Carl von Ossietzky
Universität
Oldenburg

Fakultät II – Informatik, Wirtschafts- und Rechtswissenshaften
Department für Informatik

Automatisierte Überwachung von Sicherheitskonfigurationen der Betriebstechnik in Stromnetzen – Stärkung des Vertrauens durch kontinuierliche Überwachung der Sicherheitskonfiguration

---

Dissertation zur Erlangung des Grades eines Doktors der Ingenieurwissenschaften

Vorgelegt von
Bastian Fraune, M.Sc. (Informatik)

Gutachter:

Prof. Dr. Sebastian Lehnhoff
Carl von Ossietzky Universität Oldenburg

Prof. Dr. Richard Sethmann
Hochschule Bremen

Prof. Dr. Andreas Peter
Carl von Ossietzky Universität Oldenburg

Datum der Disputation: 16. März 2026

Zusammenfassung

Die fortschreitende Digitalisierung des Stromnetzes erhöht die Angriffsfläche für Cyber-Attacken, die die Stabilität und Zuverlässigkeit der Stromversorgungsnetze beeinträchtigen. Mit dem Ziel, das Stromnetz zu schützen und resilienter zu betreiben, beschreiben verfügbare Cybersicherheitsstandards Sicherheitsanforderungen, die auf die Kommunikationsinfrastruktur und intelligente elektronische Geräte (IEDs) angewendet werden sollten. Um die Cybersicherheit in den Komponenten des Stromnetzes zu gewährleisten, sind kontinuierliches Monitoring, Audit und Compliance-Überprüfung dieser IT-Sicherheitsmaßnahmen notwendig und müssen automatisiert werden.

Eine bedeutende Herausforderung ist jedoch der Mangel an Fernzugriffsmöglichkeiten auf die Sicherheitsmaßnahmen der IEDs im Stromnetz, um deren Sicherheitskonfigurationen zu verifizieren und zu bewerten. Ob die Sicherheitseinstellungen eines IEDs mit den definierten Sicherheitsanforderungen übereinstimmen und den festgelegten Sicherheitsstandards entsprechen, bleibt ohne manuelle Überprüfung ungewiss. Diese Einschränkung verhindert die automatische Feststellung der Übereinstimmung mit Sicherheitsstandards für IEDs im Stromnetz. Um automatisierte Sicherheitsbewertungen zu ermöglichen, müssen Sicherheitskonfigurationsinformationen auf einheitliche Weise bereitgestellt werden. Diese Dissertation bietet daher einen Ansatz, Cybersicherheitskonfigurationen von IEDs innerhalb der Referenzarchitektur des Stromnetzes abzufragen.

Diese Lösung besteht aus zwei Säulen. Die erste Säule etabliert Vertrauen in die IEDs durch die Überprüfung der Software der Hardwareplattform. Zu diesem Zweck wurden Trusted-Platform-Modules integriert und darauf basierend wurde Remote Attestation in die Kommunikationsinfrastruktur eingebettet. Die zweite Säule befasst sich mit den Sicherheitskonfigurationen der Geräte und deren Übertragung innerhalb der bestehenden Kommunikationsarchitektur. Hierzu wurden die relevantesten Cybersicherheitsstandards analysiert und es wurde ein Datenmodell aus ihren Anforderungen erstellt. In der Bewertung wird die Implementierung beider Säulen anhand einer Evaluationsumgebung mit IEDs demonstriert, die über IEC 61850 mit dem Controlcenter kommunizieren. Diese Dissertation zeigt die Machbarkeit der Integration von beidem, verifizierbarem Vertrauen durch Fernattestierung sowie

Sicherheitskonfigurationsinformationen innerhalb der Kommunikations- und Sicherheitsarchitektur des Stromnetzes, um neue, automatisierte Sicherheitsbewertungen zu ermöglichen.

Abstract

The proceeding digitalisation of the power grid increases the surface for cyber-attacks affecting the stability and reliability of supply of electricity grids. To protect the power grid, available cyber security standards describe security controls that should be applied to the communication infrastructure and intelligent electronical devices (IEDs). In order to ensure cyber security of the components in the electricity grid, continuous monitoring, audit and compliance verification with IT security measures are necessary and need to be automated.

However, a significant challenge is the lack of remotely accessing the security measures of IEDs in the power grid to verify and assess their security configurations. Whether the security settings of an IED comply with the defined security requirements and are aligned with defined security standards remains uncertain without manual verification. This limitation prevents automatic determination of compliance with security standards for IEDs in the power grid. In order to enable automated security assessments, security configuration information needs to be provided in a uniform manner. This dissertation hence offers an approach to query cyber security configurations of IEDs within the power grids reference architecture.

This solution consists of two pillars. The first pillar establishes trust in the IEDs and the verification of the hardware platform's software. Trusted platform modules were used for this purpose and remote attestation was embedded in the communication infrastructure based on this. The second pillar addresses the devices' security configurations and their transfer within existing communication architecture. For this purpose, the most relevant cyber security standards were analysed and a data model was created from their requirements.

In the evaluation, the implementation of both pillars is demonstrated based on virtual IEDs, communicating to the control centre via IEC 61850. This thesis shows the feasibility of integrating both, verifiable trust through remote attestation as well as security configuration information within the communication and security architecture of the power grid, to enable new automated security assessments.

Danksagungen

Die Arbeit an dieser Dissertation und deren Fertigstellung haben mich viel Energie und Freizeit gekostet. Es war der bisher längste Marathon meines Lebens, bei dem der Weg nicht markiert war und ich ihn selbst abstecken musste. Am Ende bin ich stolz darauf, die Dissertation „ins Ziel“ gebracht zu haben. Auf diesem Weg war ich meistens nicht allein, weshalb mein besonderer Dank denjenigen gilt, die mich während der Promotion unterstützt haben:

An erster Stelle danke ich meiner Frau **Nele**. Ohne deine bedingungslose, unermüdliche und uneingeschränkte Unterstützung wäre ich nicht so weit gekommen. Du hast dir immer meine Sorgen, Zweifel und Ängste angehört und mir dabei geholfen, optimistisch zu bleiben und nach vorne zu schauen.

Ein ganz großer Dank gilt **Richard**, den ich seit dem ersten Tag meines Bachelorstudiums kenne. Der Zufall, meine Bachelorarbeit über IT-Sicherheit in Stromnetzen schreiben zu können und anschließend an diesen Zukunftsthemen mitarbeiten zu dürfen, hat mein Interesse an diesem Bereich geweckt. Während der gesamten Zeit standest du mir vor allem als Mentor zur Seite. Ich konnte viel von dir lernen und mich persönlich weiterentwickeln – und genau das hat es mir ermöglicht, diese Dissertation zu schreiben. Vielen herzlichen Dank!

Den **KollegInnen** der Forschungsgruppe danke ich für die abwechslungsreichen Projekte und die gute Zusammenarbeit. Mit euch habe ich über die fachlichen Themen hinaus enorm viel gelernt und mich persönlich weiterentwickelt. Danke auch für die konsequent hohen Ansprüche, die wir an uns selbst gestellt haben.

Mein Dank für die ganzheitliche Betreuung gebührt **Sebastian Lehnhoff**. Von der Themenfindung bis zur Verteidigung stand er mir mit seiner Expertise stets zur Seite. Und danke für den Kugelschreiber, der mich in den Stammbaum „einschreibt“.

Danke an **Björn** für den häufigen Austausch und vielen Diskussionen, mit denen wir zusammen während der ersten Corona-Phase unsere Vorhaben gestartet haben.

Abschließend möchte ich all jenen danken, die mich während meiner Studienzeit und auch danach inspiriert haben! Auch wenn viele dieser Begegnungen unbewusst Einfluss auf meinen Weg genommen haben, so haben sie doch alle dazu beigetragen, dass ich heute hier stehe.

Inhaltsverzeichnis

1 Einleitung

Dieses Kapitel dient der Einführung in die vorliegende Arbeit. Zunächst wird die Problemstellung erörtert, aus der die Forschungsfragen abgeleitet werden. Im Anschluss erfolgt die Darlegung des methodischen Vorgehens, welches für die genannte Problemstellung Anwendung findet. Das erste Kapitel schließt mit einer Zusammenfassung sowie der Beschreibung des Aufbaus der Arbeit.

1.1 Motivation

Anmerkung: Einige Teile der Motivation wurden in den Publikationen [Fra22] und [Fra+23] bereits veröffentlicht.

Transformation des Stromnetzes

Der aktuelle Wandel im Stromnetz besteht in der Transformation der bisher zentralen Stromerzeugung hin zur dezentralen Erzeugung. Bislang wurde die Stromerzeugung von einigen wenigen Kraftwerken übernommen und der Strom von dort aus über Stromleitungen und Stromtrassen an die Verbraucher verteilt. Motiviert durch das allgemeine Ziel der CO_2-Reduzierung in der Stromerzeugung kommen zunehmend kleinere und kleinste Stromerzeuger in das Stromnetz [BS20; @Bun13]. Die prominentesten und sichtbarsten Beispiele für diese Entwicklung sind Windkrafträder, Photovoltaik- und Biogasanlagen. Dies führt zu einer Einspeisung auf sämtlichen Ebenen im Stromnetz.

Im Stromnetz müssen die Stromerzeugung und der Verbrauch sekundengenau ausgeglichen sein. Folglich muss zu jedem Zeitpunkt exakt so viel Strom verbraucht werden, wie erzeugt wird. Da im Stromnetz hauptsächlich Wechselspannung vorherrscht, muss zudem eine Netzfrequenz von 50 Hertz (+/- 0,2 Hz) gewährleistet werden [Nor]. Die Systemverantwortung zur Stabilisation der Netzfrequenz obliegt dem Übertragungsnetzbetreiber (ÜNB).

Neben den genannten Beispielen kommen weitere Akteure im Stromversorgungsnetz hinzu: Private Photovoltaikanlagen, Elektroautos mit ihren Batteriespeichern sowie private Speicheranlagen sind bekannte Beispiele für Lasten und Erzeuger im Stromnetz. Das Elektroauto ist aufgrund des derzeit großen Batteriespeichers besonders interessant; denn es kann Strom speichern, an das Stromnetz abgeben und damit im Stromnetz sogenannte Flexibilitäten als Dienstleistung für den Netzbetreiber anbieten. Für die Gesamtstabilität kommen im Stromnetz weitere Systeme zum Einsatz, welche Dienstleistungen bereitstellen, beispielsweise die Einspeisung von Blindstrom durch Photovoltaikanlagen oder andere Geräte. Betreiber eines virtuellen Kraftwerks (VPP) können unterschiedliche Dienstleistungen erbringen: Zum einen für den Eigentümer von einzelnen Photovoltaikanlagen, bei dem das VPP den erzeugten Strom für den Eigentümer am Strommarkt verkauft, zum anderen kann ein VPP am Strommarkt als ein großes Kraftwerk auftreten und so Verteilnetzbetreibern Dienstleistungen anbieten, die eine einzelne Privatperson nicht ökonomisch erbringen könnte. Weiter in der Zukunft, aber dennoch notwendig, sind Agenten, welche kleine Erzeugungsanlagen in privaten Haushalten autonom steuern und die Leistungen anbieten können. Für solche Anwendungsfälle wurde untersucht, wie koalierende Agenten gegenseitig Vertrauen aufbauen können, um gemeinsam dezentral erzeugte Energie zu vermarkten [RUS14].

Zunehmende Kommunikationstechnik im Stromnetz

Die Teilnahme vieler Akteure am Strommarkt sowie deren Integration in das Stromnetz erfordern einen reibungslosen und zuverlässigen Informationsaustausch zwischen Netzbetreibern, Stromanbietern sowie den einzelnen Erzeugern und Verbrauchern. Dazu ist vor allem eine starke Vernetzung durch Informations- und Kommunikationstechnik (IKT) erforderlich. Diese ist notwendig, damit die zahlreichen Lasten, Erzeuger, Service-Anbieter und Marktakteure Statusinformationen austauschen und auf deren Basis das Stromnetz gesteuert werden kann. Das zugrunde liegende IKT-Netz spielt dabei eine entscheidende Rolle. Es ermöglicht die notwendige dezentrale Steuerung von Last und Erzeugung für eine Vielzahl von Erzeugungsanlagen und Verbrauchern und wird durch die fortwährende Stärkung seiner Integration zum Rückgrat des Stromnetzes [BS20].

Angriffe auf das Stromnetz und Bedrohungen

Die zunehmende Vernetzung dieser Supervisory, Control, and Data Acquisition (SCADA)-Systeme sowie die Zunahme von Intelligent Electronic Devices (IEDs) im

Stromnetz vergrößern die Angriffsfläche erheblich. Ein derart komplexes und umfangreiches System eröffnet potenziellen Angreifern eine Vielzahl von Möglichkeiten und eine breite Angriffsfläche [GD20]. Diese Angriffsfläche sowie die steigende Anzahl potenzieller Angriffsvektoren sind gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits evident [Bun23].

Den stärksten Zuwachs an Cyber-Angriffen verzeichnen die Sektoren der kritischen Infrastruktur. In seinem Lagebericht aus dem Jahr 2023 führt das BSI insgesamt 452 Angriffe auf die Sektoren der kritischen Infrastruktur (KRITIS) auf. Mit 82 Angriffen auf den Energiesektor nimmt dieser bei den Meldungszahlen des BSI den zweiten Platz unter den KRITIS-Sektoren ein. Zu den zehn gravierendsten Sicherheitsproblemen der Geräte im Bereich der Industrial Control System (ICS) zählen laut dem IT-Grundschutzkompendium des BSI unter anderem eine **unsichere Konfiguration**, eine **unzureichende Dokumentation**, eine Manipulation bzw. Sabotage sowie eine **manipulierte Firmware** [Sic18, S. 640]. Darüber hinaus listet der Lagebericht zur IT-Sicherheit in Deutschland des BSI **„sicherheitstechnische Fehlkonfigurationen" (Security-Misconfigurations) als derzeit häufigste Ursache** unter den gemeldeten Schwachstellen auf [Bun23, S. 36]. Neben diesen Zahlen des BSI findet sich in der wissenschaftlichen Literatur eine Reihe von Angriffen auf die Stromversorgung, welche über die IKT erfolgen. Es folgt eine Auswahl relevanter Angriffe:

- Beispielsweise können Strompreismanipulationen durch Angriffe über die IKT erfolgen. Im von Shekari et al. untersuchten Szenario wurden Geräte, die zusammen eine hohe Last erzeugen können, zu einem sogenannten „High-Wattage"-Botnetz zusammengeschaltet [She+21]. Die darin befindlichen Geräte wurden zuvor manipuliert und arbeiten nun als Teil eines Botnetzes, welches die Anlagen ebenfalls steuert. Durch diese feindliche Übernahme ist es möglich, Lasten zu manipulieren und diese für die Erlangung von Profiten am Strommarkt zu nutzen, indem diese eine unerwartet hohe Nachfrage generieren [She+21].

- Die Autoren Qias et al. zeigen in einer Simulationsumgebung ausführlich die Manipulation von Telegrammen nach IEC 60870-5-104, die über TCP/IP verschickt werden [Sai+18].

- Die Übernahme von bestimmten Sensoren im physikalischen Stromnetz kann ebenfalls zu Manipulationen an Strompreismärkten (ex-post real-time-market) führen, um damit Gewinne zu erzeugen. Dies geschieht durch eine False Data

Injection Attack (FDIA), die so ausgestaltet ist, dass die State-Estimation[1] diese nicht erkennt [XMS11].

- Ein weiterer FDIA-Angriff wird in [Wan+18] beschrieben. Dort wird mittels Q-Learning (ein Verfahren aus dem Bereich des maschinellen Lernens) eine automatisierte FDIA durchgeführt und in einem IEEE-39-Bussystem mittels Co-Simulation evaluiert.

- Weitere FDIA-Angriffe und deren Auswirkungen auf das Stromnetz werden in [Wan+14; Jha+19] beschrieben.

