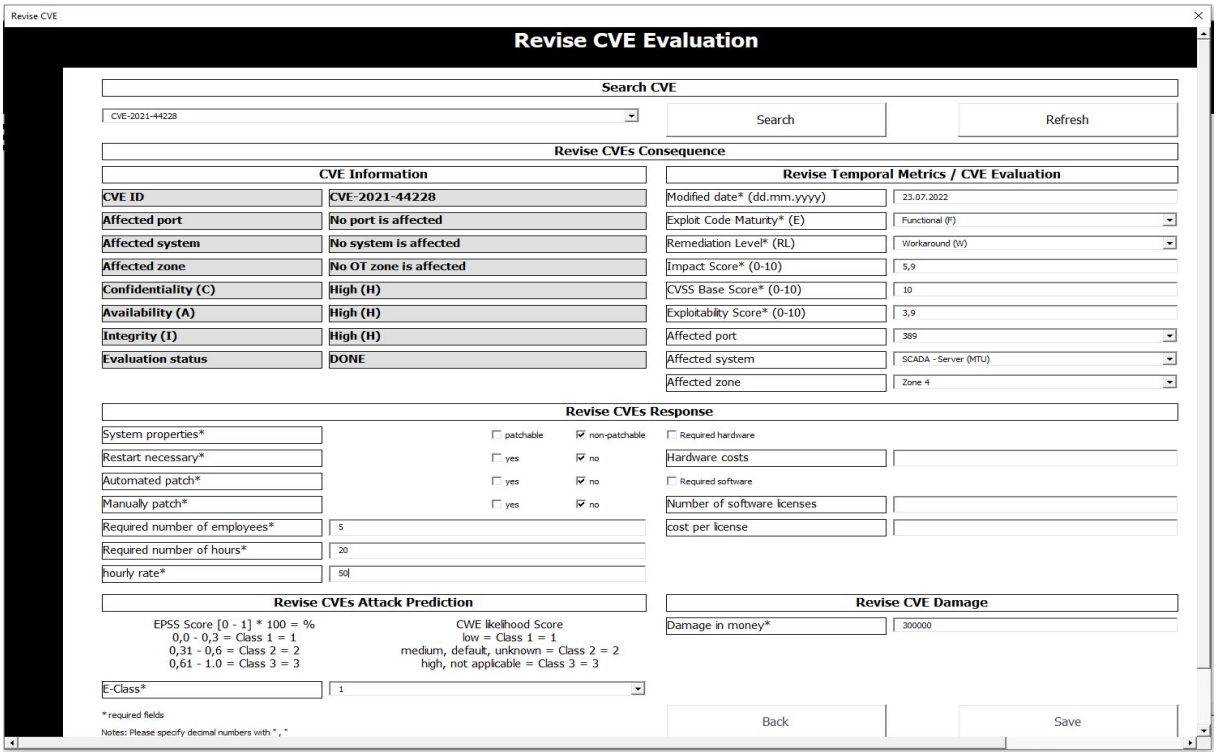


Back | Refresh | Create PDF | Continue

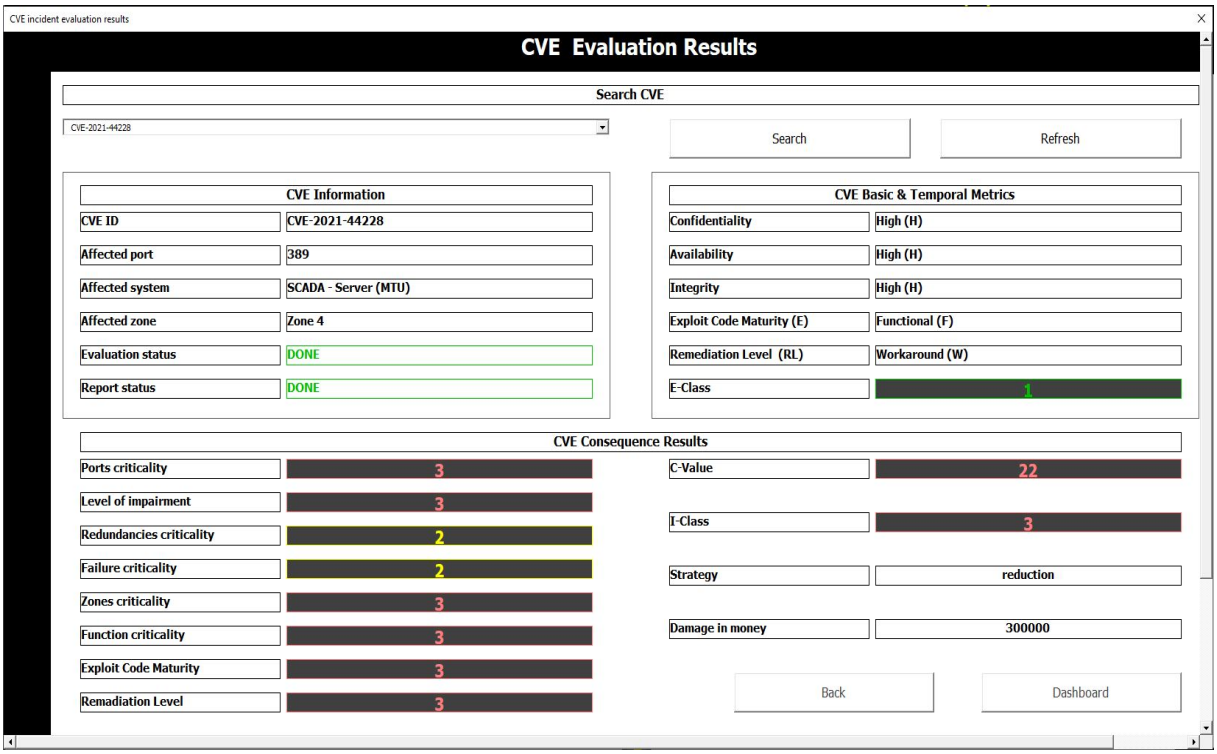
A.23: *IRET-ISMS-Report (Quelle: Eigene Darstellung)*



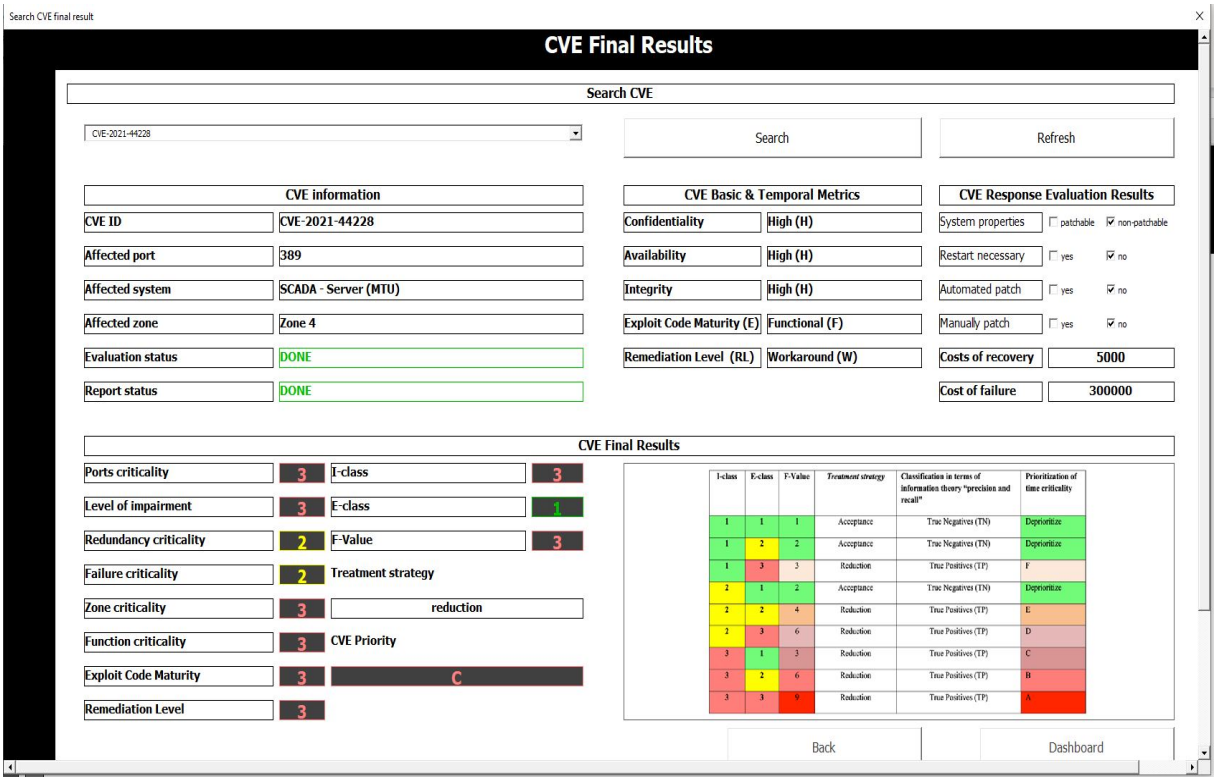
A.24: *IRET-CVE Evaluation mit veränderter Eintrittswahrscheinlichkeit (Quelle: Eigene Darstellung)*