- Angriffe, die tatsächlich die reale Stromversorgung getroffen haben, konnten in der Ukraine mehrfach beobachtet werden. Im Jahr 2015 wurde dort eine Malware (dt. Schadsoftware) namens Blackenergy 3 entdeckt. Diese wurde eingesetzt, um manipulierte Daten an die SCADA-Systeme eines Energieversorgers auszuliefern. Es resultierte ein 6-stündiger Blackout im Stromnetz, der durch eine manuelle Steuerung aufgehoben werden konnte. Der Schaden durch die Malware war so enorm, dass der Netzbereich teilweise länger als ein Jahr nicht automatisiert gesteuert werden konnte [Dra17].

- Eine Weiterentwicklung der zuvor genannten Malware konnte ebenfalls identifiziert werden und wird mit weiteren Angriffen auf die Stromversorgung in der Ukraine in Verbindung gebracht. Diese trägt den Namen Crashoverwrite und wird ebenfalls dafür genutzt, manipulierte Firmware über legitime Updatemechanismen auszuliefern. Die Software enthält eine Vielzahl konfigurierbarer Module, kann unterschiedliche Kommunikationsprotokolle anbieten (OPC, IEC 61850, IEC 60870-5-101, IEC 60870-5-104), gibt sich flexibel und wird deshalb in einer Kategorie mit Stuxnet eingeordnet [Dra17].

FDIA-Angriffe zielen in der Regel darauf ab, die auf Netzzustandsdaten basierende Zustandsberechnung (engl. State-Estimation) zu täuschen und somit eine falsche Schlussfolgerung über den aktuellen Ist-Zustand im Stromnetz zu bewirken. Aus der Perspektive der IT-Sicherheit manifestiert sich das Problem bereits vor der Manipulation. Die potenzielle Schwachstelle liegt entweder in der unzureichenden Absicherung der Kommunikationsprotokolle, welche durch einen sogenannten Man-in-the-Middle (MITM)-Angriff kompromittiert werden können, oder in der

[1] Die State-Estimation (deutsch: Zustandsabschätzung) ist ein Prozess, dessen Ziel die Berechnung und Darstellung des aktuellen Zustandes des Netzes ist. Zu diesem Zweck werden beobachtete und verfügbare Daten in mathematischen Modellen verarbeitet. Die State-Estimation spielt insbesondere im Stromnetz eine bedeutende Rolle, da auf Basis der Ergebnisse entscheidende Maßnahmen abgeleitet werden können [Mon00].

Möglichkeit eines unberechtigten Zugriffs auf ein IED und der daraus resultierenden Manipulation von Informationen auf dem IED. Die vorgestellten FDIA-Angriffe basieren auf der Voraussetzung, dass entweder das Kommunikationsprotokoll oder das IED selbst unzureichend geschützt ist, wodurch es Dritten möglich ist, die Informationen auf dem Gerät leicht zu manipulieren.

Definition 1: In dieser Arbeit wird der Begriff *Sicherheit* als Synonym für *Informationssicherheit* und *IT-Sicherheit* verwendet. Beide Begriffe sind unterschiedlich definiert und haben verschiedene Schwerpunkte [Eck18] [Poh22]. Informationssicherheit zielt darauf ab, Informationen gegen Unbefugte zu schützen, und verwendet dazu die drei Eigenschaften *Vertraulichkeit*, *Integrität* und *Verfügbarkeit*. IT-Sicherheit ist ein Teil der Informationssicherheit und umfasst die technischen Maßnahmen zur Sicherstellung der Informationssicherheit [Poh22]. Im Kontext dieser Arbeit bezieht sich die Informationssicherheit ausschließlich auf digitale Informationen.

Aktuelle Strategien und Maßnahmen der Informationssicherheit

Ein Ansatz, der sich mit der allgemeinen und systematischen Bewältigung dieser Problematiken befasst, ist die Implementierung von Sicherheitsmaßnahmen. Die konsequente Umsetzung von Sicherheitsmaßnahmen erfordert jedoch einen ganzheitlichen, komplexen und fortlaufenden Prozess, der unter anderem technische Sicherheitsmaßnahmen sowie deren Konfigurationen definiert und umsetzt. Aufgrund der Komplexität durch eine Vielzahl von unterschiedlichen Komponenten und Systemen, die über IKT-Netzwerke miteinander kommunizieren, bedarf es eines strukturierten Managementprozesses für die zielführende Umsetzung technischer IT-Sicherheitsmaßnahmen.

Die internationale Normenreihe International Standards Organisation (ISO) 27001 beschreibt ein solches Managementsystem für Informationssicherheit (ISMS) [ISO17]. Die Norm zeigt einen Managementprozess auf, mit dem Ziel, Informationssicherheit zu etablieren, umzusetzen, zu betreiben und zu verbessern [Ker+16]. Um die Relevanz dieser Norm für die Informationssicherheit zu unterstreichen, ist ihre Anwendung in Deutschland für alle Betreiber kritischer Infrastrukturen gesetzlich vorgeschrieben (siehe § 11 Abs. 1b deutsches Energiewirtschaftsgesetz).

Zusammenfassend kann IT-Sicherheit als fortlaufender Prozess betrachtet werden, welcher Sicherheitsmaßnahmen definiert und daraus Anforderungen an technische Umsetzungen ableitet. Die Umsetzung der Anforderungen erfordert konkrete Sicherheitskonfigurationen, die in einem Gerät realisiert werden. Wie in [KL15,

p. 359] dargelegt wird, befindet sich ein großer Teil solcher kritischen Konfigurationsinformationen auf den Geräten selbst, auf denen proprietäre oder geschlossene Betriebssysteme arbeiten, was die Abfrage dieser Konfigurationsinformationen von solchen Geräten erschwert. Gleichzeitig erteilt die ISO 27001 den Auftrag, Geräte und Systeme zu überwachen, um die Einhaltung der Sicherheitsmaßnahmen kontinuierlich zu gewährleisten und Abweichungen unmittelbar zu identifizieren [Ker+16, p. 65]. Problematisch ist, dass bislang keine technischen Möglichkeiten verfügbar sind, die eine einheitliche Überwachung der Sicherheitskonfigurationen auf den Geräten und Systemen im Bereich der Operational Technology (OT) und SCADA ermöglichen würden.

In der Gesamtschau betrachtet besteht die Problematik darin, dass zwar Anforderungen an die IT-Sicherheit gestellt werden, die daraus resultierenden Konfigurationen auf den Geräten allerdings nicht ausreichend überwacht werden. Sicherheitstechnische Fehlkonfigurationen, ob bewusst oder unbewusst, gelten laut dem IT-Grundschutzkompendium des BSI als Top Ten der Gefährdungen der IT-Sicherheit in industriellen Systemen [Sic18, S. 640].

Da es sich bei der Umsetzung von Sicherheitskonfigurationen um technische Anforderungen handelt, sollten diese nach Möglichkeit auch mit technischen Mitteln überwacht werden können, sofern sie verfügbar sind. Ebendies ist für die Überwachung von Sicherheitskonfigurationen nicht der Fall.

Anwendungsfälle von Sicherheitsautomation

Das Potenzial der Möglichkeit, Sicherheitskonfigurationen direkt auf den Geräten abzufragen, ist groß und kann einen entscheidenden Beitrag zur Informationssicherheit im Smart Grid leisten. Um dies zu veranschaulichen, werden einige Anwendungsszenarien beschrieben:

1. **Automatisiertes Audit:** Der erste Anwendungsfall betrifft die ISO 27001. Die Einhaltung der ISMS-Prozesse und der erstellten Anforderungen wird in der Regel durch (externe) Auditoren überprüft und bewertet. Im Rahmen einer Auditierung ist es in der Regel nicht möglich, jedes IKT- und Operational Technology (OT)-System einer individuellen und detaillierten Inspektion zu unterziehen. Stattdessen erfolgt in der Praxis die Auswahl über Stichproben. Eine automatisierte Überwachung der Sicherheitskonfigurationen könnte diese Lücke schließen und somit die Aussagekraft einer Auditierung wesentlich verbessern.

2. **Sicherheitsmonitoring:** Der zweite Anwendungsfall umfasst ein Sicherheitsmonitoring. Dieses Monitoring ruft in regelmäßigen Abständen die Sicherheitskonfigurationen von den IEDs ab und vergleicht diese mit den Soll-Werten des ISMS. Im Falle einer Abweichung erfolgt eine automatische Alarmierung an das IT-Sicherheitsteam. Durch die kontinuierliche Überwachung der Sicherheitseinstellungen können bewusste oder unbewusste Fehlkonfigurationen direkt erkannt und gemeldet werden.

3. **Datenaustausch zwischen Stakeholdern im Energienetz:** Ein weiterer Anwendungsfall ist die Weitergabe von Sicherheitsinformationen an Dritte, um diese Informationen für die Bildung von (gegenseitigem) Vertrauen zu nutzen. Dieser Anwendungsfall betrachtet das Energienetz im größeren Kontext, sodass beispielsweise ein Übertragungsnetzbetreiber Zugriff auf die Sicherheitskonfigurationen eines Windparks erhält, der sich in seiner Regelzone befindet, um die Vertrauenswürdigkeit bzw. das Sicherheitslevel zu ermitteln. Der Austausch solcher Sicherheitskonfigurationen mit anderen Stakeholdern kann weitere Vorteile bringen. Beispielsweise können diese Informationen in Form von automatisierten Compliance-Nachweisen am Strommarkt genutzt werden, um gegenüber anderen Marktteilnehmern eine hohe Vertrauenswürdigkeit auszudrücken oder durch höhere Sicherheitsstandards einen Wettbewerbsvorteil zu erlangen.

4. **Im Bereich des Energy-IoT** erfolgt zukünftig eine bedarfsorientierte Zusammenschaltung kleinerer Erzeuger, um regional oder in lokalen Nachbarschaften Netzdienstleistungen zu erbringen [WFN22]. Das Zu- und Abschalten einer Vielzahl von Erzeugern und Lasten (z. B. Elektroautos) wird zukünftig nicht mehr von Menschen in Controlcenter übernommen, sondern von autonomen Agenten [Lin24, p. 127]. Die Forschung von [RUS14] zeigt ein Konzept autonomer Agenten, welche zur gemeinsamen und autonomen Auftragsabwicklung ein gegenseitiges Vertrauensverhältnis aufbauen. Im Prozess der Vertrauensbildung wird die Sicherheit der Agenten berücksichtigt.

5. **In anderen Domänen:** Die zunehmende Vernetzung und resultierende vergrößerte Angriffsfläche betrifft nicht nur das Stromnetz der Zukunft, sondern alle Lebensbereiche auch im privaten Umfeld. Unter dem Begriff Internet of Things (IoT) sind Aktuatoren und Sensoren allgegenwärtig. Die Bandbreite reicht von Smartwatches, Fahrradtachos und Türschlössern, die mit der Cloud verbunden sind, um so von überall auf der Welt steuerbar zu sein, bis hin zu Beleuchtung und Haushaltsgeräten wie Waschmaschinen, die ebenfalls über das Internet kommunizieren können. Hier ergibt sich dieselbe Lücke: Informationen über

Sicherheitskonfigurationen können nicht abgefragt werden, um sie für eine Bewertung der Informationssicherheit im Smart Home zu nutzen.

Möglichkeiten von automatisierter Überwachung der Sicherheitskonfigurationen

Die Notwendigkeit der Überwachung der Sicherheitseinstellungen auf IED ergibt sich bereits aus den Anforderungen der ISO 27001 und stellt grundsätzlich eine logische Konsequenz dar. Die Möglichkeiten und Potenziale von automatisierter Überwachung von Sicherheitskonfigurationen sind mannigfaltig: Zum einen ist es aus der Sicht eines Netzbetreibers möglich, seine eigenen IED abzufragen und die Informationen für die weitere Verarbeitung zur Verfügung zu stellen. Eine Integration solcher Informationen in die State-Estimation ist sinnvoll, um das aktuelle Vertrauensniveau besser einschätzen zu können. Automatisierte Soll-Ist-Vergleiche der Sicherheitskonfigurationen sind ein nahezu offensichtlicher Anwendungsfall, welcher es ermöglicht, Fehlkonfigurationen und manipulierte Sicherheitskonfigurationen direkt zu erkennen.

Vor dem Hintergrund der zunehmenden Anzahl an Akteuren im Energienetz, deren IED nicht unter der Kontrolle der Netzbetreiber oder Marktakteure stehen, bedarf es neuer Möglichkeiten, die Sicherheitseinstellungen dieser Geräte abzufragen. Dies betrifft auch private Haushalte, welche kein Sicherheitsmanagementsystem für ihre Lasten und Erzeuger betreiben können. Aber auch größere Anbieter von Photovoltaik (PV) oder Windparks sollten befähigt sein, ihre Sicherheitsinformationen der IED mit Netzbetreibern und anderen Akteuren zu teilen. Vorbilder für solche Möglichkeiten finden sich bereits in der Automobilindustrie. Ergebnisse von Compliance und Sicherheitsberichten werden dort durch den Standard Trusted Information Security Assessment Exchange (TISAX) ausgetauscht. TISAX ist ein unternehmensübergreifendes Prüf- und Austauschverfahren für Informationssicherheit in der Automobilindustrie. Die Teilnehmenden tauschen über ein Online-Portal die Informationen zum Status der Informationssicherheit aus [Tec23].

Mit Blick auf eine Realisierung von einem automatisierten Sicherheitskonfigurationsmonitoring im Smart Grid kommen weitere Fragen auf: beispielsweise die Frage nach der Integritätssicherheit der IED. Kann man den Konfigurationsinformationen überhaupt vertrauen? Was ist, wenn ein IED manipuliert wurde und die abgefragten Sicherheitskonfigurationen nicht denen auf dem Gerät entsprechen? Mit welchen Mitteln lässt sich dies erkennen, um dadurch das IT-Sicherheitsniveau zu erhöhen?

Neben der Frage nach Integrität der IED stellt sich auch die Frage, wie sich solche Informationen in die Kommunikationsarchitektur des Energienetzes integrieren lassen. Ergibt es Sinn, dafür zusätzliche oder neue Informationskanäle innerhalb der IKT-Architektur im Stromnetz zu schaffen, oder gibt es Möglichkeiten, diese Informationen auf bestehenden Kommunikationskanälen zu transportieren? Wenn ein Datenaustausch stattfinden kann, welche Sicherheitsstandards eignen sich als Referenz?

Aus diesen Gründen befasst sich dieses Promotionsvorhaben mit der folgenden Forschungsfrage. Darin enthalten sind Anforderungen, die den sicheren Betrieb von IKT gewährleisten beziehungsweise für die jeweiligen Betreiber davon abzuleiten sind.

1.2 Forschungsfrage

Aus der beschriebenen Motivation und der Diskussion mündet die Forschungsfrage, die in dieser Dissertation beantwortet werden soll, um die IT-Sicherheitskonfigurationen auf IEDs und insbesondere deren Überprüfbarkeit zu ermöglichen.

Forschungsfrage *Wie kann eine automatisierte Bewertung von technischen Sicherheitskonfigurationen für SCADA-Komponenten im Stromnetz ermöglicht werden?*

1.2.1 Forschungsziele

Die Beantwortung der Forschungsfrage erfolgt durch die Definition von Forschungszielen. Die Forschungsziele dienen insbesondere der Strukturierung und der Generierung von einzelnen Lösungsansätzen in Form von Artefakten sowie der Ableitung nichtfunktionaler Anforderungen.

Das erste Forschungsziel besteht in der Identifikation relevanter IT-Sicherheitsanforderungen für IED in den SCADA der Energietechnik und der Untersuchung auf deren Automatisierbarkeit. Dies ist zum einen notwendig, um sicherzustellen, dass die Sicherheitsanforderungen auf die IEDs anwendbar sind. Zum anderen ist die Möglichkeit der Automatisierbarkeit dieser die Voraussetzung für die weiteren Schritte der vorliegenden Arbeit. Deshalb werden von den ermittelten IT-Sicherheitsanforderungen Konfigurationsmöglichkeiten abgeleitet, um ihre technische Umsetzung so zu beschreiben, dass sie automatisiert verarbeitet werden können.

Eine Bewertung jeder IT-Sicherheitsanforderung hinsichtlich der Möglichkeit, diese automatisiert zu erfassen bzw. abzufragen, ist dafür unabdingbar.

Um die zuvor abgeleiteten Konfigurationsinformationen innerhalb bestehender Informations- und Datenmodelle des Stromnetzes übertragen zu können, ist eine Identifikation geeigneter Informations- und Datenmodelle erforderlich. Dies stellt das zweite Forschungsziel dar.

Das dritte Forschungsziel besteht in der Integration von Attestierungsmöglichkeiten als sogenannte Remote Attestation in das zuvor identifizierte Informationsmodell und Kommunikationsprotokoll. Die Sicherstellung der Plattformintegrität des IED ist Gegenstand dieses Forschungsziels, um dessen Integrität aus der Ferne verifizieren zu können.

Das vierte Forschungsziel stellt die Instanziierung der vorangehend dargelegten Forschungsziele durch die Implementierung derselben in einen Demonstrator dar, welcher der Evaluation des gesamten Systems dient.

Zusammenfassend sind die Forschungsziele wie folgt aufgeteilt:

1. Identifikation und Analyse von IT-Sicherheitsanforderungen, welche für IED im elektrischen Energienetz anwendbar sind.
2. Entwicklung eines Daten- und Informationsmodells für die identifizierten IT-Sicherheitsanforderungen.
3. Integration von Remote-Attestation-Verfahren in die IED als Vertrauensbasis zur Verifizierung der Integrität.
4. Entwicklung eines Demonstrators zur Umsetzung der Forschungsziele.

Beitrag zur Trust-Pyramide

Die Trust-Pyramide stellt ein Konzept dar, welches seinen Ursprung im Forschungsfeld des Organic Computing findet und dessen sieben Facetten des Vertrauens nutzt. [Ste+10]. Durch eine systematische Weiterentwicklung wurde Vertrauen beschrieben als ëin subjektives, kontextabhängiges und multivariates Gefühl in Bezug auf die funktionale Korrektheit, Sicherheit, Zuverlässigkeit, Glaubwürdigkeit und Benutzerfreundlichkeit einer Einrichtung"([Bra+20]. Der Ansatz findet Anwendung bei der ganzheitlichen Ermittlung der Vertrauenswürdigkeit komplexer Systeme unter Berücksichtigung verschiedener Vertrauensfacetten [Bra+20], [BNL24]. Die weitere

Adaption im Bereich von cyberphysischen Systemen im Kontext des technischen Energiemanagements ist in [Bro+24] zusammengefasst. Die nachfolgende Abbildung 1.1 zeigt den Aufbau der Trust-Pyramide für vertrauenswürdige Energiesysteme und wird im folgenden Absatz beschrieben.

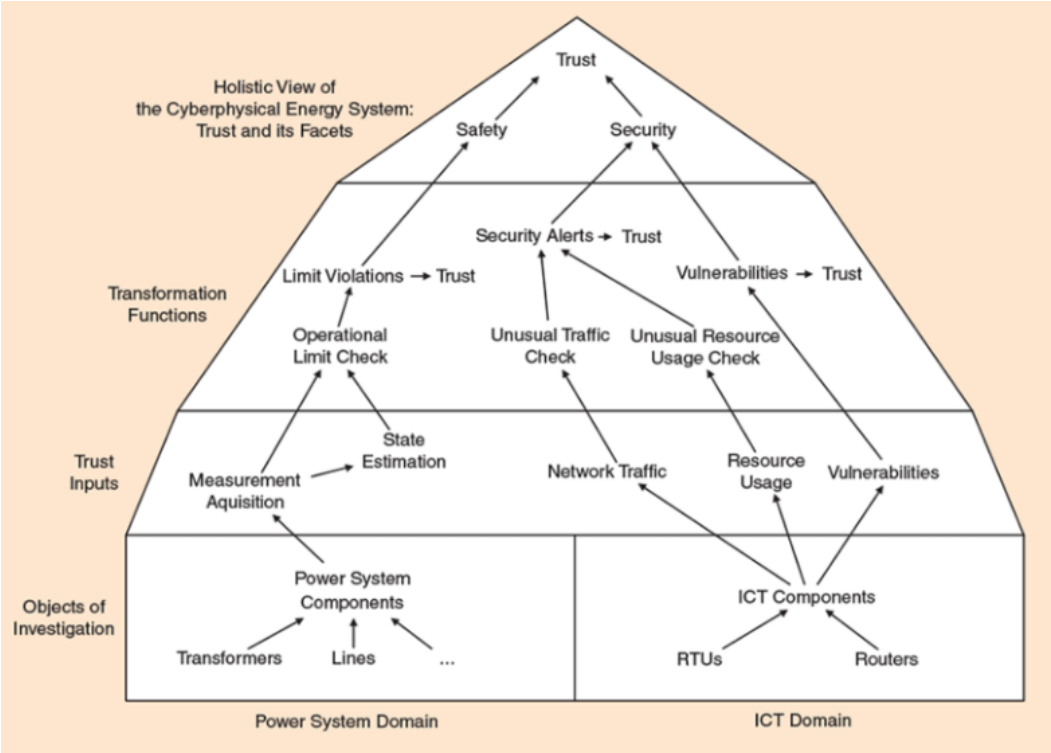

Abbildung 1.1.: Visualisierung von Vertrauen und seinen Facetten in cyberphysischen Energiesystemen, Quelle: [Bro+24]

Die Abbildung 1.1 veranschaulicht den Aufbau der Trust-Pyramide für vertrauenswürdige Energiesysteme. Die Daten werden von unten nach oben verarbeitet, wobei sich unten die Objekte (Objects of Investigation) befinden, über die ein Vertrauenswert bestimmt werden soll. Aus der Vielzahl der am Fuße der Pyramide angeordneten Geräte und Systeme soll durch Erfassen unterschiedlicher Informationen an der Spitze der Pyramide ein Vertrauenswert entstehen. Dazu werden Daten auf unterschiedlichen Ebenen der Pyramide aggregiert und durch verschiedene Metriken Werte berechnet, die jeweils einen Beitrag zur Bestimmung der Vertrauenswürdigkeit leisten. Als Beispiel kann die Arbeit von Brand et al. angeführt werden, bei der die Qualität der Prozessdaten verwendet wird, um mittels unterschiedlicher Metriken einen Vertrauenswert zu bestimmen, der für die Zustandsbestimmung des Energienetzes verwendet werden kann [BEL23].

Die vorliegende Arbeit unterstützt das Forschungsthema der Trust-Pyramide, indem zwei Beiträge hinzugefügt werden: 1. Die Absicherung der Plattform und der damit

verbundenen Fernattestierung, 2. Die Abfragbarkeit und Bereitstellung von SKI als Eingangsinformationen der Trust-Pyramide. Damit wird das Ziel adressiert, die in dieser Arbeit entwickelten Artefakte in die Trust-Pyramide integrieren zu können.

1.2.2 Anforderungen an die Lösung

Die Erreichung der Forschungsziele erfolgt unter der Prämisse, dass die resultierenden Lösungen eine praktische Relevanz aufweisen und in die Kommunikations- und Sicherheitsarchitektur des Smart Grid integrierbar sind. Die genannten Bedingungen werden als nichtfunktionale Anforderungen definiert.

Die erste Anforderung zielt darauf ab, sicherzustellen, dass die für die Stromnetzdomäne geltenden und anwendbaren IT-Sicherheitsnormen und -standards berücksichtigt werden. Auf diese Weise kann gewährleistet werden, dass die gewählten Sicherheitsanforderungen relevant sind. In diesem Kontext ist es ebenfalls erforderlich, IT-Sicherheitsstandards und Normen zu berücksichtigen, die für den Bereich von SCADA-Systemen anwendbar sind. Dies ist dadurch begründet, dass es sich bei den Steuerungsanlagen im Stromnetz um eine Spezialisierung der Automatisierungstechnik handelt.

Unter der Berücksichtigung der gravierenden Konsequenzen von Datenmanipulation für die Stabilität und Sicherheit kommt der Integritätsüberwachung der Softwarekomponenten eine besondere Bedeutung zu. Dieser Aspekt muss folglich in der zu entwickelnden Lösung adäquat berücksichtigt werden. Die Überwachung der IED-Plattform erweist sich als essenziell, um Manipulationen von Firmware, Betriebssystem und Anwendungssoftware aus der Ferne identifizieren zu können.

Eine weitere Anforderung an die Lösung ist, dass sie eine Möglichkeit zum Einsammeln der Sicherheitskonfigurationen beschreibt. Diese nichtfunktionale Anforderung soll sicherstellen, dass die Konfigurationseinstellungen der Sicherheitsanforderungen in einem IED verfügbar gemacht werden können. Darüber hinaus ist eine weitere nichtfunktionale Anforderung, dass die Gesamtlösung mit der TC57-Referenzarchitektur kompatibel ist bzw. in diese integriert werden kann.

1.3 Methodik

Die Vorgehensweise zur wissenschaftlichen Beantwortung der zuvor gestellten Forschungsfrage besteht in der Methodik des Design Science Research Process (DSRP)

nach [Pef+20]. Die Methodik des DSRP ist eine Ausprägung der Design-Science, die sich in besonderem Maße für die angewandte Forschung an Informationssystemen eignet. Insbesondere wenn eine Problemlösung gesucht wird, ist die Methodik darauf ausgelegt, einen Prozess zum Erreichen von Lösungsartefakten zu definieren. Der nominale Prozessablauf dieser Methodik ist in Abbildung 1.2 dargestellt und besteht aus sechs Phasen: 1. Problemerkennung und Motivation, 2. Zielsetzung einer Lösung, 3. Design und Entwicklung, 4. Demonstration, 5. Evaluation und 6. Kommunikation.

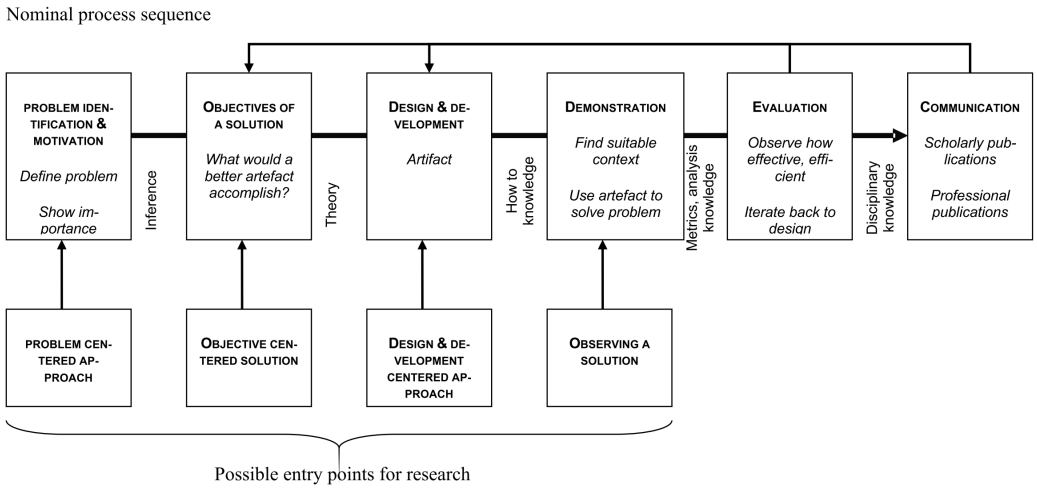

Abbildung 1.2.: Nominaler Prozessablauf des DSRP, Quelle: [Pef+20]

In der Abbildung 1.2 sind die Phasen der DSRP-Methodik als Prozessablauf dargestellt. Die Methodik ermöglicht unterschiedliche Einstiegspunkte. Die vorliegende Arbeit hat mit der Problemidentifikation begonnen und den problemzentrierten Ansatz gewählt. Die darauf folgenden Zielsetzungen wurden ebenfalls bereits vorgestellt. Die DSRP-Methodik erlaubt es, im Prozess zurückzugehen, um beispielsweise das Design der Artefakte zu verbessern (iteratives Vorgehen). Auf einzelne für die Arbeit besonders relevante Phasen wird im Folgenden genauer eingegangen.

1.3.1 Design und Entwicklung

In der Design- und Entwicklungsphase wurden die einzelnen Artefakte und Komponenten konzipiert. Für die vorliegende Arbeit ist vorgesehen, dass diese aufeinander aufbauen.

Das erste Artefakt ist die Entwicklung und Beschreibung eines Informationsmodells für SKI. Dieses Informationsmodell bildet die Grundlage, um IT-Sicherheitsanforderungen

technisch einheitlich darzustellen. Es soll auf den IEDs platziert werden, um eine Abfrage der SKI zu ermöglichen. Um dies zu erreichen, werden zunächst IT-Sicherheitsstandards und -normen analysiert, die die Anforderungen an den Inhalt des Informationsmodells stellen. Die dazugehörige Identifikation und Analyse von IT-Sicherheitsstandards und -normen werden im Kapitel 3 behandelt. Das eigentliche Informations- und Datenmodell für die SKI ist im Kapitel 4 beschrieben.

Das zweite Artefakt ist die Entwicklung eines Konzepts zur Integration von Remote Attestation in IEDs und in die Kommunikationsprotokolle des Stromnetzes. Dieses Artefakt stellt die Voraussetzung dar, um die Plattformintegrität von IEDs aus der Ferne abfragen zu können und damit Vertrauen in das IED aufzubauen. Um dies zu erreichen, werden Trusted-Computing-Technologien und -Konzepte in die (Referenz-)Kommunikationsinfrastruktur des Stromnetzes integriert und implementiert. Das Artefakt ist im Kapitel 4 beschrieben.

Das dritte Artefakt beschreibt die Implementierung und Integration der ersten beiden Artefakte in einem technischen Demonstrator. Es umfasst einerseits das Datenmodell für die SKI und andererseits das Datenmodell für die Remote Attestation. Das Artefakt ist im Kapitel 5 beschrieben.

1.3.2 Demonstration und Evaluation

Die Abschnitte der Demonstration und Evaluation dienen dazu, die geschaffenen Artefakte zu demonstrieren. Das primäre Ziel des Demonstrators ist es zu zeigen, dass die vorherigen Artefakte unter genannten Bedingungen und Einschränkungen SKI übertragen können und die Funktionalitäten der Absicherung der IED-Plattform zeigen können. Die Demonstration soll darlegen, wie ein automatisiertes Security-Assessment von SKI für die Primärtechnik im Stromnetz in bestehende Kommunikationsarchitekturen integriert werden kann. Gleiches gilt für die Funktionen der Remote Attestation. Darüber hinaus sollen in der Evaluation praktische Erkenntnisse gewonnen werden, die für zukünftige Entwicklungen oder Verbesserungen relevant sind.

1.3.3 Dissemination und Kommunikation

Einzelne Artefakte sowie das Gesamtvorhaben wurden bereits in unterschiedlichen Prozessphasen einem interessierten Fachpublikum präsentiert. Die Relevanz des Themas für die Energietechnik wurde durch eine erfolgreiche Publikation auf der

Institute of Electrical and Electronics Engineers (IEEE) Power and Energy Society (PES) PowerTech Konferenz 2023 untermauert. Im Rahmen der Konferenz wurde die Integration von Remote Attestation in die Norm IEC 61850 präsentiert, anschließend wurde sie in der IEEE-Xplore-Bibliothek publiziert [Fra+23]. Des Weiteren wurde das Gesamtvorhaben mit dem Schwerpunkt der Problemstellung und der sicheren Lösungsansätze auf der Fachtagung *Sicherheit – Schutz und Zuverlässigkeit* der Gesellschaft für Informatik e. V. präsentiert und diskutiert sowie als Publikation im Tagungsband der GI SICHERHEIT 2022 abgedruckt [Fra22]. Diese Konferenz richtet sich an ExpertInnen aus dem (deutschsprachigen) IT-Sicherheitsumfeld. Neben den wissenschaftlichen Tagungen und Konferenzen wurden die Fortschritte und Ergebnisse dieser Arbeit in internen curricularen Seminaren am Institut OFFIS der Universität Oldenburg diskutiert. Die hier vorliegende Dissertation stellt die abschließende und zugleich umfassendste Publikation dar.