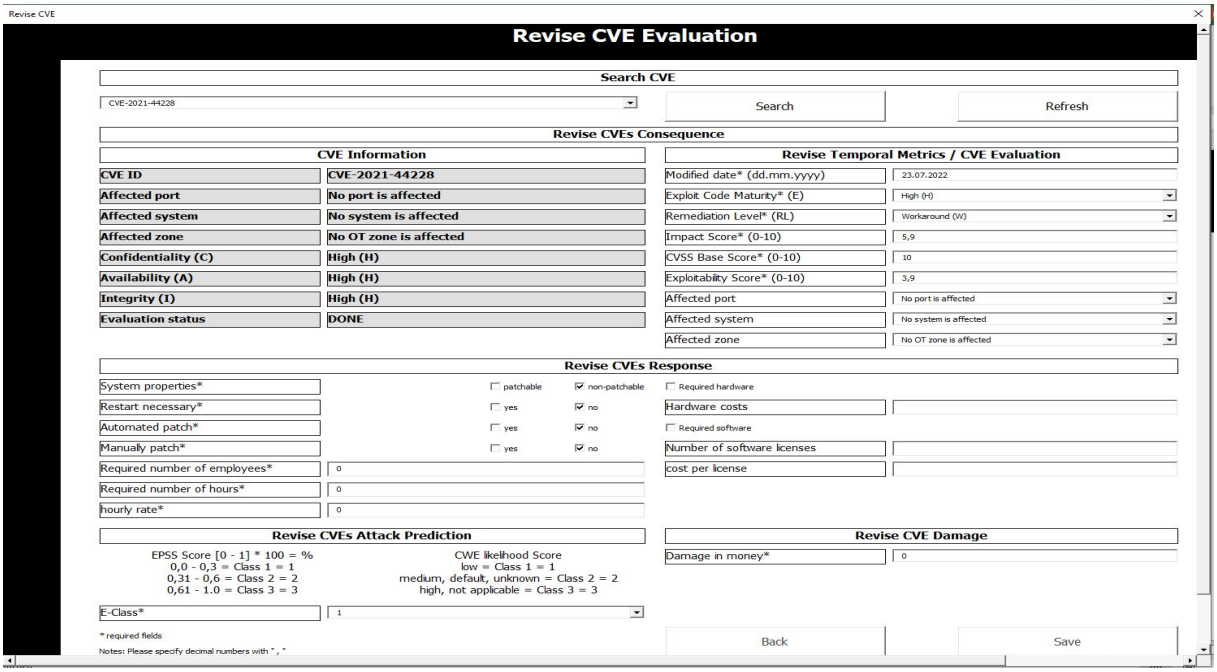
A.25: *IRET-CVE Evaluation Results CVE-2021-44228 (Quelle: Eigene Darstellung)*



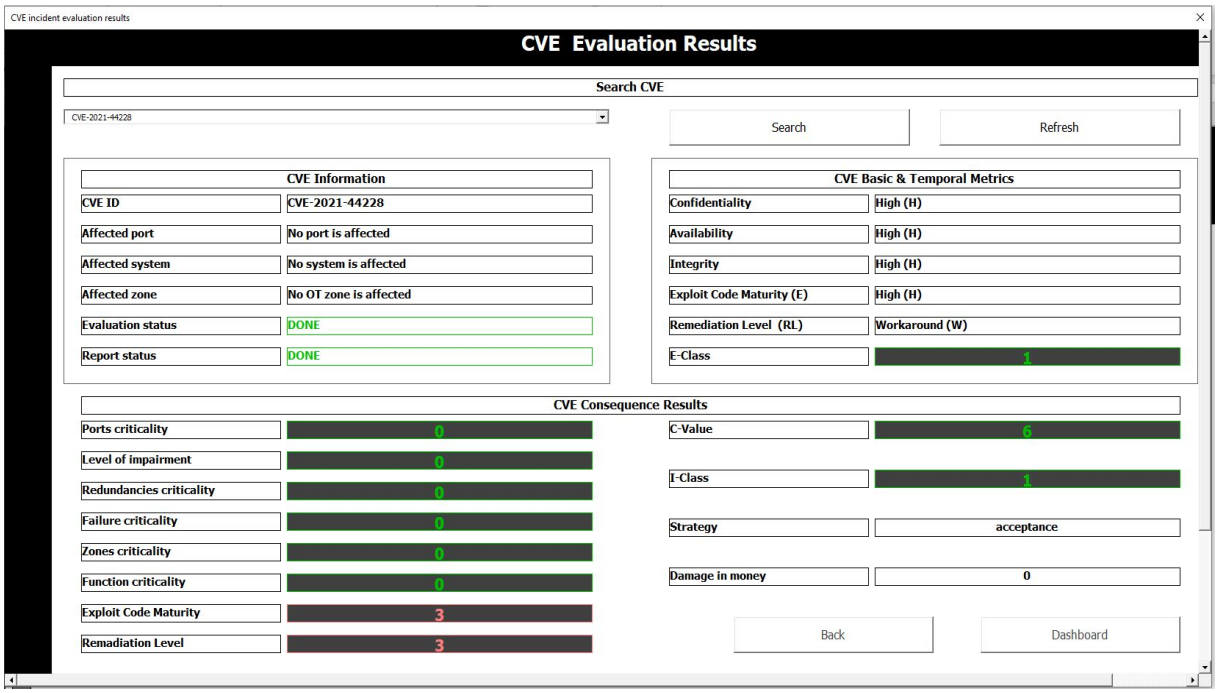
A.26: *IRET-CVE Final Results CVE-2021-44228 (Quelle: Eigene Darstellung)*



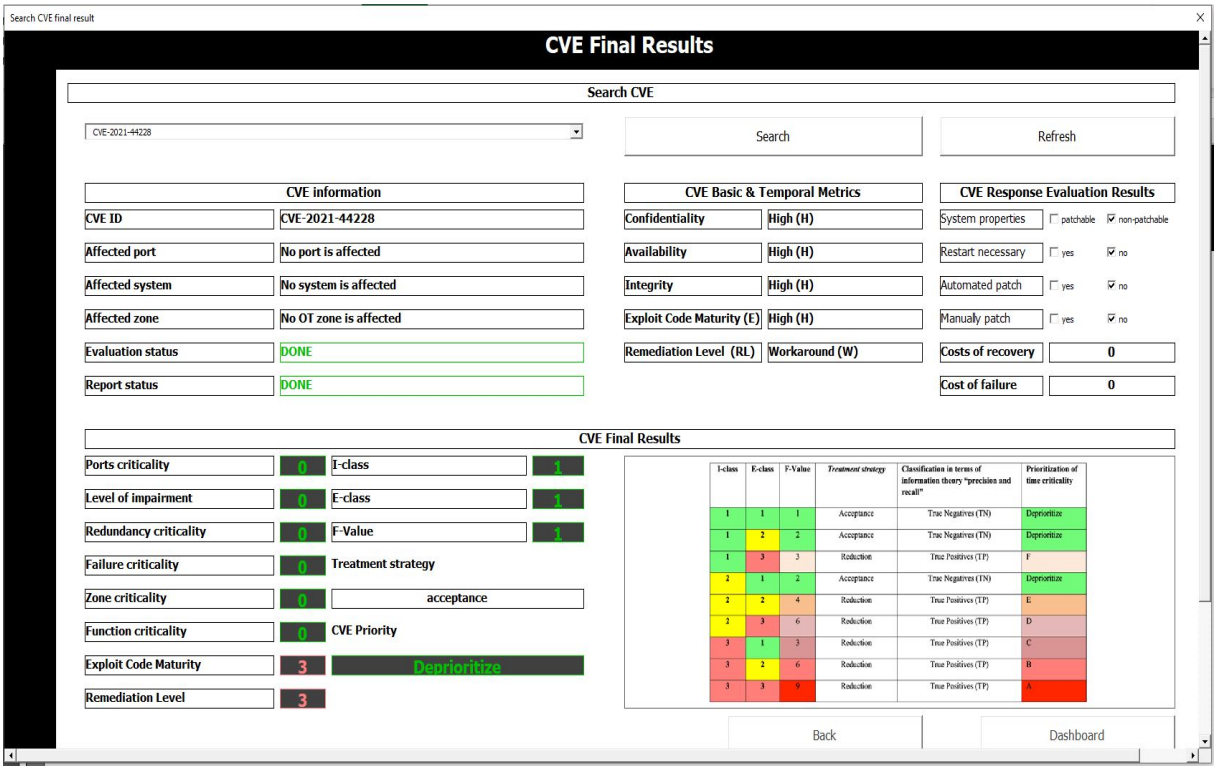
A.27: *IRET-CVE Evaluation mit veränderten Zuordnungswerten (Quelle: Eigene Darstellung)*



A.28: *IRET-CVE Neuberechnung mit veränderten Zuordnungswerten (Quelle: Eigene Darstellung)*