1.4 Struktur der Arbeit

- Die vorliegende Arbeit gliedert sich in sieben Kapitel. Das erste Kapitel hat die Arbeit bereits motiviert, die Forschungsfragen vorgestellt und die Forschungsziele beschrieben.

- Das zweite Kapitel stellt die Grundlagen der beiden Bereiche Informationssicherheit und Smart Grid vor. Der Bereich Informationssicherheit deckt den Schwerpunkt Trusted Computing ab. Die notwendigen Grundlagen des Smart Grids werden ebenfalls präsentiert, mit dem Fokus auf der bestehenden Kommunikations- und Sicherheitsarchitektur des Energienetzes.

- Im dritten Kapitel werden die unterschiedlichen Standards zu IT-Sicherheit analysiert, die Anforderungen daraus aggregiert und in einer umfassenden Analyse vorgestellt. Die identifizierten Anforderungen stellen das erste Forschungsartefakt dar.

- Das vierte Kapitel stellt das zweite Forschungsartefakt dar. Es beinhaltet das entwickelte und primäre Informationsmodell sowie die Abbildung der Sicherheitskonfigurationen.

- Die Vorstellung des Demonstrators erfolgt im fünften Kapitel und zeigt die Umsetzung der Artefakte sowie deren Integration in die bestehende Kommunikationsarchitektur des Energienetzes.

- Es folgt die Evaluation in Kapitel 6 unter Betrachtung aller Anforderungen. Hier wird auch eine Bewertung vorgenommen.
- Die Arbeit schließt mit der Schlussbetrachtung und einem Fazit im siebten Kapitel.

2 Grundlagen

In diesem Kapitel werden die Grundlagen für die vorliegende Arbeit beschrieben. Diese bestehen aus zwei verschiedenen Säulen. Die erste Säule ist der Themenbereich des intelligenten Stromnetzes. Die zweite Säule bilden die Eigenschaften der Informationssicherheit sowie das notwendige Vorwissen zum Thema Trusted Computing.

2.1 Intelligentes Stromnetz

Das allgemein als Stromnetz bezeichnete Netz dient der Verteilung und dem Transport elektrischer Energie vom Erzeuger zum Verbraucher. Damit ein Stromnetz seine Funktion erfüllen kann, müssen Erzeugung und Verbrauch[1] zu jedem Zeitpunkt identisch sein. Folglich muss zu jedem Zeitpunkt exakt so viel Strom eingespeist werden, wie entnommen und verbraucht wird. Da im europäischen Stromnetzverbund überwiegend Wechselspannung übertragen wird, ist zudem die Einhaltung einer Netzfrequenz von 50 Hertz erforderlich.

Das Stromnetz ist in seiner Struktur und seinem Aufbau historisch gewachsen und in verschiedene Netzebenen mit unterschiedlichen Aufgaben unterteilt. Die wichtigsten Gründe für diese Aufteilung sind Ausfallsicherheit, wirtschaftliche Aspekte und nicht zuletzt der Ausbau der regenerativen und dezentralen Energieerzeugung. Die Weiterentwicklung des Stromnetzes hin zum Smart Grid (dt. intelligentes Stromnetz) ist vor allem durch die zunehmende Digitalisierung des Netzbetriebs gekennzeichnet. Dies ist aus verschiedenen Gründen erforderlich. Die Abbildung 2.1 zeigt den elektrischen Energiefluss sowie die Kommunikationsverbindungen im Smart Grid.

2.1.1 Kommunikationsarchitektur / TC57

Die vorliegende Arbeit berücksichtigt vor allem die bestehenden Kommunikationsarchitekturen im Stromnetz. Dabei wird ein besonderes Augenmerk auf den komplexen

[1] Strom bzw. elektrische Energie wird physikalisch betrachtet nicht verbraucht, die Details werden in dieser Arbeit nicht weiter vertieft.

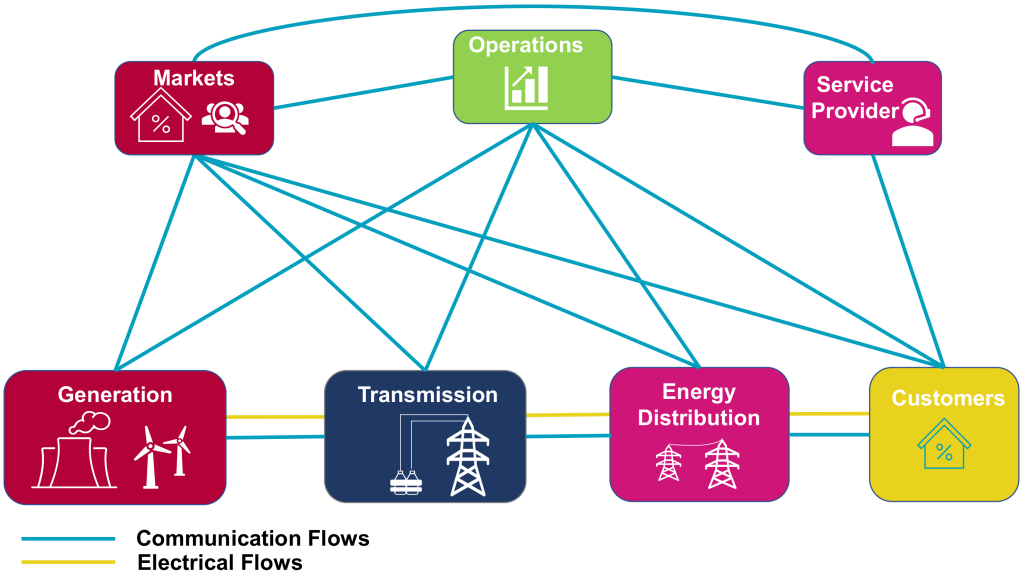

Abbildung 2.1.: Kommunikationsverbindungen innerhalb des Smart Grid, Quelle: [Dem+21]

Informationsaustausch gelegt, um eine möglichst nahtlose Integration in die bereits bestehende Kommunikationsarchitektur zu gewährleisten.

Für die Vielzahl an unterschiedlichen Systemen, Bereichen und Anwendungen wurde von der International Electrotechnical Commission (IEC) Working Group (WG) 15 Technical Committee (TC) 57 Power System Architecture Model (TC) eine Referenzarchitektur für Kommunikationsstandards zum Austausch von Stromnetzinformationen erstellt und in der IEC 62357-1 beschrieben [Cle14]. Die Kommunikationsverbindungen und -protokolle zwischen den Anwendungen, Domänen und Systemen sind in der Abbildung 2.2 dargestellt. Das Controlcenter (dt. Leitstelle) befindet sich in der Mitte der Abbildung und ist rot hinterlegt. Auf einem zentralen Communication-Bus werden alle relevanten Stromnetzinformationen zusammengeführt und stehen dort zur weiteren Verwendung in anderen Bereichen und Anwendungen zur Verfügung.

Die Kommunikationsverbindungen zum Strommarkt und Back-Office (Innendienst) sind in grauer Farbe hinterlegt. Mit Blau markiert sind die dezentralen Energiequellen wie Windkrafträder und Photovoltaikanlagen (DER[2] Generator), aber auch Elektroautos (Electric Vehicle) sowie Speichersysteme der dezentralen Energiequellen (DER Storage). Des Weiteren ist der Bereich der Gas- und Wasserkraftturbinen (Hydroelectric / Gas Turbine Power Plants) in Blau dargestellt.

[2]DER – distributed energy resources, dt. dezentrale Energiequellen.

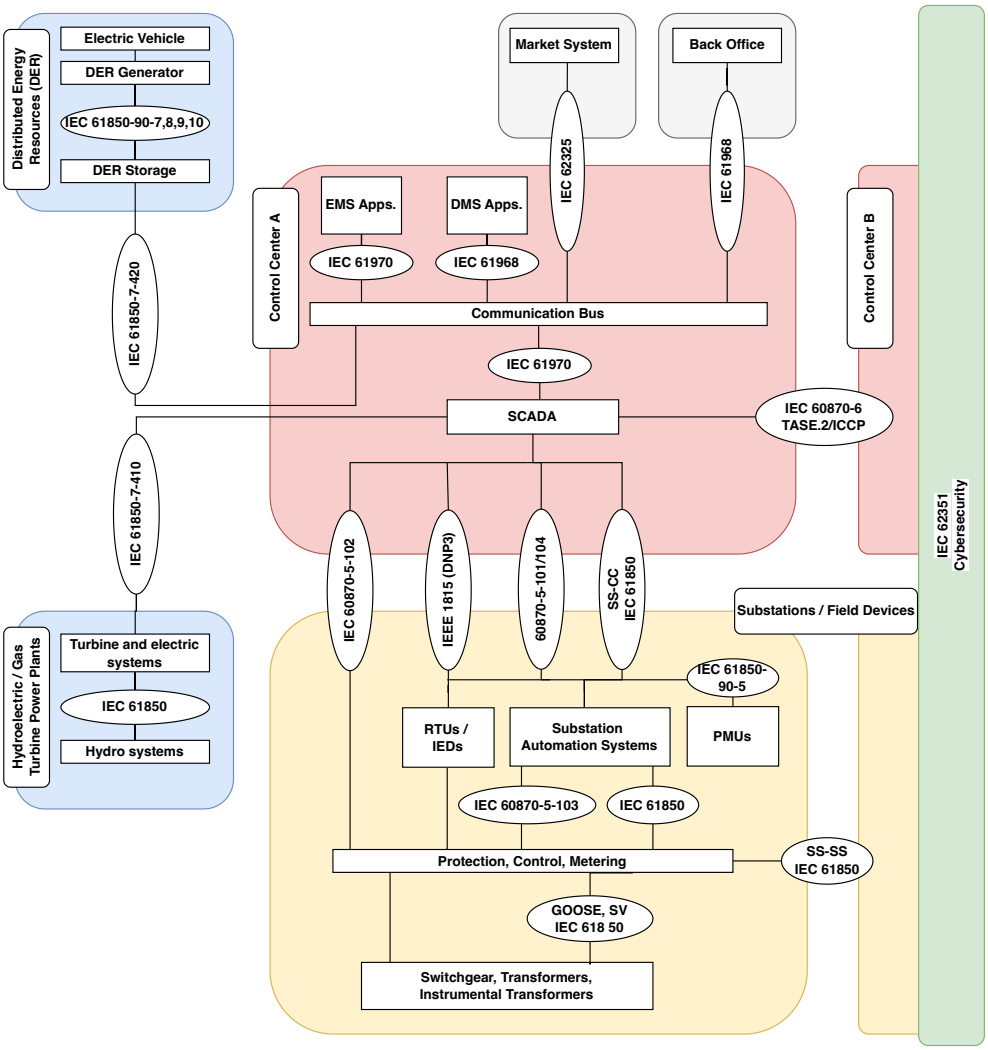

Abbildung 2.2.: TC57-Architektur der Kommunikationsstandards [Cle14, S. 32]

In der vorliegenden Arbeit wird ein besonderes Augenmerk auf den gelb markierten Bereich gelegt. Dieser stellt die Unterstationen und Feldgeräte (Substation / Field Devices) dar. Dort finden sich Remote Terminal Units (RTUs) und Automatisierungssysteme (Substation Automation Systems), welche über eine Vielzahl an möglichen Kommunikationsprotokollen nach „oben“ kommunizieren und dort als Teil der SCADA-Infrastruktur ihre Stromnetzdaten in das Controlcenter transportieren. Die RTUs fungieren als Kommunikationsschnittstelle zwischen der lokalen Automatisierungstechnik in den Unterstationen auf der einen Seite und dem Controlcenter auf der anderen Seite. Sie kommunizieren auf der horizontalen Ebene mit der Primärtechnik des Stromnetzes und stellen auf der vertikalen Ebene den Zugang für das Controlcenter bereit, beispielsweise um Messdaten zu liefern oder um Konfi-

gurationen umzusetzen. Des Weiteren ist in der Abbildung ersichtlich, dass die RTUs über verschiedene Kommunikationsprotokolle angesprochen werden können.

Die grün markierte Zone verortet die IT-Sicherheit in der Abbildung. Diese verläuft vertikal und parallel zu den Kommunikationsprotokollen und Domänen in der Abbildung. Darin enthalten ist die IEC 62351, welche IT-Sicherheitsmaßnahmen (Cybersecurity) für die Kommunikationsprotokolle des Energiemanagementsystems beschreibt. Die IEC 62351 verläuft parallel, da sie den Anspruch hat, die gesamte Bandbreite der Kommunikationsprotokolle abzudecken und deren spezifische Eigenschaften zu berücksichtigen. Zusammenfassend bietet die TC57-Referenzarchitektur der Kommunikationsstandards eine umfassende Grundlage für die zu verwendenden Normen, Standards sowie Modelle und stellt den Rahmen für die weiteren Entwicklungen und Implementierungen in der vorliegenden Arbeit dar.

Ein in der TC57-Referenzarchitektur in zahlreichen Bereichen vertretener Kommunikationsstandard ist die Norm IEC 61850. Dieser eignet sich sowohl für die Kommunikation in horizontaler als auch in vertikaler Richtung. In der Architektur TC57 Power System Architecture Model ist er daher an vielen Stellen vermerkt, so z. B. in der verteilten Erzeugung, links in der Abbildung. Dies kann damit begründet werden, dass die IEC 61850 vor allem eine Norm zur Automatisierung von Schaltanlagen und der Datenerfassung ist [18]. Sie kann ebenfalls für die Steuerung aus der Ferne verwendet werden [Fal19a, S. 5].

Die Vielzahl an Kommunikationsprotokollen und -modellen sowie eine über Jahrzehnte gewachsene Kommunikationsinfrastruktur mit unterschiedlichen Normen und Standards machte es erforderlich, im Rahmen von Harmonisierungsarbeiten auf Normungsebene Kernstandards zu definieren und festzulegen. Die Zielsetzung besteht in der nahtlosen Integration neuer bzw. zukünftiger Anwendungsfälle und Systeme [Roh+10]. Die IEC 61850 ist im Rahmen dessen als einer der Kernstandards für das intelligente Stromnetz (der Zukunft) hervorgegangen und als solcher festgelegt worden [18; Lef+15].

2.1.2 IEC 61850

Der erste Schritt, um eine Integration von Sicherheitstechnologien in die stromnetzspezifischen Protokolle zu erreichen, besteht in der Auseinandersetzung mit der vorgestellten Referenzarchitektur des IEC TC57 Power System Architecture Model. Wie bereits beschrieben, umfasst die Referenzarchitektur zahlreiche Protokolle, Modelle, Dienste und Anwendungen, die in Stromnetzen weit verbreitet sind. Ein

wesentliches Ziel bestand in der Integration der Remote Attestation in bestehende Kommunikationsprotokolle des Stromnetzes. Dies ist vor dem Hintergrund der ebenfalls bereits angesprochenen nahtlosen Integration für neue Anwendungsfälle zu sehen. Ein weiterer Grund besteht darin, die Akzeptanz neuer Sicherheitstechnologien innerhalb des Stromnetzes zu erhöhen.