A.29: *Neue CVE-Priorisierungsstrategie durch veränderte Zuordnungswerte (Quelle: Eigene Darstellung)*



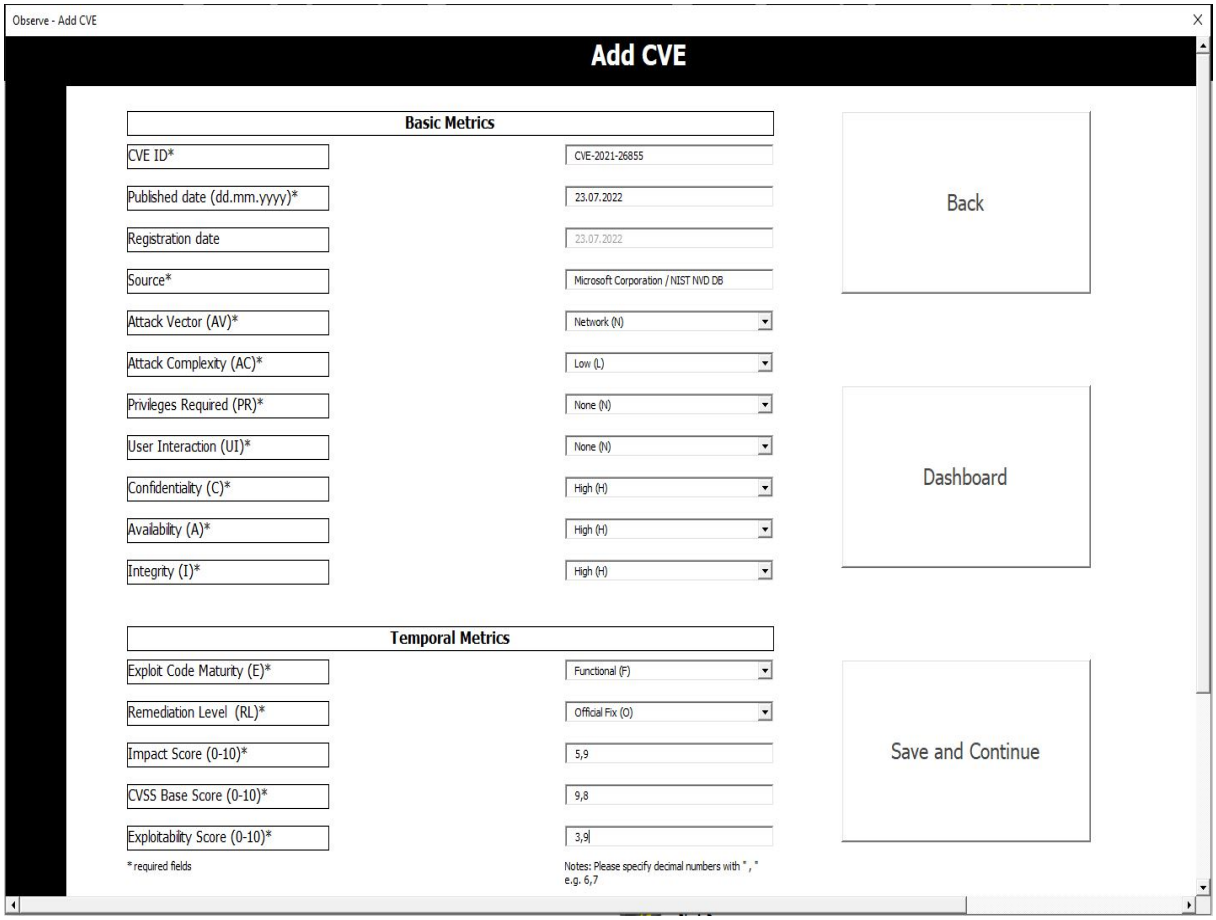
A.30: *IRET-Neue Redundanzkritikalitäten für die Berechnung der CVE-2021-26855 (Quelle: Eigene Darstellung)*

Do not change data from here (use arrow to change)

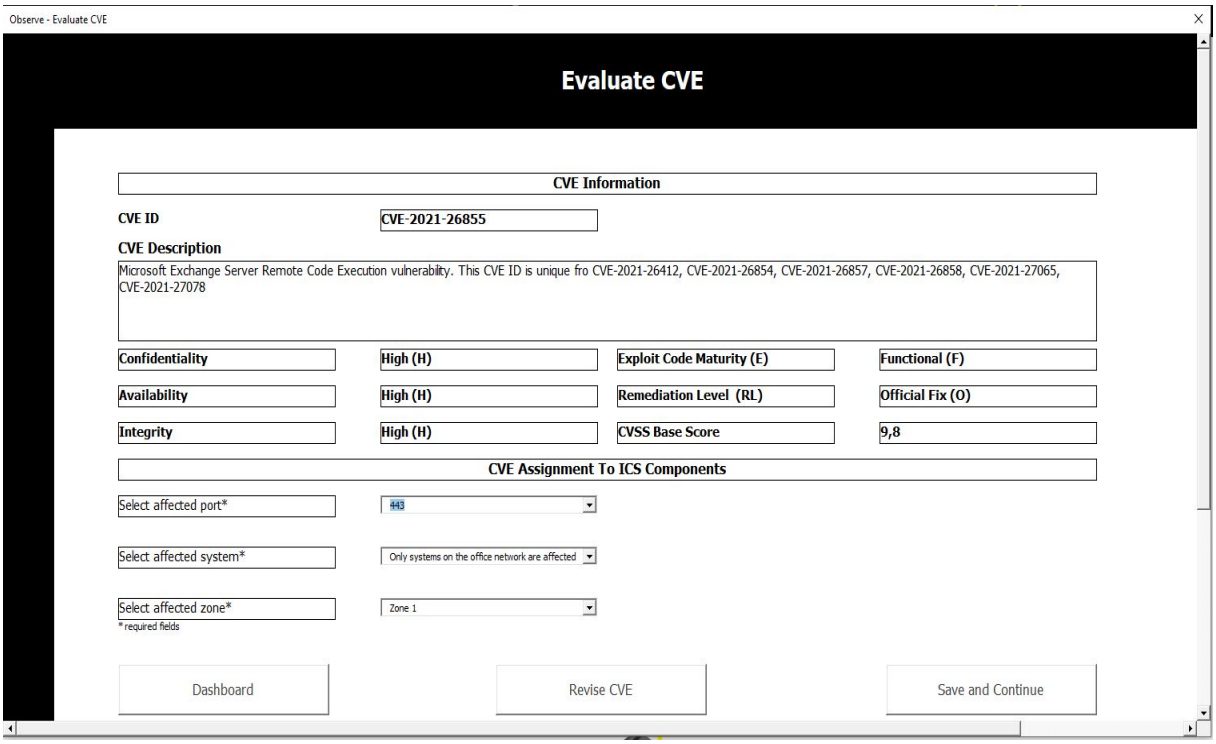
f2 _ Redundancy - Criticality

ID	System	Value	Criticality
0	No system is affected	0	none
1	Only systems on the office network are affected	3	none
2	Affected systems are outside the ICS network	3	none
3	Multiple systems are affected	3	critical

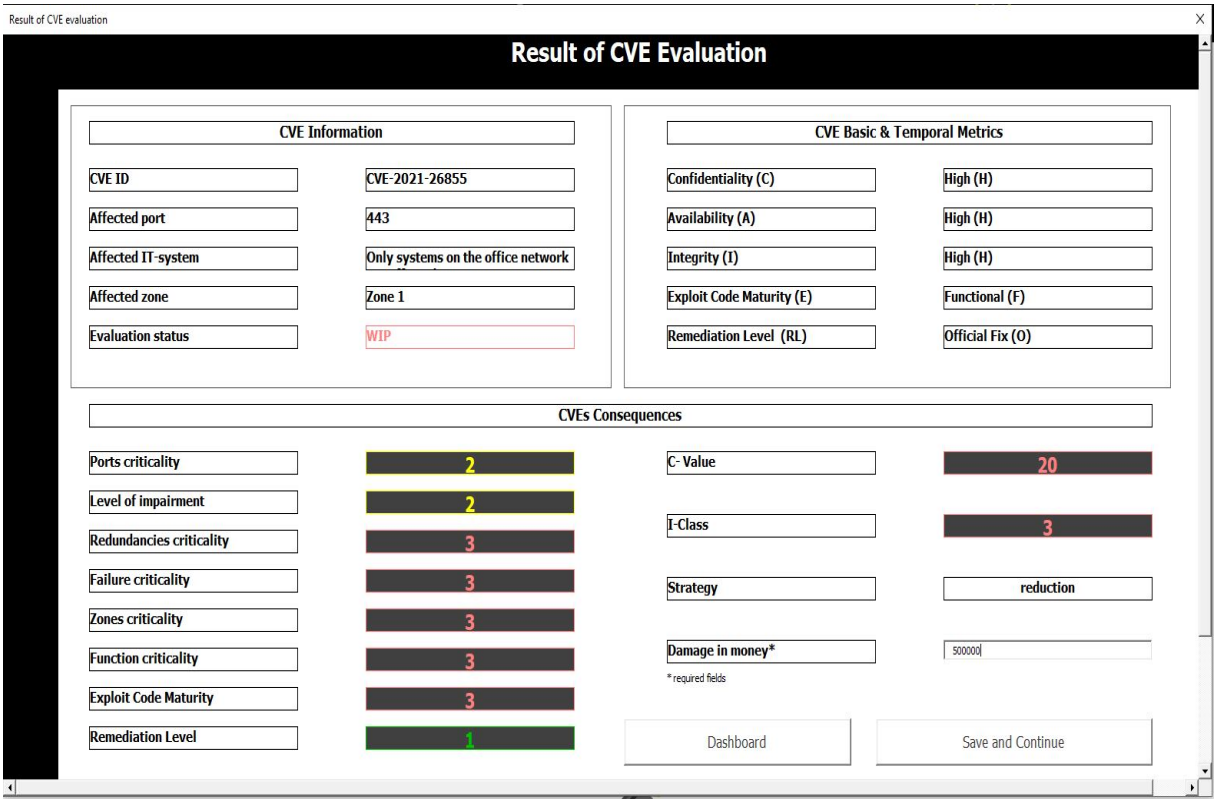
A.31: *IRET-Add CVE 2021-26855 (Quelle: Eigene Darstellung)*