Entsprechend dieser Architektur stehen drei Kommunikationsstandards für die Kommunikation mit Unterstationen und RTUs zur Verfügung: die IEC 60870-5, die DNP3 (IEEE 1815) und die IEC 61850. IEC 61850 ist der neueste der drei Standards und soll wie oben angeführt der Kernkommunikationsstandard für intelligente Stromnetze sein [BS20, S. 358]. Zudem kann mittels IEC 61850 ein weitaus breiteres Anwendungsspektrum adressiert werden, da die Kommunikationsnorm auch für Energiespeicher und in der Integration von Elektrofahrzeugen als Distributed Energy Resources (DERs) [SRA13] eingesetzt werden kann. Die IEC 61850 wurde mit dem Ziel entwickelt, eine hohe Flexibilität und Erweiterbarkeit für zukünftige Anwendungen von IEDs im Stromnetz zu ermöglichen [Roh+10][Fal19a]. Daher wurde die Norm IEC 61850 zur Integration der Remote-Attestation-Funktionalitäten ausgewählt.

Der Kern der IEC 61850-Norm besteht in der Definition abstrakter Datenmodelle und abstrakter Klassen sowie in deren Abbildung auf Kommunikationsprotokolle. Die Norm definiert insbesondere eine hierarchische Struktur sowie einen abstrakten Rahmen für die Implementierung wichtiger Funktionen. Typische Geräte- und Datenklassen sind bereits vordefiniert, um ein hohes Maß an Interoperabilität zu erreichen. Darüber hinaus bieten diese Klassen Datenattribute, die ebenfalls abstrakt definiert wurden. Abbildung 2.3 zeigt die hierarchische Beziehung zwischen diesen Klassen vom sogenannten Typ Abstract Communication Service Interface (ACSI), die von der IEC 61850 verwendet werden.

Die oberste Hierarchiestufe wird durch ein physikalisches IED abgebildet, das als Server fungiert. Darüber hinaus existiert mindestens ein logisches Gerät, welches einen logischen Knoten beinhaltet, der wiederum mindestens ein Datenobjekt umfasst. Das hierarchische Modell wird in der vorliegenden Arbeit als Vorlage verwendet, um eigene Datenmodelle davon abzuleiten.

Die Norm IEC 62351 beschreibt die Sicherheit in Energiemanagementsystemen sowie den damit verbundenen Datenaustausch.

- Server: Repräsentiert das nach außen sichtbare Verhalten eines Geräts und ist ein abstraktes Konzept, das eine Reihe von Kommunikationsendpunkten darstellt, die den Zugang zu anderen IEC-61850-Objekten ermöglichen [Int10].

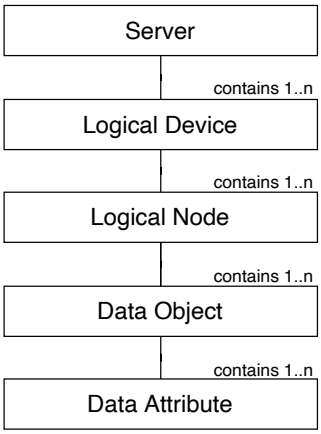

Abbildung 2.3.: Grundlegendes konzeptionelles Klassenmodell des ACSI, Darstellung nach [Int10]

- Logical Device: Ist ein benanntes Objekt, das eine Ansammlung von anderen IEC-61850-Ressourcen oder -Objekten darstellt. Es repräsentiert in erster Linie die Informationen, die von einer Gruppe domänenspezifischer Anwendungsfunktionen erzeugt und verbraucht werden [Fal19b].

- Logical Node: Repräsentiert eine bestimmte Funktionalität, die Informationen bereitstellt, die ausgetauscht werden sollen. Das Kommunikationskonzept der IEC 61850 ermöglicht es logischen Knoten, Informationen mit anderen logischen Knoten auszutauschen. Diese Knoten repräsentieren die Funktionalität zur Steuerung der Ressourcen im logischen Gerät. Ein logischer Knoten enthält die Informationen, die von einer einzelnen domänenspezifischen Anwendungsfunktion erzeugt und konsumiert werden, z. B. einem Überspannungsschutz oder einem Leistungsschalter [Fal19b].

- Data Object: Repräsentiert ein benanntes Unterobjekt eines logischen Knotens, das eine spezifische Semantik und Austauschfähigkeit bietet. Es stellt Mittel zur Definition typisierter Informationen bereit, z. B. die Position eines Schalters sowie Qualitätsinformationen und Zeitstempel, die in logischen Knoten enthalten sind [Int10; Fal19b]. Diese können auch als Nutzdaten angesehen werden.

- Data Attribute: Repräsentiert ein benanntes Unterobjekt eines Datenobjekts, das eine spezifische Semantik und Austauschfähigkeit bietet. Um beispielsweise die Position eines Schalters darzustellen, werden fünf Datenattribute verwendet. Jedes dieser Attribute besitzt eine funktionale Einschränkung, die hauptsächlich Lese-/Schreibeigenschaften definiert [Int10].

2.2 Informationssicherheit

Die Informationssicherheit soll an dieser Stelle mit den grundlegenden Eigenschaften beschrieben werden.

- **Vertraulichkeit:** Stellt sicher, dass nur autorisierte Objekte die Informationen einsehen können.
- **Integrität:** Stellt sicher, dass Informationen korrekt und unverändert bleiben.
- **Verfügbarkeit:** Stellt sicher, dass die Informationen verfügbar sind, wenn sie benötigt werden.
- **Authentizität:** Stellt sicher, dass die Quelle der Informationen verifiziert sind.
- **Verbindlichkeit / Nichtabstreitbarkeit:** Stellt sicher, dass eine Handlung oder Information nicht im Nachhinein geleugnet werden kann.
- **Zuverlässigkeit:** Stellt sicher, dass eine Anwendung / ein System in der erwartbaren Funktionalität korrekt arbeitet.
- **Zurechenbarkeit:** Stellt sicher, dass alle getätigten Aktionen in einem System einem bestimmten Objekt zugeordnet werden können (im Sinne von Protokollierung/Logging).

Um die genannten Ziele zu erreichen, werden digitale Informationen durch Techniken der IT-Sicherheit geschützt. Dabei spielen insbesondere kryptografische Verfahren eine wichtige Rolle, da sie beispielsweise mittels Verschlüsselung die Vertraulichkeit sicherstellen.

2.2.1 Trusted Computing Group

Die Trusted Computing Group (TCG) ist ein Herstellerkonsortium, dessen Ziel die Erstellung offener Industriestandards für Hard- und Software ist, mit denen das Vertrauen in Computersysteme erhöht werden kann [Eck18, S. 381] [@Trua]. Die veröffentlichten Konzepte basieren in erster Linie auf dem Trusted Platform Module (TPM), einem passiven Kryptochip, der in etwa mit einer Smartcard vergleichbar ist [Eck18, S. 382].

2.2.2 Root of Trust

In der Terminologie der Trusted Computing Group (TCG) wird eine Root of Trust (RoT) als eine Komponente definiert, die eine oder mehrere sicherheitsspezifische Funktionen ausführt. Zu den genannten Funktionen zählen unter anderem das Messen, Speichern, Berichten (Logging) sowie das Verifizieren von Informationen. Es wird darauf vertraut, dass sich eine RoT stets in einer erwarteten Art und Weise verhält, da etwaiges Fehlverhalten nicht erkannt werden kann [Tru17].

Infolgedessen werden RoTs auch als Vertrauensanker (engl. trust anchor) eingesetzt. In hierarchischen kryptografischen Systemen wird der Begriff des Vertrauensankers verwendet, um eine Entität zu bezeichnen, von der nicht nur abgeleitete Vertrauenswürdigkeit angenommen wird. Als Beispiele können Wurzelzertifikate (engl. root certificate) angeführt werden, denen vertraut wird. In der Konsequenz gelten davon abgeleitete Zertifikate als vertrauenswürdig, da sie sich in die kryptografische Hierarchie einordnen lassen.

Hardware-Sicherheitsmodule wie zum Beispiel das Trusted Platform Module v.2 (TPM2) können ebenfalls eine RoT zur Verfügung stellen. Auf dieser Grundlage wird durch die kryptografische Hierarchie vertrauenswürdiges Material erzeugt (bzw. technisch abgeleitet), wie zum Beispiel kryptografische Schlüssel, Daten werden signiert und weitere kryptografische Operationen zur Verfügung gestellt. Die sichere Speicherung von Schlüsselmaterial stellt beispielsweise ein Merkmal des TPM2 dar [Art15].

2.2.3 Trusted Platform Module

Das Trusted Platform Module (TPM) ist ein Hardwaresicherheitsmodul in Form eines fest verbauten Mikrochips, welches manchmal auch als kryptografischer Co-Prozessor bezeichnet wird. Der TPM ist erstmals 2009 als internationale Norm als ISO/IEC 11889-2015 spezifiziert worden [ISO15]. Neben der ISO/IEC entwickelt und pflegt die TCG auf ihrer Webseite die sogenannte „Trusted Platform Module Library Specification“, welche alle dazugehörigen Teilspezifikationen in der aktuellsten Revision und die ISO/IEC-Version bereitstellt[3]. Der TPM2 erlangte erstmals größere Aufmerksamkeit, als er von Microsoft für die Festplattenverschlüsselung Bitlocker eingesetzt wurde. Mittlerweile ist der TPM2 eine obligatorische Komponente für die Nutzung von Windows 11 [@Mic].

[3]TPM 2.0 Library: https://trustedcomputinggroup.org/resource/tpm-library-specification.

Der TPM2 verfügt über unterschiedliche Funktionen für kryptografische Operationen und Konzepte. Zu den wichtigsten Funktionen zählen ein sicherer Zufallszahlengenerator, ein sicherer Speicher für kryptografische Schlüssel, eine sichere kryptografische Schlüsselerzeugung (symmetrisch/asymmetrisch) sowie insbesondere die sogenannten Platform Configuration Register (PCR) [Art15, S. 135]. Des Weiteren verfügt der TPM2 auch über Funktionen wie das sogenannte „sealing“ (dt. versiegeln). Besonders hervorzuheben sind die sogenannten PCRs, diese dienen dazu, Konfigurationszustände in Form von Hash-Werten zu speichern.

Platform Configuration Register

Die sogenannten PCR sind eigene Register im TPM2, in welchen der TPM2 Hashwerte ablegen kann. Gemäß Spezifikation kann der TPM2 mehrere PCR-Bänke beinhalten. Eine PCR-Bank kann als Sammlung von PCRs betrachtet werden, die mit demselben Hash-Algorithmus erweitert wurden. Jeder PCR-Bank ist ein eigener Hash-Algorithmus vorbehalten [Tru24a, S. 53]. Abhängig vom jeweiligen TPM2-Typ sind SHA-1, SHA-256 und SHA-512 verfügbar. Um die Inhalte bzw. die Werte eines PCR-Registers zu ändern, können diese entweder zurückgesetzt oder erweitert werden. Es ist nicht möglich, einen beliebigen Hash-Wert in einem PCR-Register abzulegen. PCRs werden wie folgt gesetzt:

$$PCR_{new} = \mathbf{H}_{alg}(PCR_{old} \parallel digest) \tag{2.1}$$

Mit:

- PCR_{new}: Neuer Wert der PCR
- PCR_{old}: Aktueller Wert der PCR
- $digest$: Neuer Hash-Wert, der hinzugefügt wird
- $\mathbf{H}_{alg}$: Hash-Algorithmus

PCRs spielen eine wesentliche Rolle im Kontext der kryptografischen Protokollierung des Bootvorgangs. Die nachfolgende Abbildung 2.4 zeigt einen Screenshot von PCRs, die teilweise gefüllt sind.

```
sha256:
  0 : 0x0000000000000000000000000000000000000000000000000000000000000000
  1 : 0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4FBABB8291E8F0872E062
  2 : 0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECEE77E42365E1D5FA9ED6C
  3 : 0x0000000000000000000000000000000000000000000000000000000000000000
  4 : 0x0000000000000000000000000000000000000000000000000000000000000000
  5 : 0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B22785D29DB324B23C53C9B4
  6 : 0x0000000000000000000000000000000000000000000000000000000000000000
  7 : 0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C5106E8E9B7153EEB36598BB
  8 : 0x0000000000000000000000000000000000000000000000000000000000000000
  9 : 0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5DE4E884F7A0E3DF506A3
 10: 0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D2ED8951D16E175E92763
 11: 0x0000000000000000000000000000000000000000000000000000000000000000
 12: 0x0000000000000000000000000000000000000000000000000000000000000000
 13: 0x0000000000000000000000000000000000000000000000000000000000000000
```

Abbildung 2.4.: Auszug von PCRs, Quelle: Eigene Darstellung

2.2.4 Measured Boot

Das Ziel des Verfahrens „Measured Boot“ besteht in der Messung sämtlicher am Bootvorgang beteiligten Softwarekomponenten. Zu diesem Zweck wird für jede gemessene Komponente ein Hash-Wert erstellt und in den PCRs durch Konkatenation hinzugefügt. Der beschriebene Vorgang und die daraus resultierenden Hash-Werte sind reproduzierbar. Auf diese Weise lassen sich Abweichungen und nicht konforme Komponenten identifizieren. Dies wird ermöglicht durch die PCR-Bänke des TPM2s. Die folgende Abbildung 2.5 zeigt den schematischen Ablauf, der anschließend erklärt wird.

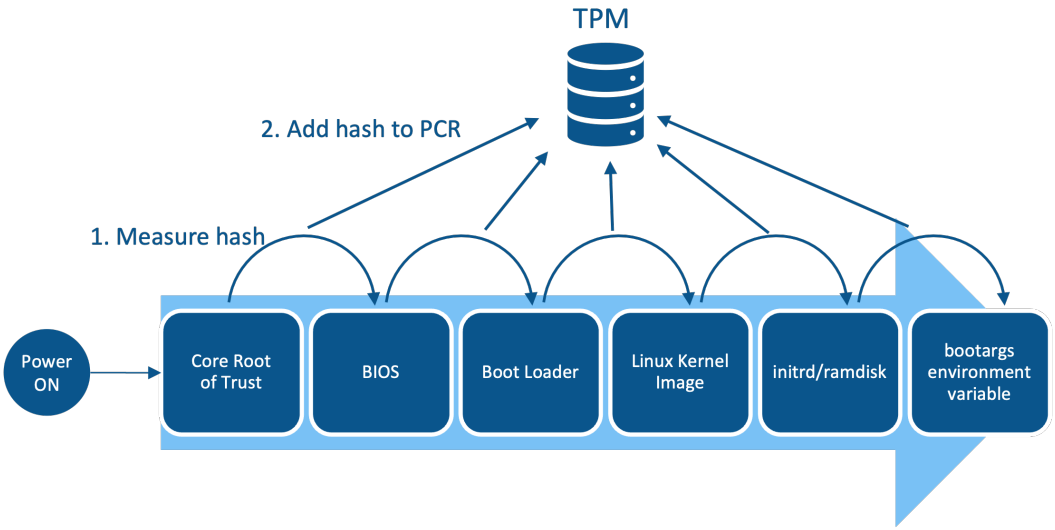

Abbildung 2.5.: Ablauf Measured Boot, Quelle: Eigene Darstellung

Mit dem Einschalten oder einem Neustart eines IEDs wird die Core Root of Trust (CRT) initialisiert. Die CRT stellt ein in Hardware integriertes, unveränderbares Softwareprogramm dar, welches das BIOS kryptografisch misst, indem es einen Hash-Wert von den BIOS-Dateien erzeugt. Anschließend wird dieser Hash-Wert an ein PCR gegeben und konkateniert. Erst danach wird das BIOS gestartet und misst den Bootloader. Das Messergebnis des Bootloaders wird ebenfalls an den TPM2 gegeben, bevor der Bootloader startet. In der Folge führt auch der Bootloader eine entsprechende Messung der nächsten Komponenten durch und leitet das Resultat an die PCR des TPM2s weiter, bevor das Linux Kernel Image gestartet wird. Der weitere Bootvorgang verläuft analog. Hier wird ein Linux-basierter Ansatz skizziert (mit initrd/ramdisk und weiteren Bootparametern).