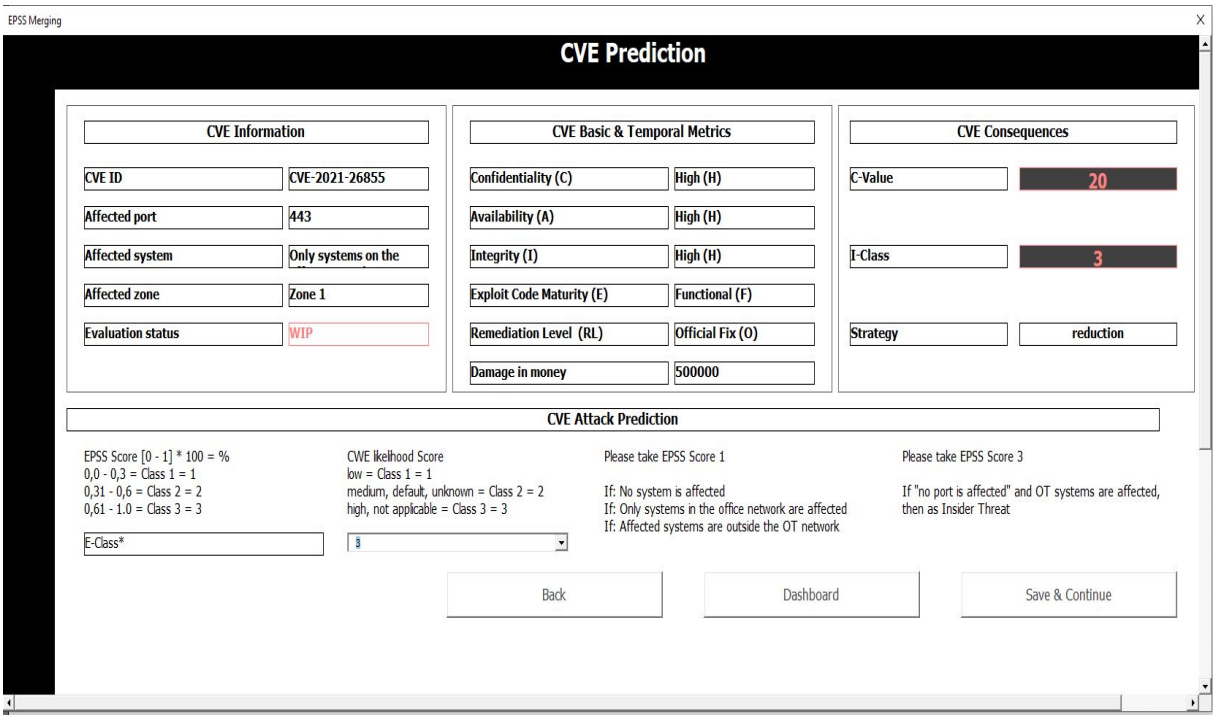
A.32: *IRET-Zuordnungswerte CVE 2021-26855 (Quelle: Eigene Darstellung)*



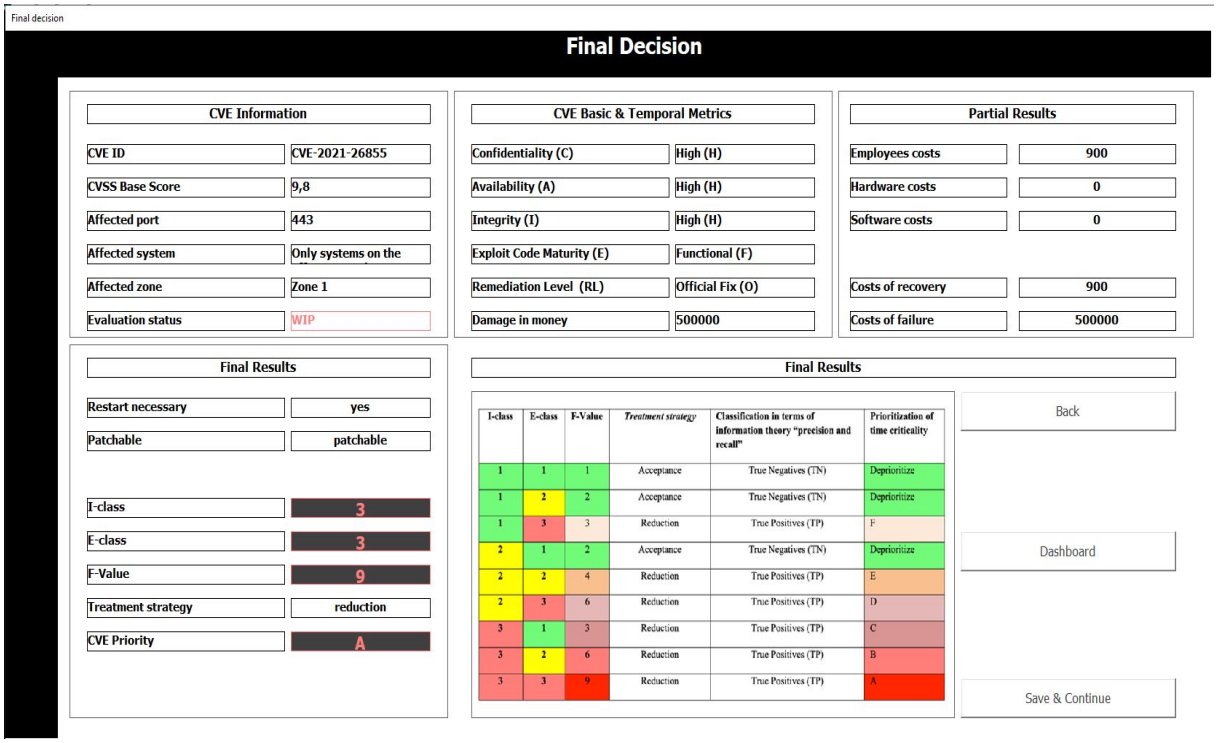
A.33: *IRET-Übersicht des erreichten Schadenausmaßes zur CVE-2021-26855 (Quelle: Eigene Darstellung)*



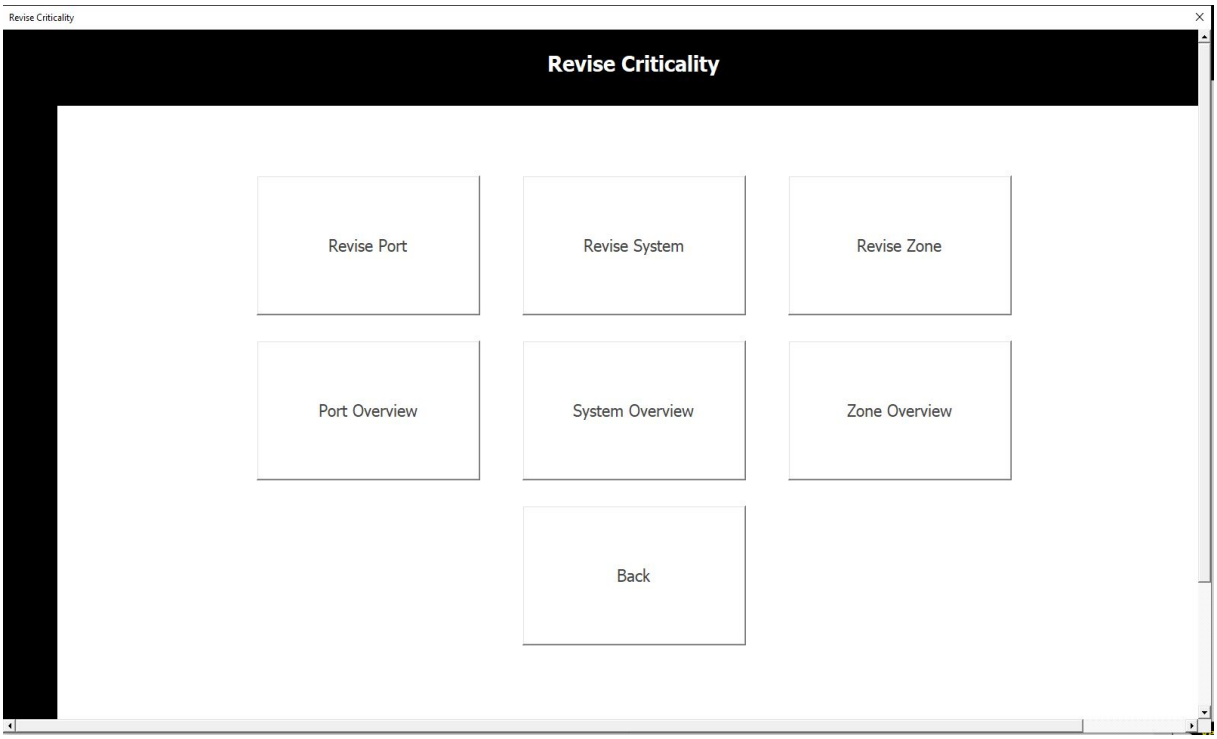
A.34: *IRET-Bestimmung der Eintrittswahrscheinlichkeit der CVE-2021-26855 (Quelle: In Anlehnung an Koza, 2023, S. 115)*



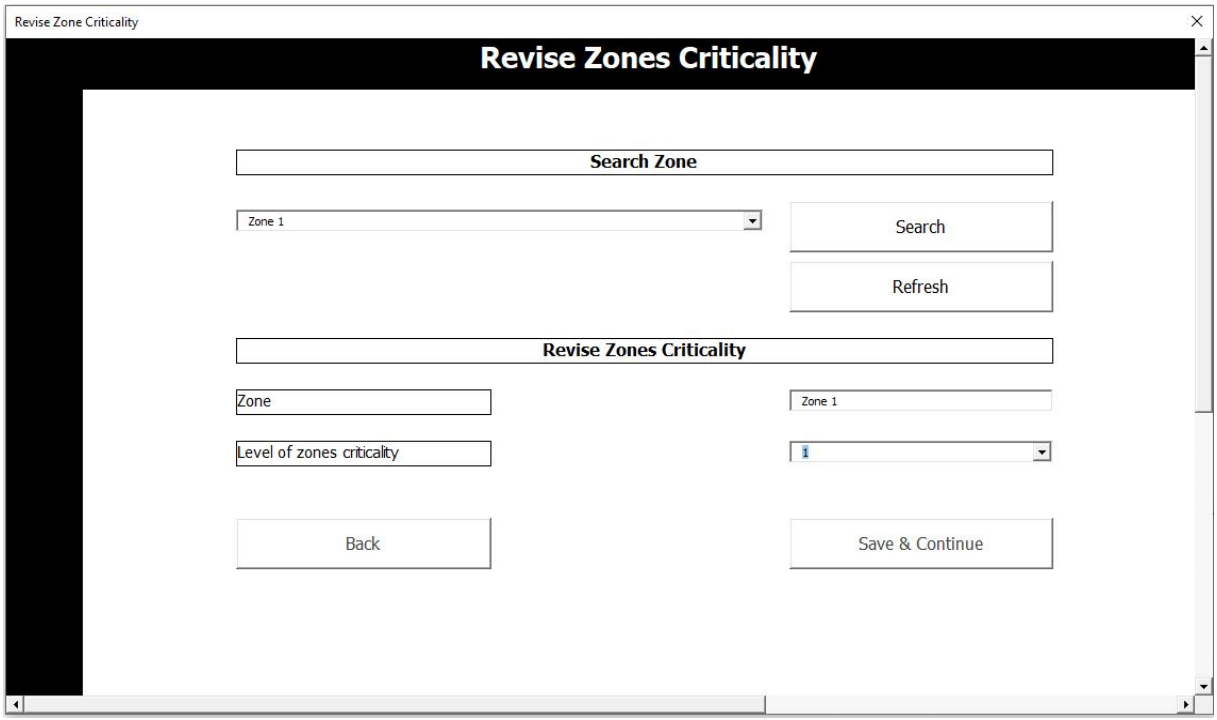
A.35: *IRET-Finale Priorisierungsstrategie zur CVE-2021-26855 (Quelle: In Anlehnung an Koza, 2023, S. 115)*



A.36: *IRET-Dialogfenster: Revise Criticality (Quelle: Eigene Darstellung)*



A.37: *IRET-Dialogfenster: Revise Zones Criticality (Quelle: Eigene Darstellung)*



A.38: *IRET-Datenblatt: Zone Criticality zum Überblick der Zonenkritikalitäten (Quelle: Eigene Darstellung)*

Do not change data from here (use arrow to change)

F 3_ Zone Criticality

ID	Zone	Value	Criticality
0	No OT zone is affected	0	none
1	Multiple zones are affected	3	critical
2	Zone 4	3	critical
3	Zone 1	1	low
4	Zone 2	2	high
5	Zone 3	3	critical
6	Zone 5	3	critical

A.39: *IRET-Datenblatt: Ports Criticality zum Überblick der Zonenkritikalitäten (Quelle: Eigene Darstellung)*

Do not change data from here (use arrow to change)

F1 _ Ports-Criticality

ID	Port	Value	Criticality
0	No port is affected	0	low
1	Insider threats	3	critical
2	389	3	critical
3	443	1	low

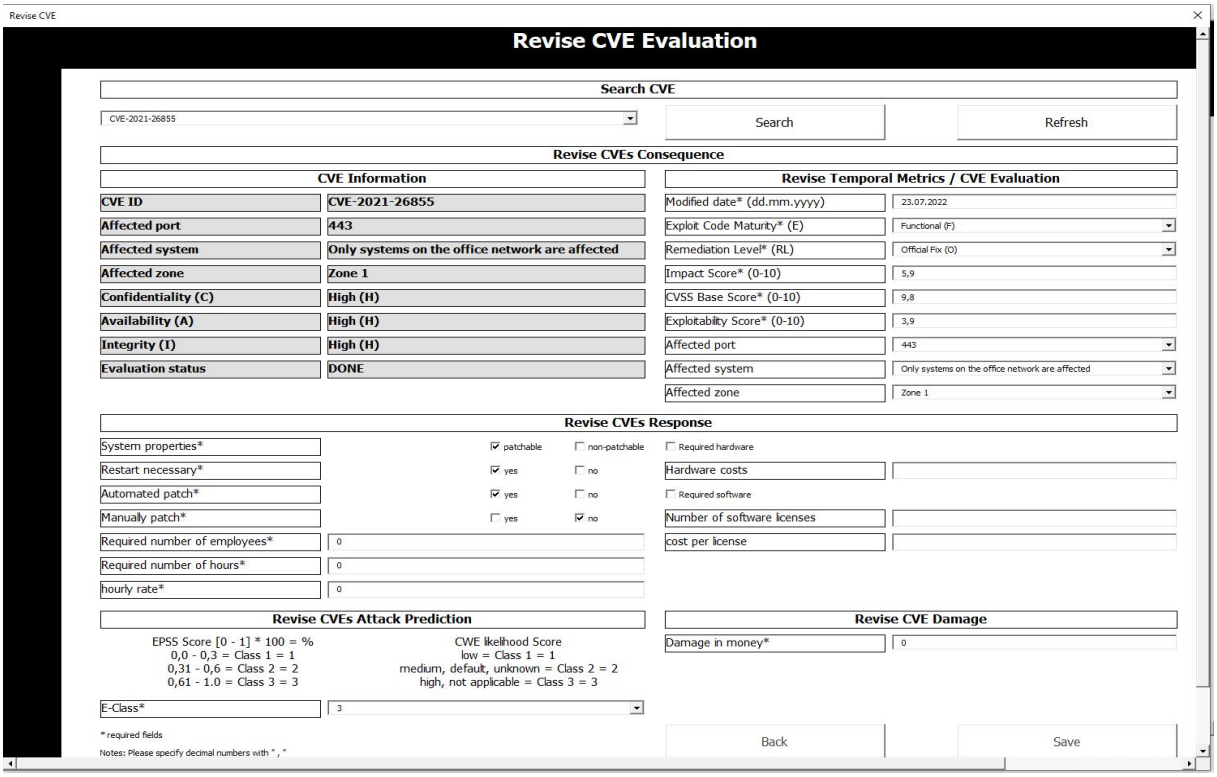
A.40: *IRET-Datenblatt: Redundancy Criticality zum Überblick der Zonenkritikalitäten (Quelle: Eigene Darstellung)*

Do not change data from here (use arrow to change)