2.2.5 Remote Attestation

Die Funktion der Remote Attestation ermöglicht die sichere Abfrage der Integrität einer Plattform aus der Ferne. Das Ziel dieser Maßnahme ist die Gewährleistung einer umgehenden Detektion von manipulierter Software bzw. Bootvorgängen und weiteren Plattformkonfigurationen. Die manipulierte Software wird durch die vom Soll abweichenden PCR-Werte entdeckt. Dies ist insbesondere sinnvoll zur Überwachung des Bootprozesses sowie der danach gestarteten Software.

Der Begriff „Remote Attestation“ kann im Deutschen am ehesten mit dem Wort „Fernbescheinigung“ übersetzt werden. Unter dem Begriff wird verstanden, „eine Aussage über die Eigenschaft eines Objektes zu machen, indem Gutachter über ein Netzwerk Beweise vorlegen“ ([Cok+11]). Die Verwendung eines TPM2s und der darin enthaltenen PCRs sowie eines vorhandenen Measured-Boot-Verfahren bildet die Grundlage für die Übertragung der PCRs als Beweise über ein Netzwerk.

Die TCG hat für Remote Attestation unterschiedliche Anwendungsfälle definiert und zuletzt als Trusted Attestation Protocol (TAP) standardisiert [Tru19b]. Das Trusted Attestation Protocol stellt somit kein technisches Protokoll dar, sondern vielmehr eine Beschreibung von Anwendungsfällen, Abläufen und Informationsmodellen [Tru19d] für die Remote Attestation. Zum besseren Verständnis wird im Folgenden das Verfahren der sogenannten expliziten Attestierung vorgestellt, welches in Abbildung 2.6 dargestellt ist.

In der gezeigten Abbildung sind zwei Rollen eingezeichnet, nämlich der Verifier und der Attester. Der Verifier ersucht vom Attester einen Nachweis über die Hash-Werte bestimmter PCR-Register, um diese mit den hinterlegten Soll-Werten abzugleichen.

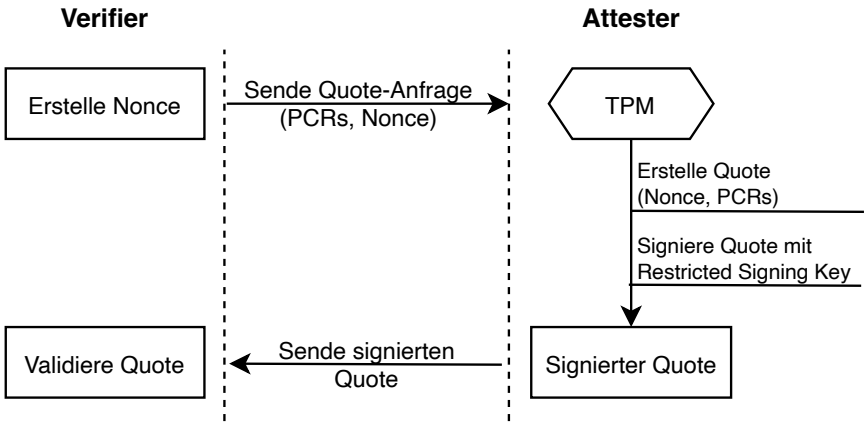

Abbildung 2.6.: Ablauf von Remote Attestion zwischen Verifier und Attester

Dadurch sollen Abweichungen an Softwarekomponenten erkannt werden. Zu diesem Zweck übermittelt der Verifier eine Quote-Anfrage (engl. quote request). Die Quote-Anfrage beinhaltet die angeforderten PCR-Register sowie eine Zufallszahlenkette, die als Nonce bezeichnet wird. In der Folge leitet der Attester diese Daten an den TPM2 weiter, welcher auf Basis dieser Angaben einen sogenannten Quote generiert. Die Funktion des Quotes ist eine Komponente des TPM2, deren Ausführung ausschließlich innerhalb des TPM2 erfolgt. Im Anschluss erfolgt die Signatur des Quotes im TPM2 durch den sogenannten Restricted Signing Key (RSK, dt. beschränkter Signaturschlüssel). Der RSK ist dafür von essenzieller Bedeutung, da er lediglich dazu befugt ist, Daten zu signieren, die vom und im TPM2-Chip selbst generiert wurden. Anschließend gibt der TPM2-Chip das Quote-Objekt aus und der Attester sendet dies zurück an den Verifier. Aufseiten des Verifiers wird zunächst die Signatur mit dem öffentlichen Schlüssel des RSKs verifiziert. Ebenfalls wird der Nonce verifiziert, indem er mit dem vorab versendeten abgeglichen wird. Danach kann der Verifier den Quote-Inhalt nutzen und diesen mit den Soll-Werten vergleichen. Die sinnvolle Nutzung eines Quotes setzt voraus, dass der öffentliche Schlüssel sowie die PCRs bereits vorab zur Verfügung stehen.

In den Dokumenten der TCG zur Remote Attestation werden hauptsächlich die Anwendungsfälle beschrieben sowie separate Informationsmodelle vorgestellt. Diese konzentrieren sich insbesondere auf die Datenstrukturen des Quotes. Die Quote-Funktion selbst ist Teil der TPM2-Spezifikationen und wird über die entsprechenden APIs angesprochen. Es konnten keine nutzbaren Bibliotheken identifiziert werden, welche den gesamten Prozess abdecken würden, inklusive der Datenübermittlung über ein Netzwerk.

2.3 Verwandte Arbeiten und Stand der Technik

In diesem Abschnitt werden die relevanten Arbeiten vorgestellt, die den Stand der Technik im Bereich der Sicherheitsautomation und von Trusted Computing widerspiegeln oder in dem Bereich zu verorten sind.

2.3.1 Sicherheitsautomatisierung

Das Security Content Automation Protocol (SCAP) ist ein Projekt vom National Institute of Standards and Technology (NIST) und entstand aus der NIST-Agenda für IT-Sicherheitsautomatisierung. SCAP ist kein Protokoll im eigentlichen Sinne, sondern wird auf der Website beschrieben als „eine Synthese interoperabler Spezifikationen, die aus Ideen der Community abgeleitet sind“ (aus dem Englischen übersetzt, siehe [Nat]). Es handelt sich also eher um eine Suite von Anwendungen zum Austausch von Inhalten der Sicherheitsautomatisierung, um die Konformität von Konfigurationen bewerten zu können und die Erkennung von vorhandenen Schwachstellen zu unterstützen. Die Suite enthält unter anderem einen Schwachstellen-Scanner, beschreibt Asset-Reporting-Formate sowie eine Asset-Identifikation und andere Beschreibungssprachen. 2018 hat NIST die Version 2 von SCAP mit einem viel breiteren Fokus auf die Gesamtarchitektur angekündigt und diese befindet sich seitdem im Internet-Draft-Status unter der Internet Engineering Task Force (IETF) als *Security Automation and Continuous Monitoring (SACM) Architecture* [WF18]. SCAP in der Version 1 zielt primär auf die typische Office-IT-Domäne ab. Ob und ggf. wie Version 2 zur Unterstützung der Ziele dieses Promotionsvorhabens genutzt werden kann, kann evaluiert werden, sobald sie den IETF-Entwurfsstatus verlassen hat.

Die automatisierte Einhaltung von geltenden Richtlinien für OT-Systeme in der Industrie 4.0 wurde von Bicaku et al. mit dem Ziel untersucht, die Einhaltung von Standards automatisch zu verifizieren [Bic+18]. Sie haben für den Zweck ein *Monitoring and Standard Compliance Verification Framework* (MSVP) entwickelt, das neben organisatorischen Indikatoren auch Security- und Safety-Standards berücksichtigt. Für die Bewertung fragten die Autoren die benötigten Daten von Geräten ab, indem sie benutzerdefinierte Agenten verwendeten, die mit ihrem Überwachungssystem kommunizieren können. Das Überwachungssystem stellt die gesammelten Daten dann dem MSVP-Rahmenwerk zur Verfügung. Die Daten von den Geräten wurden mithilfe von benutzerdefinierten Skripten in die Management- und Analysekomponente, die sich in der Cloud befindet, transferiert. Da die Datenerfassung nicht ihr Schwerpunkt war, erwähnten sie, dass „messbare Metriken von standardisierten

Stellen vorgeschrieben werden sollten“ [Bic+18, p. 751]. Dies unterstreicht im Kontext der hier vorliegenden Dissertation, wie wichtig es ist, messbare Sicherheitskonfigurationen in integrierter Form bereitzustellen.

2.3.2 Informationsmodelle für IT-Sicherheitsinformationen

Der von der Organization for the Advancement of Structured Information Standards (OASIS) veröffentlichte und als Open Source verfügbare Structured Threat Information Expression (STIX) (dt. strukturierter Bedrohungsinformationsaustausch) ist ein Datenformat für den strukturierten Austausch von Bedrohungsinformationen [BRT21]. Damit ist das Format im Bereich der sogenannten Cyber-Threat-Intelligence (CTI) angesiedelt und ermöglicht den Erkenntnisaustausch zwischen Organisationen über ein strukturiertes Datenformat. Dazu kompatibel definiert OASIS den Standard Trusted Automated Exchange of Intelligence Information (TAXII), welcher den Austausch von Informationen über Cyberbedrohungen als RESTful-API (representational state transfer) auf der Schicht der Anwendungsebene beschreibt [OAS21]. Dazu gehören auch Beschreibungen und Definitionen für den jeweiligen Client und Server. TAXII wurde entwickelt, um den Austausch von STIX-Informationen an den Schnittstellen zu beschreiben. Die beiden Standards unterstützen den Austausch zu konkreten Bedrohungen und definieren entsprechende Datenmodelle und Schnittstellen. Der Austausch von Bedrohungen ist nicht der entsprechende Fokus dieser Arbeit, daher werden STIX und TAXII nicht weiter berücksichtigt. Auch deren Informationsmodelle sind für die vorliegende Arbeit nicht interessant, da sie keine Sicherheitskonfigurationen beinhalten und nicht gerätespezifisch sind, sondern spezifische Bedrohungen beschreiben. Darüber hinaus ist der Einsatz weiterer Kommunikationsprotokolle über die zuvor definierten nichtfunktionalen Anforderungen nicht vorgesehen.

2.3.3 Trusted-Computing-Technologien

In einem Übersichtspaper aus dem Jahr 2010 wird von Kuntze et al. allgemein aufzeigt, welche Verbesserungen hinsichtlich der Sicherheit der OT- und IKT-Komponenten im Smart Grid durch den Einsatz von Trusted Computing und Trusted Platform Module v1 (TPM1) erreicht werden könnten [Kun+10]. Als Anwendungsmöglichkeiten im Smart Grid wird insbesondere auf die typischen Anwendungsfälle wie „Secure Identification of Devices“, „Integrity of Executable Software and Configuration“,

„Accounting-Support and Reliable Time-Information“, „Economic and Efficient Security“ sowie „Privacy-Protection“ eingegangen. Damit umfasst die Publikation alle offensichtlichen Vorteile von TCG-Konzepten in Verbindung mit einem TPM1 in Bezug auf das Smart Grid. Allerdings wird in der Veröffentlichung keine konkrete Umsetzung oder ein Proof of Concept vorgestellt. Es werden die Anwendungsgebiete eines TPM1 auf das Smart Grid bezogen und deren Vorteile bzw. Sicherheitsoptionen beschrieben.

In [Rei+16] wird der Einsatz von TCG- und TPM1-Konzepten für Steuerungsanlagen im Anwendungskontext eines Staudamms dargelegt. Die Autoren beschreiben darin zusammenarbeitende cyberphysische Systeme (CPS), wie sie in typischen SCADA-Infrastrukturen zu finden sind, und ihre neue Lösung: einen sogenannten Trusted Information Agent (TIA). Der TIA nutzt einen TPM1-Chip, um damit die Software der Sensoren und Aktuatoren zu messen und darauf aufbauend eine Vertrauenskette zu etablieren. Zur Übermittlung der Werte und zur Aufrechterhaltung der Vertrauenskette wird Remote Attestation eingesetzt. Der TPM1 übernimmt dabei die Stellung als Root of Trust (RoT). Die Implementierung wurde laut den Autoren im Rahmen des europäischen Forschungsprojektes „MAnagement of Security information and events in Service InFrastructures“ (MASSIF) umgesetzt und an ein Security Information and Event Management (SIEM) angebunden [Nev+13].

2.3.4 Remote-Attestation-Integrationen

Die Autoren Tan et al. untersuchen in einer Publikation unterschiedliche Sicherheitsmechanismen und Sicherheitstechnologien, um Firmware besser zu schützen [Tan+19]. Ausgehend von den Angriffen auf das ukrainische Stromnetz haben die Autoren einen Sicherheitsrahmen für das intelligente Stromnetz vorgestellt und erörtert. Remote Attestation wird dabei als Teil verschiedener Sicherheitsprinzipien nach dem Grundsatz „Defence in Depth“ (dt. mehrschichtige Verteidigung) betrachtet. Die Autoren kommen zu dem Schluss, dass die Sicherheit der Firmware von entscheidender Bedeutung ist und dass die Daten auf der RTU besser abgesichert werden müssen. Sie betrachten die Remote Attestation als eine gute Grundlage dafür.

In der Publikation von Birnstill et al. [Bir+17] ist die Funktion von Remote Attestation mittels Trusted Platform Module der Version 1.2 in das Industrieprotokoll OPC UA integriert worden. Die Autoren haben zusätzlich den Zufallszahlengenerator, die Schlüsselerzeugung und die Speicherfunktionen in diesem Kontext eingesetzt. Abschließend empfehlen die Autoren die Integration von TPM-basierten Funktionen

in den OPC-UA-Standard und schlagen die Verwendung von OPC-UA-Profilen für die Integration von Remote Attestation vor.

2.3.5 Common Information Model / IEC 61970

Die Publikation von Lehnhoff et al. [Leh+11] beschreibt, wie IEC 61850 und IEC 61970/61968 (Common Information Model (CIM)) auf OPC UA abgebildet werden können. Sie zeigen verschiedene Ansätze der Modellierung von Attributen, mit und ohne funktionale Einschränkungen. Die Mappings werden in drei verschiedenen Beispielen demonstriert, die gezeigt haben, dass es mehrere Möglichkeiten gibt, typische Datenmodelle abzubilden [Leh+11]. Kombiniert mit dem bereits erwähnten Konzept in [Bir+17] könnte dies auch als Ansatz genutzt werden, um Remote Attestation für IEC 61850 auf eine indirekte Weise zu implementieren. Für OPC UA existiert ebenfalls ein sogenannter Begleitstandard(companion standard) -Entwurf, welcher das Mapping von IEC 61850 in OPC UA beschreibt (OPC 10040 IEC 61850 [@Fou]).

3 Analyse der IT-Sicherheitsstandards und -Anforderungen

In diesem Kapitel erfolgt eine Analyse von bestehenden und veröffentlichten IT-Sicherheitsnormen, um daraus abzuleiten und zu analysieren, inwieweit die darin beschriebenen Anforderungen technisch abgefragt werden können. Dieses Kapitel stellt somit die Grundlage für die weitere Arbeit dar, da die Identifikation von IT-Sicherheitskonfigurationen über die Anforderungen aus den Normen heraus erfolgen soll.

Das Kapitel Analyse der IT-Sicherheitsstandards und -Anforderungen ist wie folgt gegliedert: Als Erstes wird der Stand der Technik hinsichtlich der Automatisierbarkeit von Anforderungen aus IT-Sicherheitsnormen beleuchtet. Im Anschluss werden die ausgewählten Normen vorgestellt und eingeordnet. Schließlich wird das Vorgehen der Analyse sowie die daraus resultierenden Ergebnisse präsentiert. Das Kapitel endet mit einer Diskussion der Ergebnisse in einem Fazit.