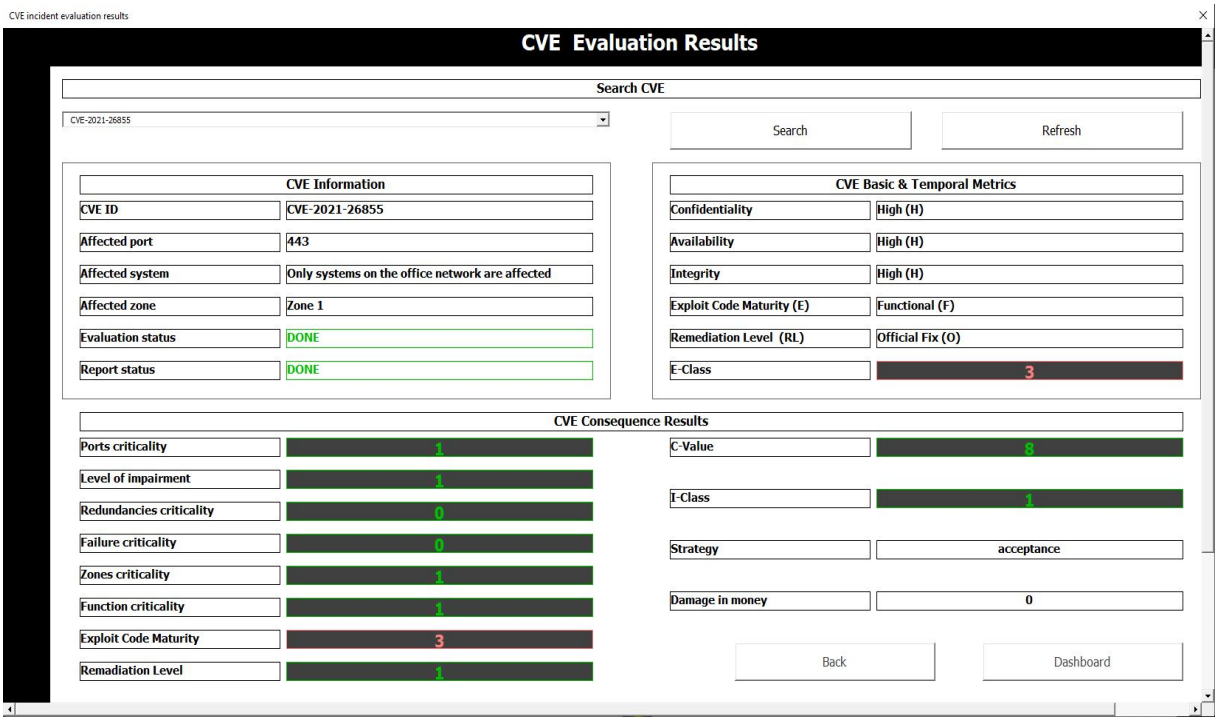
f2 _ Redundancy - Criticality

ID	System	Value	Criticality
0	No system is affected	0	none
1	Only systems on the office network are affected	0	none
2	Affected systems are outside the ICS network	0	none
3	Multiple systems are affected	3	critical
4	SCADA - Server (MTU)	2	high

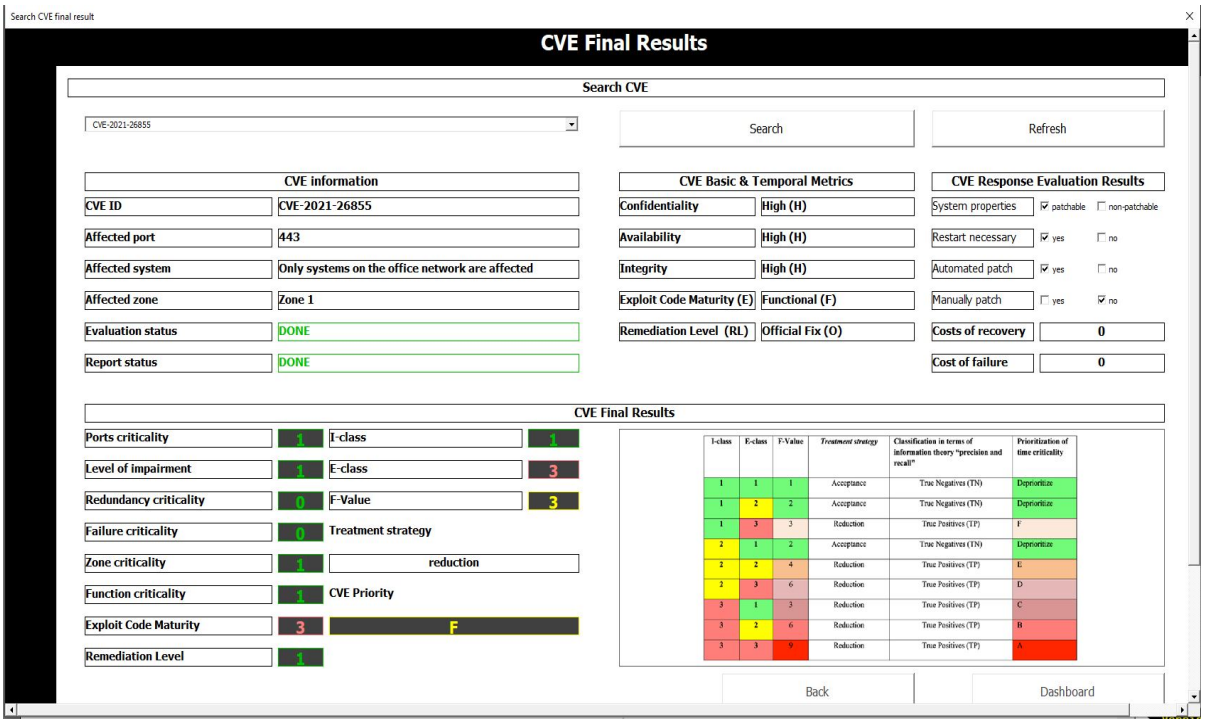
A.41: *IRET-Revise CVE Evaluation der CVE-2021-26855 (Quelle: Eigene Darstellung)*



A.42: *IRET-CVE Evaluation Results der CVE-2021-26855 (Quelle: Eigene Darstellung)*



A.43: *IRET-CVE Final Results der CVE-2021-26855 (Quelle: Eigene Darstellung)*



B. Nachfolgend werden die Ergebnisse der industriellen Evaluierung vorgestellt, die in Kap. 6 der Dissertation ausführlich beschrieben sind. Die Evaluierung sieht in den Tabellen B.1 bis B. 6 die Betrachtung der 60 CVE vor, die durch die Fachanwender sowohl manuell als auch mit IRET bewertet wurden.

B.1: Zunächst erfolgt in B.1 eine Übersicht über die CVE, die Bestandteil der Evaluierung waren, zugeordnet zu ihrem CVSS B-Score.

B.1: *Übersicht der CVE in der industriellen Evaluierungsphase (Quelle: Eigene Darstellung)*

ID	CVE-ID	CVSS B-Score
ID-01	CVE-2022-0xxx	7,5
ID-02	CVE-2022-2xxx	8,8
ID-03	CVE-2022-3xxx	9,8
ID-04	CVE-2022-2xxx	9,6
ID-05	CVE-2021-4xxx	7,5
ID-06	CVE-2022-2xxx	9,8
ID-07	CVE-2022-0xxx	9,8
ID-08	CVE-2021-3xxx	7,5
ID-09	CVE-2021-2xxx	8,5
ID-10	CVE-2022-3xxx	8,8
ID-11	CVE-2022-3xxx	8,0
ID-12	CVE-2022-2xxx	9,6
ID-13	CVE-2022-2xxx	7,5
ID-14	CVE-2021-3xxx	6,5
ID-15	CVE-2018-1xxx	9,8
ID-16	CVE-2021-2xxx	9,8
ID-17	CVE-2022-2xxx	9,6
ID-18	CVE-2022-2xxx	8,8
ID-19	CVE-2022-1xxx	7,5
ID-20	CVE-2022-2xxx	6,8
ID-21	CVE-2022-2xxx	8,6
ID-22	CVE-2022-2xxx	9,8
ID-23	CVE-2022-2xxx	8,0
ID-24	CVE-2022-2xxx	7,8
ID-25	CVE-2022-2xxx	7,3
ID-26	CVE-2021-3xxx	8,8
ID-27	CVE-2022-1xxx	8,8
ID-28	CVE-2022-1xxx	9,6
ID-29	CVE-2022-2xxx	8,8
ID-30	CVE-2022-1xxx	6,4

ID-31	CVE-2021-2xxx	8,1
ID-32	CVE-2021-0xxx	8,8
ID-33	CVE-2021-3xxx	8,8
ID-34	CVE-2021-2xxx	6,5
ID-35	CVE-2022-0xxx	8,8
ID-36	CVE-2022-2xxx	4,3
ID-37	CVE-2022-2xxx	8,8
ID-38	CVE-2022-2xxx	8,2
ID-39	CVE-2021-2xxx	6,5
ID-40	CVE-2021-0xxx	8,2
ID-41	CVE-2022-2xxx	8,2
ID-42	CVE-2022-2xxx	9,6
ID-43	CVE-2022-0xxx	6,3
ID-44	CVE-2021-2xxx	6,5
ID-45	CVE-2021-3xxx	8,8
ID-46	CVE-2022-0xxx	8,8
ID-47	CVE-2021-2xxx	8,2
ID-48	CVE-2022-2xxx	7,4
ID-49	CVE-2022-2xxx	8,8
ID-50	CVE-2021-0xxx	7,3
ID-51	CVE-2022-0xxx	9,6
ID-52	CVE-2022-2xxx	9,8
ID-53	CVE-2022-2xxx	9,8
ID-54	CVE-2021-4xxx	6,5
ID-55	CVE-2022-0xxx	8,8
ID-56	CVE-2021-2xxx	7,3
ID-57	CVE-2021-3xxx	7,3
ID-58	CVE-2021-2xxx	9,8
ID-59	CVE-2022-2xxx	7,5
ID-60	CVE-2021-3xxx	8,5

B.2 stellt eine Übersicht dar, aus der hervorgeht, wie die einzelnen CVE zum einen von den Experten manuell eingestuft wurden (als TN oder TP) und zum anderen die Bewertung, die auf Grundlage objektiver Kriterien durch IRET erfolgt.

B.2: *Gegenüberstellung der Expertenbewertung und IRET-Bewertung (Quelle: Eigene Darstellung)*

ID	CVE-ID	Expertenbewertung	IRET-Bewertung
ID-01	CVE-2022-0xxx	TN	TP
ID-02	CVE-2022-2xxx	TP	TP
ID-03	CVE-2022-3xxx	TP	TP
ID-04	CVE-2022-2xxx	TN	TP
ID-05	CVE-2021-4xxx	TP	TP
ID-06	CVE-2022-2xxx	TP	TP
ID-07	CVE-2022-0xxx	TP	TP
ID-08	CVE-2021-3xxx	TP	TP
ID-09	CVE-2021-2xxx	TN	TP
ID-10	CVE-2022-3xxx	TN	TP
ID-11	CVE-2022-3xxx	TN	TP
ID-12	CVE-2022-2xxx	TP	TP
ID-13	CVE-2022-2xxx	TN	TP
ID-14	CVE-2021-3xxx	TN	TP
ID-15	CVE-2018-1xxx	TP	TN
ID-16	CVE-2021-2xxx	TN	TN
ID-17	CVE-2022-2xxx	TN	TP
ID-18	CVE-2022-2xxx	TN	TP
ID-19	CVE-2022-1xxx	TP	TP
ID-20	CVE-2022-2xxx	TN	TP
ID-21	CVE-2022-2xxx	TN	TN
ID-22	CVE-2022-2xxx	TN	TP
ID-23	CVE-2022-2xxx	TP	TP
ID-24	CVE-2022-2xxx	TP	TP
ID-25	CVE-2022-2xxx	TP	TN
ID-26	CVE-2021-3xxx	TP	TP
ID-27	CVE-2022-1xxx	TP	TN
ID-28	CVE-2022-1xxx	TP	TN
ID-29	CVE-2022-2xxx	TP	TP
ID-30	CVE-2022-1xxx	TP	TP
ID-31	CVE-2021-2xxx	TN	TP
ID-32	CVE-2021-0xxx	TN	TN
ID-33	CVE-2021-3xxx	TP	TN

ID-34	CVE-2021-2xxx	TN	TP
ID-35	CVE-2022-0xxx	TP	TP
ID-36	CVE-2022-2xxx	TP	TP
ID-37	CVE-2022-2xxx	TN	TP
ID-38	CVE-2022-2xxx	TP	TP
ID-39	CVE-2021-2xxx	TP	TP
ID-40	CVE-2021-0xxx	TN	TP
ID-41	CVE-2022-2xxx	TN	TN
ID-42	CVE-2022-2xxx	TN	TP
ID-43	CVE-2022-0xxx	TN	TN
ID-44	CVE-2021-2xxx	TN	TN
ID-45	CVE-2021-3xxx	TN	TN
ID-46	CVE-2022-0xxx	TP	TP
ID-47	CVE-2021-2xxx	TN	TN
ID-48	CVE-2022-2xxx	TP	TP
ID-49	CVE-2022-2xxx	TP	TP
ID-50	CVE-2021-0xxx	TN	TN
ID-51	CVE-2022-0xxx	TP	TP
ID-52	CVE-2022-2xxx	TP	TP
ID-53	CVE-2022-2xxx	TP	TP
ID-54	CVE-2021-4xxx	TP	TP
ID-55	CVE-2022-0xxx	TP	TP
ID-56	CVE-2021-2xxx	TP	TP
ID-57	CVE-2021-3xxx	TP	TP
ID-58	CVE-2021-2xxx	TP	TP
ID-59	CVE-2022-2xxx	TP	TP
ID-60	CVE-2021-3xxx	TP	TN

B.3 zeigt die gemessene Zeit an, in der die einzelnen CVE bewertet wurden. Die gemessene Zeiteinheit der Expertenbewertung manuell sowie durch Anwendung des Kohärenzmodells in IRET.

B.3: *Gemessene Zeit der Experten- und IRET-Bewertungen (Quelle Eigene Darstellung)*

ID	CVE-ID	Gemessene Zeiteinheit der Expertenbewertung	Gemessene Zeiteinheit der IRET-Bewertung
ID-01	CVE-2022-0xxx	00:20:00	00:06:00
ID-02	CVE-2022-2xxx	00:16:00	00:08:00
ID-03	CVE-2022-3xxx	00:14:00	00:08:00
ID-04	CVE-2022-2xxx	00:20:00	00:07:00
ID-05	CVE-2021-4xxx	00:20:00	00:06:00
ID-06	CVE-2022-2xxx	00:20:00	00:07:00
ID-07	CVE-2022-0xxx	00:20:00	00:05:00
ID-08	CVE-2021-3xxx	00:18:00	00:06:00
ID-09	CVE-2021-2xxx	00:20:00	00:07:00
ID-10	CVE-2022-3xxx	00:20:00	00:07:00
ID-11	CVE-2022-3xxx	00:20:00	00:05:00
ID-12	CVE-2022-2xxx	00:20:00	00:06:00
ID-13	CVE-2022-2xxx	00:10:00	00:05:00
ID-14	CVE-2021-3xxx	00:20:00	00:06:00
ID-15	CVE-2018-1xxx	00:16:00	00:06:00
ID-16	CVE-2021-2xxx	00:18:00	00:05:00
ID-17	CVE-2022-2xxx	00:18:00	00:06:00
ID-18	CVE-2022-2xxx	00:24:00	00:05:00
ID-19	CVE-2022-1xxx	00:20:00	00:04:00
ID-20	CVE-2022-2xxx	00:18:00	00:04:00
ID-21	CVE-2022-2xxx	00:26:00	00:05:00
ID-22	CVE-2022-2xxx	00:24:00	00:06:00
ID-23	CVE-2022-2xxx	00:20:00	00:05:00
ID-24	CVE-2022-2xxx	00:28:00	00:04:00
ID-25	CVE-2022-2xxx	00:32:00	00:04:00
ID-26	CVE-2021-3xxx	00:20:00	00:05:00
ID-27	CVE-2022-1xxx	00:24:00	00:05:00
ID-28	CVE-2022-1xxx	00:22:00	00:06:00
ID-29	CVE-2022-2xxx	00:18:00	00:05:00
ID-30	CVE-2022-1xxx	00:30:00	00:09:00
ID-31	CVE-2021-2xxx	00:26:00	00:05:00
ID-32	CVE-2021-0xxx	00:18:00	00:06:00
ID-33	CVE-2021-3xxx	00:16:00	00:04:00

ID-34	CVE-2021-2xxx	00:14:00	00:06:00
ID-35	CVE-2022-0xxx	00:20:00	00:05:00
ID-36	CVE-2022-2xxx	00:18:00	00:04:00
ID-37	CVE-2022-2xxx	00:22:00	00:05:00
ID-38	CVE-2022-2xxx	00:18:00	00:05:00
ID-39	CVE-2021-2xxx	00:20:00	00:04:00
ID-40	CVE-2021-0xxx	00:18:00	00:05:00
ID-41	CVE-2022-2xxx	00:22:00	00:04:00
ID-42	CVE-2022-2xxx	00:26:00	00:05:00
ID-43	CVE-2022-0xxx	00:20:00	00:05:00
ID-44	CVE-2021-2xxx	00:30:00	00:03:00
ID-45	CVE-2021-3xxx	00:24:00	00:04:00
ID-46	CVE-2022-0xxx	00:18:00	00:03:00
ID-47	CVE-2021-2xxx	00:30:00	00:04:00
ID-48	CVE-2022-2xxx	00:24:00	00:05:00
ID-49	CVE-2022-2xxx	00:28:00	00:04:00
ID-50	CVE-2021-0xxx	00:22:00	00:05:00
ID-51	CVE-2022-0xxx	00:32:00	00:04:00
ID-52	CVE-2022-2xxx	00:24:00	00:04:00
ID-53	CVE-2022-2xxx	00:14:00	00:05:00
ID-54	CVE-2021-4xxx	00:20:00	00:04:00
ID-55	CVE-2022-0xxx	00:20:00	00:06:00
ID-56	CVE-2021-2xxx	00:16:00	00:08:00
ID-57	CVE-2021-3xxx	00:14:00	00:08:00
ID-58	CVE-2021-2xxx	00:20:00	00:07:00
ID-59	CVE-2022-2xxx	00:20:00	00:06:00
ID-60	CVE-2021-3xxx	00:20:00	00:07:00
	∑	**21:44:00**	**05:03:00**

B.4 zeigt die Gemeinsamkeiten (Match) und Unterschiede (Mismatch) an, die bei den beiden Bewertungen durch die Experten und durch Nutzung des Kohärenzmodells im IRET erfolgt sind.