3.1 Verwandte Arbeiten

In dem speziellen Themenbereich Analyse von IT-Sicherheitsnormen mit dem Fokus auf die Automatisierbarkeit der Anforderungen konnte genau eine Publikation identifiziert werden. Montesino et al. haben in [MF11] untersucht, wie weit Informationssicherheit automatisiert werden kann, welche Werkzeuge es dafür gibt und welche Ansätze dafür existieren. Für ihre Untersuchung wurden global anerkannte Sicherheitsstandards betrachtet, welche Sicherheitsmaßnahmen spezifizieren, die sich auf die Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen beziehen. In der Folge wurden drei Normen betrachtet: Die ISO 27001, die NIST SP 800-53 und die sogenannten Consensus Audit Guidelines. Die Consensus Audit Guidelines stellen 20 Sicherheitsmaßnahmen, welche von IT-Sicherheitsexperten im Konsensverfahren aufgestellt wurden und als wirksam gegen Angriffe betrachtet wurden.

Eine Sicherheitsmaßnahme wird von den Autoren als automatisierbar betrachtet, wenn der Betrieb der Sicherheitsmaßnahme ohne das Eingreifen durch einen Menschen erfolgen kann. Um Sicherheitsmaßnahmen für diese Kriterien zu identifizieren, werden auch die Maßnahmen betrachtet, die teilweise automatisiert werden können, wenn der Betrieb und die Kontrolle über die Sicherheitsmaßnahmen nur maschinenlesbare und -verarbeitbare Ressourcen erfordert, oder diese durch Sicherheitsanwendungen übernommen werden können.

Die Ergebnisse von Montesino et al. lassen sich wie folgt zusammenfassen:

- **ISO 27001:** Enthält 133 Sicherheitsmaßnahmen, davon wurden 37 Sicherheitsmaßnahmen als automatisierbar eingestuft (entspricht 27,8 %).
- **NIST SP 800-53:** Beschreibt insgesamt 198 Sicherheitsmaßnahmen, davon wurden 62 als automatisierbar eingestuft (entspricht 31,3 %).
- **Consensus Audit Guidelines:** Definiert 20 Sicherheitsmaßnahmen, davon wurden 15 Maßnahmen als automatisierbar eingestuft (entspricht 75 %).

Des Weiteren wurden Überschneidungen identifiziert. Diese betrafen insbesondere die Consensus Audit Guidelines, deren Anforderungen bzw. Sicherheitsmaßnahmen zu einem Drittel direkt auf die NIST SP 800-53 abgebildet werden können.

Die Publikation von Montesino et al. zeigt, dass Sicherheitsmaßnahmen grundsätzlich automatisiert werden können. Im Kontext der vorliegenden Arbeit ist dies ein wichtiges Indiz, dass zum einen die maschinelle Ausführung von Sicherheitsmaßnahmen möglich ist und zum anderen auch die Menge der als automatisierbar identifizierten Maßnahmen ausreichend groß ist, um darauf weiter aufzubauen. Die Publikation überprüft allerdings nicht im Sinne der vorliegenden Arbeit, ob die aus einer Anforderung abgeleitete Konfiguration technisch ausgedrückt oder für Auswertungen des Ist-Zustandes genutzt werden können. Die Autoren betrachten zum Beispiel die Forderung nach einem Back-up als eine automatisiert ausführbare Maßnahme und setzen damit einen anderen Schwerpunkt.

3.2 Auswahl der Normen

Für die vorliegende Arbeit erfolgt eine Betrachtung von IT-Sicherheitsnormen, die innerhalb der Energiedomäne und im Bereich der IT-Sicherheit Konsens sind oder von der Agentur der Europäischen Union für Cybersicherheit (ENISA) vorgeschlagen

wurden. Die ausgewählten Normen bilden dadurch Maßnahmen und Vorgehensweisen zur IT-Sicherheit nach international vereinbartem Standard ab. Infolgedessen werden für die vorliegende Arbeit ebenfalls Normen betrachtet, die zu unterschiedlichen Zeitpunkten entstanden sind und dadurch unterschiedliche Innovationshöhen bzw. Modernität aufweisen. Die Auswahlkriterien ermöglichen ebenfalls eine Übertragbarkeit der Ergebnisse auf andere, verwandte Domänen wie zum Beispiel die Automatisierungstechnik.

Die Vollständigkeit zur Abdeckung aller existierenden Anforderungen in den Normen ist für die Zielsetzung der vorliegenden Arbeit nicht zwingend erforderlich. Die ausgewählten Normen sollen für die vorliegende Arbeit ein ausreichendes Spektrum an Anforderungen abdecken, um hinreichend gute Ergebnisse zu erzielen. Als Schwellenwert werden mindestens 30 Anforderungen pro Norm bzw. Standard als ausreichend für die Beantwortung der Forschungsfrage erachtet.

In der Vorgehensweise für die Auswahl der Normen wurden zunächst zwei Kategorien von Normen betrachtet. Zum einen wurde die organisatorische Norm ISO 27001 in den Blick genommen, da deren Umsetzung und das daraus resultierende ISMS in Deutschland für Betreiber kritischer Infrastrukturen gesetzlich vorgeschrieben sind. Zum anderen wurden technische Normen und Standards berücksichtigt, die Anforderungen an die technischen Umsetzungen stellen.

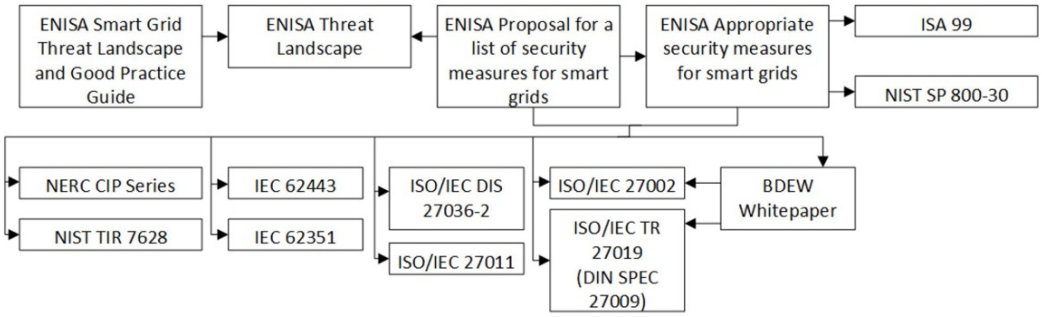

Abbildung 3.1.: ENISA Threat Landscape for Smart Grids, Quelle: [GHS17]

Der Fokus dieser Arbeit liegt jedoch auf der Analyse und Betrachtung von technischen Sicherheitsstandards für Informationssicherheit. Im Gegensatz zu den organisatorischen Sicherheitsnormen sind die Anforderungen an technische Maßnahmen darin deutlich konkreter und in der Regel technischer gefasst. Die Ausgangslage für die Auswahl der technischen IT-Sicherheitsstandards sind zwei Publikationen: die Publikation „Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilnetzbetreiber“ von Genzel et al. [GHS17] und die Publikation „Smart Grid Security: IEC 62351 and Other Relevant Standards“ von Rosinger et al. [RU13]. Genzel et al. leiten aus der Bedrohungslandschaft der Agentur der Europäischen Union

für Cybersicherheit (ENISA) für Smart Grids die für Verteilnetzbetreiber relevanten Standards ab. Diese sind in Abbildung 3.1 dargestellt und zeigen auch die jeweiligen Einflussstandards, beginnend mit den Empfehlungen der ENISA.

Rosinger et al. stellen die Normen IEC 62351- 1-11 sowie IEC 62443-4,5 und IEC62443/ISA99, die North American Electric Reliability Corporation (NERC) CIP 002-009, das BDEW-Whitepaper und die ISO-27001-Serie vor. Im Fazit betrachten die Autoren die vorgestellten Normen als geeignete und etablierte IT-Sicherheitsstandards für das Smart Grid.

Die Relevanz der Norm IEC 62443 für das Energienetz wird von Rintala et al. dargelegt [Rin+23]. Die Autoren setzen die Norm für einen ganzheitlichen und systematischen Ansatz eines Sicherheitsprogramms eines Verteilnetzbetreiber (VNB) ein und kommen zu dem Ergebnis, dass diese den Sicherheitsbedürfnissen entspricht. Die Autoren überzeugt der ganzheitliche Ansatz durch die jeweilige Adressierung von Mitarbeitern, Prozessen sowie Technologien. Zudem wird die Übernahme von Best Practices aus der SCADA-Domäne positiv bewertet. Die zuvor genannte Publikation von Rosinger et al. [RU13] stellt ebenfalls fest, dass der IEC 62443 dem ISO 2700x ähnlich ist, allerdings einen deutlich technischeren Fokus hat. In der Veröffentlichung [Fra+19] wurde untersucht, inwiefern sich der Teil 3–3 der Normenreihe IEC 62443 als ganzheitlicher Ansatz für die Anwendbarkeit auf Anlagen im Verteilnetz eignet. Für die Untersuchung haben die Autoren eine Risiko- und Bedrohungsmatrix erstellt und anschließend geprüft, ob die im IEC 62433-3-3 enthaltenen Maßnahmen die Risiken und Bedrohungen abdecken können. Sie kommen zu dem Schluss, dass es im Bereich kritischer Infrastruktur sinnvoll ist, einen international anerkannten Sicherheitsstandard zu verwenden, dessen Sicherheitsanforderungen den gesamten Lebenszyklus abdecken.

Damit es im Rahmen dieser Arbeit möglich ist, die Forschungsfrage zu beantworten, wurden die in den Publikationen vorgestellten Normen und Standards weiter eingegrenzt. So ist beispielsweise die Norm IEC 62443 aus dem Standard der ISA 99 hervorgegangen, bzw. die ISA 99 war ihr Vorgänger, und wird daher nicht näher betrachtet. Ergänzend werden die in Deutschland relevanten Regularien, Regelwerke und Normen auch berücksichtigt. Diese sind:

- Die Normenreihen ISO 27001 und ISO 27002 aufgrund gesetzlicher Vorgaben in Deutschland.

- Die IEC 62351, weil diese Normenreihe die IT-Sicherheit in Energiemanagementsystemen und zugehörigem Datenaustausch beschreibt.

- Die IEC 62443, weil diese Normenreihe IT-Sicherheit für industrielle Kommunikationsnetze und Systeme beschreibt und über ein hohes Sicherheitslevel verfügt.

3.3 Vorstellung der Normen

Dieser Abschnitt stellt die ausgewählten und in der vertieften Analyse berücksichtigten Normen und Standards vor. Diese sind:

- IEC 62443
- IEC 62351
- BSI IT-Grundschutzkompendium

3.3.1 IEC 62443

Die internationale Normenreihe IEC 62443 beschreibt *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme für Industrial Automation and Control Systems (IACS)*. Damit Industrial Automation and Control Systems (IACS) resilienter gegen Bedrohungen über die Kommunikationsnetze bzw. den Cyberraum werden, enthält die Norm IEC 62443 spezifische Anforderungen zur Erreichung der CIA-Eigenschaften, Vertraulichkeit (engl. confidentiality), Integrität (engl. integrity) und Verfügbarkeit (engl. availability), für Komponenten und Systeme im Bereich der industriellen Automatisierung.

Die Normenreihe besteht aus mehreren Teilen, welche sich spezifisch an Systemintegratoren, Hersteller und Betreiber von IACS richten [Kob16]. Einen Überblick gibt die Abbildung 3.2. Sie veranschaulicht, dass die Norm in vier Bereiche gegliedert ist: Allgemeines, Leitlinien und Vorgehensweise, System sowie Komponenten.

Des Weiteren werden im Standard Themen wie die sichere Implementierung von IACS sowie die sichere Beschaffung dieser (siehe Teil 2–1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber, [DIN EN IEC 62443-2-1 (VDE 0802-2-1): 2020-10]) adressiert. Die einzelnen Teile der Norm bauen aufeinander auf und sind miteinander abgestimmt.

Teil 1-1 der Normenreihe beschreibt grundlegende Sicherheitsprinzipien (vgl. [Kob16, S. 15]. Dazu zählen beispielsweise *Defense in Depth*, *Risikobewertungen* (siehe Teil

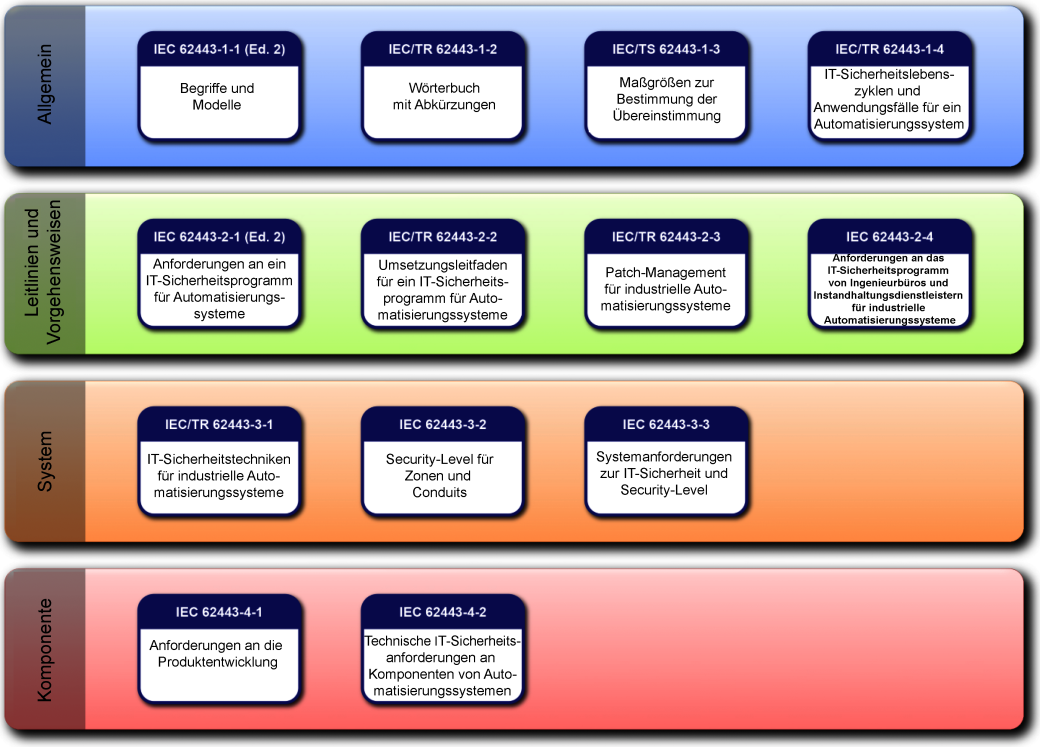

Abbildung 3.2.: Aufbau der Normenreihe IEC 62443 [20]

3–2: Sicherheitsrisikobeurteilung [DIN EN IEC 62443-3-2 (VDE 0802-3-2): 2021-12]) sowie Systemgestaltung und auch der *bewusste Einsatz von sicheren Produktlebenszyklen* (siehe Teil 4–1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung [DIN EN IEC 62443-4-1 (VDE 0802-4-1): 2018-10]).

Darüber hinaus definiert die Norm vier Security-Level (SL), welche genutzt werden, um das eigene Schutzlevel zu bestimmen und darüber Anforderungen abzuleiten. Diese sind wie folgt definiert:

- SL 1: Schutz gegen ungewollten, zufälligen Missbrauch,
- SL 2: Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation,
- SL 3: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und moderater Motivation,
- SL 4: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation.

Die Schutzlevel erlauben zudem eine Einschätzung und Vorstellung von den potenziellen Angreifern und tragen somit zur Abschätzung des eigenen Sicherheitslevels bei. Offenkundig ist, dass kritische Infrastruktur mindestens SL 3 erfüllen sollte, eigentlich aber SL 4 der Standard sein sollte. Eine Kombination der SL 3 und SL 4 kann ebenfalls eine geeignete Lösung darstellen, die sich aus der Risikoanalyse ableiten lässt. Die Security-Level gelten sowohl für einzelne Zonen als auch für einzelne Systeme.