B.4: *Einzelbewertung beider Verfahren (Quelle Eigene Darstellung)*

ID	CVE-ID	Expertenbewertung	IRET-Bewertung	Gegenüberstellung	Gesamtbewertung
ID-01	CVE-2022-0xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-02	CVE-2022-2xxx	TP	TP	Match	TP
ID-03	CVE-2022-3xxx	TP	TP	Match	TP
ID-04	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-05	CVE-2021-4xxx	TP	TP	Match	TP
ID-06	CVE-2022-2xxx	TP	TP	Match	TP
ID-07	CVE-2022-0xxx	TP	TP	Match	TP
ID-08	CVE-2021-3xxx	TP	TP	Match	TP
ID-09	CVE-2021-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-10	CVE-2022-3xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-11	CVE-2022-3xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-12	CVE-2022-2xxx	TP	TP	Match	TP
ID-13	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-14	CVE-2021-3xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-15	CVE-2018-1xxx	**TP**	**TN**	**Mismatch**	**FP**
ID-16	CVE-2021-2xxx	TN	TN	Match	TN
ID-17	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-18	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-19	CVE-2022-1xxx	TP	TP	Match	TP
ID-20	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-21	CVE-2022-2xxx	TN	TN	Match	TP
ID-22	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-23	CVE-2022-2xxx	TP	TP	Match	TP
ID-24	CVE-2022-2xxx	TP	TP	Match	TP
ID-25	CVE-2022-2xxx	**TP**	**TN**	**Mismatch**	**FP**
ID-26	CVE-2021-3xxx	TP	TP	Match	TP
ID-27	CVE-2022-1xxx	**TP**	**TN**	**Mismatch**	**FP**
ID-28	CVE-2022-1xxx	**TP**	**TN**	**Mismatch**	**FP**
ID-29	CVE-2022-2xxx	TP	TP	Match	TP
ID-30	CVE-2022-1xxx	TP	TP	Match	TP
ID-31	CVE-2021-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-32	CVE-2021-0xxx	TN	TN	Match	TN
ID-33	CVE-2021-3xxx	**TP**	**TN**	**Mismatch**	**FP**
ID-34	CVE-2021-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-35	CVE-2022-0xxx	TP	TP	Match	TP

ID-36	CVE-2022-2xxx	TP	TP	Match	TP
ID-37	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-38	CVE-2022-2xxx	TP	TP	Match	TP
ID-39	CVE-2021-2xxx	TP	TP	Match	TP
ID-40	CVE-2021-0xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-41	CVE-2022-2xxx	TN	TN	Match	TN
ID-42	CVE-2022-2xxx	**TN**	**TP**	**Mismatch**	**FN**
ID-43	CVE-2022-0xxx	TN	TN	Match	TN
ID-44	CVE-2021-2xxx	TN	TN	Match	TN
ID-45	CVE-2021-3xxx	TN	TN	Match	TN
ID-46	CVE-2022-0xxx	TP	TP	Match	TP
ID-47	CVE-2021-2xxx	TN	TN	Match	TN
ID-48	CVE-2022-2xxx	TP	TP	Match	TP
ID-49	CVE-2022-2xxx	TP	TP	Match	TP
ID-50	CVE-2021-0xxx	TN	TN	Match	TN
ID-51	CVE-2022-0xxx	TP	TP	Match	TP
ID-52	CVE-2022-2xxx	TP	TP	Match	TP
ID-53	CVE-2022-2xxx	TP	TP	Match	TP
ID-54	CVE-2021-4xxx	TP	TP	Match	TP
ID-55	CVE-2022-0xxx	TP	TP	Match	TP
ID-56	CVE-2021-2xxx	TP	TP	Match	TP
ID-57	CVE-2021-3xxx	TP	TP	Match	TP
ID-58	CVE-2021-2xxx	TP	TP	Match	TP
ID-59	CVE-2022-2xxx	TP	TP	Match	TP
ID-60	CVE-2021-3xxx	**TP**	**TN**	**Mismatch**	**FP**

B.5 zeigt die CVE an, die durch die Experten sowohl manuell als auch durch Anwendung des Kohärenzmodells übereinstimmend bewertet wurden (TP = TP).

B.5: *Übersicht der übereinstimmenden CVE-Bewertungen beider Verfahren (Quelle: Eigene Darstellung)*

ID	Expertenbewertung	IRET-Bewertung	Konstellation | Gesamtbewertung	
ID-02	TP	TP	TP<>TP	**TP**
ID-03	TP	TP	TP<>TP	**TP**
ID-05	TP	TP	TP<>TP	**TP**
ID-06	TP	TP	TP<>TP	**TP**
ID-07	TP	TP	TP<>TP	**TP**
ID-08	TP	TP	TP<>TP	**TP**
ID-12	TP	TP	TP<>TP	**TP**
ID-16	TN	TN	TN<>TN	**TN**
ID-19	TP	TP	TP<>TP	**TP**
ID-21	TN	TN	TN<>TN	**TN**
ID-23	TP	TP	TP<>TP	**TP**
ID-24	TP	TP	TP<>TP	**TP**
ID-26	TP	TP	TP<>TP	**TP**
ID-29	TP	TP	TP<>TP	**TP**
ID-30	TP	TP	TP<>TP	**TP**
ID-32	TN	TN	TN<>TN	**TN**
ID-35	TP	TP	TP<>TP	**TP**
ID-36	TP	TP	TP<>TP	**TP**
ID-38	TP	TP	TP<>TP	**TP**
ID-39	TP	TP	TP<>TP	**TP**
ID-41	TN	TN	TN<>TN	**TN**
ID-43	TN	TN	TN<>TN	**TN**
ID-44	TN	TN	TN<>TN	**TN**
ID-45	TN	TN	TN<>TN	**TN**
ID-46	TP	TP	TP<>TP	**TP**
ID-47	TN	TN	TN<>TN	**TN**
ID-48	TP	TP	TP<>TP	**TP**
ID-49	TP	TP	TP<>TP	**TP**
ID-50	TN	TN	TN<>TN	**TN**
ID-51	TP	TP	TP<>TP	**TP**

ID-52	TP	TP	TP<>TP	**TP**
ID-53	TP	TP	TP<>TP	**TP**
ID-54	TP	TP	TP<>TP	**TP**
ID-55	TP	TP	TP<>TP	**TP**
ID-56	TP	TP	TP<>TP	**TP**
ID-57	TP	TP	TP<>TP	**TP**
ID-58	TP	TP	TP<>TP	**TP**
ID-59	TP	TP	TP<>TP	**TP**

B.6 zeigt die CVE an, die durch die Experten sowohl manuell als auch durch Anwendung des Kohärenzmodells nicht übereinstimmend bewertet wurden (TN = TP), bzw. (TP = TN).

B.6: *Übersicht der nicht-übereinstimmenden CVE-Bewertungen beider Verfahren (Quelle: Eigene Darstellung)*

ID	Expertenbewertung	IRET-Bewertung	Konstellation | Gesamtbewertung	
ID-01	TN	TP	TN<>TP	**FN**
ID-04	TN	TP	TN<>TP	**FN**
ID-09	TN	TP	TN<>TP	**FN**
ID-10	TN	TP	TN<>TP	**FN**
ID-11	TN	TP	TN<>TP	**FN**
ID-13	TN	TP	TN<>TP	**FN**
ID-14	TN	TP	TN<>TP	**FN**
ID-15	TP	TN	TP<>TN	**FP**
ID-17	TN	TP	TN<>TP	**FN**
ID-18	TN	TP	TN<>TP	**FN**
ID-20	TN	TP	TN<>TP	**FN**
ID-22	TN	TP	TN<>TP	**FN**
ID-25	TP	TN	TP<>TN	**FP**
ID-27	TP	TN	TP<>TN	**FP**
ID-28	TP	TN	TP<>TN	**FP**
ID-31	TN	TP	TN<>TP	**FN**
ID-33	TP	TN	TP<>TN	**FP**
ID-34	TN	TP	TN<>TP	**FN**
ID-37	TN	TP	TN<>TP	**FN**
ID-40	TN	TP	TN<>TP	**FN**
ID-42	TN	TP	TN<>TP	**FN**
ID-60	TP	TN	TP<>TN	**FP**

Lebenslauf

Der Lebenslauf ist in der Online-Version aus Gründen des Datenschutzes nicht enthalten.

Der Lebenslauf ist in der Online-Version aus Gründen des Datenschutzes nicht enthalten.

Der Lebenslauf ist in der Online-Version aus Gründen des Datenschutzes nicht enthalten.