Für die vorliegende Arbeit werden die technischen Anforderungen an die IACS berücksichtigt, was zur Auswahl von zwei Teilen des Standards führt: Teil 3-3 und Teil 4-2. In beiden Teilen werden die grundlegenden Anforderungen (FR, engl. Foundational Requirement) gemäß IEC 62443-1-1 kategorisiert. Die sieben grundlegenden Anforderungen sind:

- FR 1 – Identifizierung und Authentifizierung (IAC)
- FR 2 – Nutzungskontrolle (UC, Use-Control)
- FR 3 – Systemintegrität (SI, System-Integrity)
- FR 4 – Vertraulichkeit der Daten (DC, Data-Confidentiality)
- FR 5 – Eingeschränkter Datenfluss (RDF, Restricted Data-Flow)
- FR 6 – Rechtzeitige Reaktion auf Ereignisse (TRE, Timely Response to Events)
- FR 7 – Ressourcenverfügbarkeit (RA, Resource-Availability)

Teil 3–3 definiert die *Anforderungen an die Systemsicherheit und Sicherheitsstufen* und kategorisiert sie entsprechend den grundlegenden Anforderungen (FRs). Diese werden um die sogenannten Systemanforderungen (SR) erweitert. Dabei besteht jede Systemanforderung aus einer Hauptforderung und weitergehenden Anforderungen (RE), welche die IT-Sicherheit verstärken (vgl. [DIN EN IEC 62443-3-3 (VDE 0802-3-3): 2020-01, Kapitel 3.3, Absatz 1]). Die Haupt- und Nebenforderungen werden auf die Security-Level abgebildet. Für ein besseres Verständnis ist in Abbildung 3.3 ein Beispiel dafür gezeigt.

Das Beispiel der Abbildung 3.3 zeigt tabellarisch die Hauptanforderung (hier SR 1.1) und für welche System-Security-Level diese Anforderung gilt. Zusätzlich sind noch drei weitere Anforderungen definiert, die je nach angestrebtem System-Security-Level ebenfalls umgesetzt werden müssen. Die vorliegende Arbeit betrachtet alle Sicherheitsanforderungen inklusive SL 4 und alle grundlegenden Anforderungskategorien.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identifizierung und Authentifizierung (IAC)				
SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern	✓	✓	✓	✓
SR 1.1 RE 1 – Eindeutige Identifizierung und Authentifizierung		✓	✓	✓
SR 1.1 RE 3 – Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze			✓	✓
SR 1.1 RE 3 – Multifaktor-Authentifizierung über alle Netze				✓

Abbildung 3.3.: Beispiel der Hierarchie der funktionalen Anforderungen (FR) und der jeweiligen Systemanforderungen (SR) sowie Systemerweiterungen (RE) zur Erreichung der Sicherheitsebenen (SL)[Kob16, S. 70/71]

Teil 4–2 definiert *technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme* (siehe [IEC 62443-4-2:2019 - EN IEC 62443-4-2]). Darin werden technische Anforderungen an die IT-Sicherheit von Komponenten beschrieben, aus denen ein industrielles Automatisierungssystem aufgebaut ist. Teil 4-2 zielt insbesondere auf eingebettete Systeme, Netzwerkkomponenten sowie Host-Komponenten und Softwareanwendungen [Kob16]. Der Teil der Norm wird daher ebenfalls berücksichtigt. Der inhaltliche Aufbau folgt dem in Teil 3-3.

3.3.2 IEC 62351

Die Normenreihe IEC 62351 beschreibt unter dem deutschen Titel „Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation“ ebenfalls Anforderungen und Maßnahmen, um die drei grundlegenden Eigenschaften der Informationssicherheit innerhalb der Energiemanagementsysteme umzusetzen. Durch die beschriebenen Vorgaben an die Authentisierungsmöglichkeiten wird die Eigenschaft der Nicht-Abstreitbarkeit hinzugefügt.

Die aktuelle Serie umfasst mittlerweile mehr als 17 Teile. Die Struktur sowie die gegenseitigen Einflüsse dieser Norm sind in Abbildung 3.4 gezeigt. Wie zu erkennen ist, handelt es sich um eine umfangreiche Norm, die innerhalb der TC57-Referenzarchitektur auf der vertikalen Ebene angesiedelt ist. Um dem Ziel der vorliegenden Arbeit gerecht zu werden, wurden die relevanten Teile der Norm für diese Arbeit berücksichtigt, welche Sicherheitsanforderungen beschreiben, die konfigurierbar erscheinen und möglichst auf IEDs abzielen. Nicht betrachtet wurden hingegen diejenigen Teile, die aus thematisch weit entfernten Bereichen stammen, beispielsweise Teil 6, welcher Anforderungen an die Implementierung der Zustandsautomaten für Generic Object Oriented Substation Events (GOOSE) und für Sampled Values (SV) beschreibt (vgl. DIN EN 62351-6).

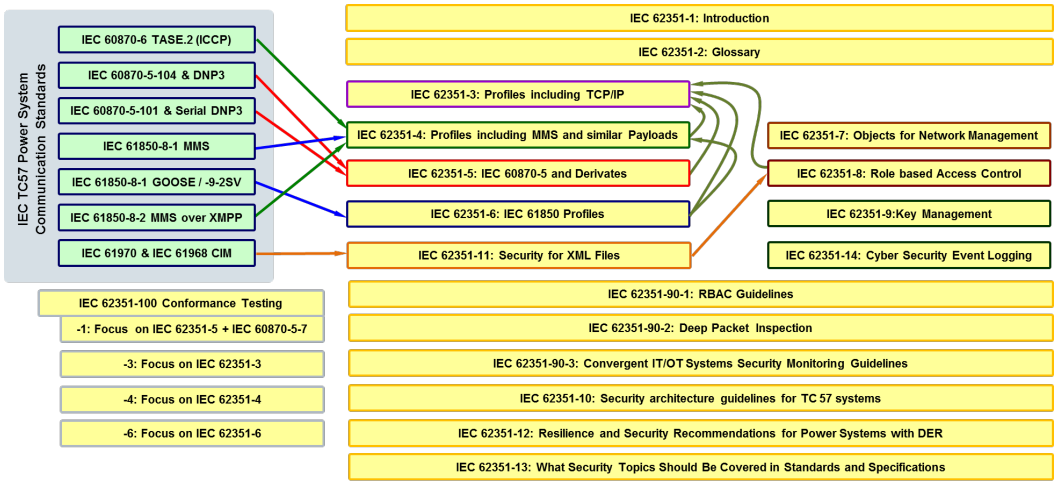

Abbildung 3.4.: Struktur, Aufbau und Beziehungen zu anderen Standards des IEC 62351, Quelle: [Int23]

Für die vorliegende Arbeit wurden folgende Teile der Norm als relevant eingestuft:

- IEC 62351-3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP (deutsche Fassung [Nor23])
- IEC 62351-4: Profile einschließlich Manufacturing Messaging Specification (MMS) und Ableitungen (deutsche Fassung [Nor21a])
- IEC 62351-6: Sicherheit für IEC 61850 (deutsche Fassung [Nor19a])
- IEC 62351-7: Datenobjektmodelle für Netzwerk- und Systemmanagement (NSM) (deutsche Fassung [Nor19b])
- IEC 62351-8: Rollenbasierte Zugriffskontrolle für Energiemanagementsysteme (deutsche Fassung [Nor21b])

3.3.3 IT-Grundschutzkompendium des BSI

Der BSI-IT-Grundschutz stellt ein Rahmenwerk und Instrumentarium bereit, welches konkrete und standardisierte Sicherheitsanforderungen für typische unternehmerische Prozesse und Projekte beschreibt, um diese nach dem Stand der Technik absichern zu können [Deu]. Der IT-Grundschutz wird kostenlos online veröffentlicht und zielt insbesondere auf kleine und mittelständische Unternehmen (KMU) ab, da er einen leichten Einstieg in den Aufbau eines ISMS ermöglicht. Beim IT-Grundschutz wird davon ausgegangen, dass die typischen Gefährdungen allgemein definiert werden können. Er erspart dem Anwender somit aufwendige Basisanalysen [Deu].

Das Ziel des IT-Grundschutzes ist es, praktisch erprobte Hilfsmittel in Form von Best Practices und Beispiellösungen für die Umsetzung von Sicherheitsanforderungen aus Standards niedrigschwellig bereitzustellen.

Der IT-Grundschutz besteht aus den drei Sicherheitsleveln Basis, Grundschutz und erhöhter Schutzbedarf. Vorrangig sollte das Basislevel umgesetzt werden, da hier mit geringem Aufwand der größtmögliche Nutzen erzielt werden kann und die Level aufeinander aufbauen. Die im IT-Grundschutz beschriebenen Best-Practice-Ansätze mit einfachen Mitteln gelten als leicht verständlich beschrieben und damit auch für ressourcenschwache Netzbetreiber zugänglicher [Lep18, S. 42].

Das IT-Grundschutzkompendium beschreibt nicht nur IT-spezifische Sicherheitsaspekte, sondern beinhaltet ebenfalls ein OT-Kapitel (Baustein industrielle IT, IND) zur Absicherung von Industriesystemen und Automatisierungstechnik. Unternehmen können die Bausteine dadurch ganzheitlich nutzen und nicht nur für einen Teilbereich des Unternehmens. Außerdem wird eine bessere Integration der Bausteine in das Gesamtmanagement gewährleistet.

Es gibt eine Bearbeitungsreihenfolge für die Bausteine, die von R1 bis R3 priorisiert sind. Erst wenn ein R vollständig umgesetzt ist, kann die nächste Stufe bearbeitet werden. Für diese Bausteine stellt das IT-Grundschutzkompendium eine fertige Tabelle zur Verfügung, die abgearbeitet werden kann.

Die Entwürfe für die kommende Version des IT-Grundschutzes werden unterjährig kommentiert, bevor sie als jährliche Edition im Februar herausgegeben werden [@Sic24]. Hinsichtlich der Aktualität ist dies ein Vorteil des IT-Grundschutzkompendiums gegenüber Normen. Der IT-Grundschutz soll auch einen leichten Einstieg zum Aufbau eines ISMS unterstützen [Deu, S. 1], dessen Umsetzung auch eine Zertifizierung nach ISO 27001 ermöglicht, wenn alle Sicherheitsanforderungen des Levels Grundschutz für den jeweiligen Geltungsbereich erfüllt sind [Deu, S. 3, Abs. 5]. Für Netzbetreiber kann dies bedeuten, dass der Einstieg über das IT-Grundschutzkompendium mit geringerem Aufwand verbunden ist als der direkte Weg über die ISO 27001, um den Sicherheitsprozess zu beginnen und zu verstetigen. Auch ist die Beschaffung von Normenreihen in der Regel kostenintensiv, während das IT-Grundschutzkompendium kostenfrei und online zur Verfügung steht und auch deshalb international genutzt wird. Der BSI-IT-Grundschutz hat im deutschsprachigen Raum auch rechtliche Relevanz [Lep18, S. 42] und ist deshalb von Bedeutung für die vorliegende Arbeit.

Der Baustein Industrielle IT (IND) beschreibt die Inhalte für den OT-Bereich und besteht aus insgesamt sieben Unterbausteinen. Diese sind im Einzelnen [Deu]:

- IND.1 Prozessleit- und Automatisierungstechnik

- IND.2.1 Allgemeine ICS-Komponente
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.3 Sensoren und Aktoren
- IND.2.4 Maschine
- IND.2.7 Safety Instrumented Systems
- IND.3.2 Fernwartung im industriellen Umfeld

Für die vorliegende Arbeit wurde die Analyse der Anforderungen des IT-Grundschutz-Kompendiums im Jahr 2021 auf Basis der IT-Grundschutz-Edition 2021 durchgeführt. Zu den jährlich neu erscheinenden Editionen gibt es ein Änderungsdokument, das die Änderungen zur Vorgängerversion dokumentiert. Der Baustein IND wurde in der Edition 2022 um den Baustein *IND.3.2 Fernwartung im industriellen Umfeld* erweitert. Dieser wurde in der hier vorliegenden Arbeit ebenfalls berücksichtigt, indem er nachträglich der Analyse hinzugefügt wurde. Darüber hinaus sind keine weiteren Änderungen zwischen den Editionen 2021 und 2023 bekannt.

3.3.4 Nicht berücksichtigte Normen und Standards

Über die ausgewählten Normen und Standards hinaus wurden weitere in Betracht gezogen, die jedoch in dieser Arbeit nicht berücksichtigt werden. Der Vollständigkeit halber werden diese kurz beschrieben:

- **ISO 27001:** Diese Norm ist relevant für die IT-Sicherheit im Stromnetz, da sie einen Organisations- und Managementprozess beschreibt, der in einem sogenannten ISMS mündet und insbesondere in Deutschland über das Energiewirtschaftsgesetz (EnWG) gesetzlich gefordert ist (vgl. § 11 EnWG). Da es sich bei dieser Norm um eine abstrakte Beschreibung von Management- und Unternehmensprozessen bzw. Vorgehensweisen handelt, wird sie in diesem Kapitel nicht weiter berücksichtigt, da von ihr aus keine technischen Anforderungen direkt gestellt werden. Die Norm ist jedoch von Bedeutung, da sie den Auftrag zum kontinuierlichen Messen, Prüfen sowie zur kontinuierlichen Verbesserung der Informationssicherheit gibt und somit einen erheblichen Teil der Motivation dieser Arbeit stellt.

- Das **Whitepaper vom Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW)** „definiert grundsätzliche Sicherheitsanforderungen für Steuerungs- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung“ ([Oes18, S. 5, Abs. 1]) und gibt Hinweise zu praktischen Umsetzungen, beispielsweise durch Verweise auf kryptografische Anforderungsdokumente der Bundesregierung. Für Themen der organisatorischen Sicherheit, wie das Risikomanagement, die Security-Awareness oder den Aufbau einer Sicherheitsorganisation, wird auf die spezifischeren Normen ISO/IEC 27001 und IES/IEC 27019 verwiesen. Das BDEW-Whitepaper wird in der vorliegenden Arbeit nicht berücksichtigt, da es für die konkreten technischen Anforderungen auf spezifischere Dokumente verweist und insgesamt eine vereinfachte Zusammenfassung der Anforderungen aus den Normenreihen ISO 27001 und 27002 darstellt.

3.4 Analyse der Standards und methodisches Vorgehen

In diesem Abschnitt wird das methodische Vorgehen bei der Analyse der Normenanforderungen beschrieben. Eine erste Vorauswahl wurde bereits im vorherigen Abschnitt durchgeführt, indem die ausgewählten Normenreihen nach technischen Anforderungen gesichtet wurden. Anschließend wurden die Anforderungen schrittweise für jede Norm in einer Excel-Tabelle erfasst.

Die meisten Anforderungen der Normen sind in Textform beschrieben und bestehen oft aus einem oder mehreren Sätzen, die teilweise mehrere Anforderungen beinhalten. Im Falle von mehreren Anforderungen in einem Absatz oder unter einem Gliederungspunkt in der jeweiligen Norm wurden diese im Rahmen der Analyse in einzelne Anforderungen aufgeteilt.

Zum besseren Verständnis schließt sich ein praktisches Beispiel aus der Norm IEC 62351-4, Abschnitt 6.2.7 an, wo die Anforderungen an die „Bewertungsdauer für den Sperrstatus von Zertifikaten mit öffentlichem Schlüssel“ wie folgt beschrieben werden:

- Absatz 1: *„Eine Implementierung, für die die Konformität mit diesem Teil von IEC 62351 erklärt wird, muss eine mindestens alle 24 Stunden erfolgende CRL-Aktualisierung unterstützen. Die Standard-Bewertungsperiode für gesperrte Zerti-*

fikate mit öffentlichem Schlüssel beträgt 24 Stunden. Diese Bewertungsperiode muss konfigurierbar sein.“ ([IEC 62351-4])

- Absatz 2: *„Eine Implementierung, welche OCSP für die Informationen aus der Überprüfung einer Sperre unterstützt, darf die OCSP-Antwort höchstens 24 Stunden im Cache speichern.“*
- Absatz 3: *„Wenn auf den CRL-Provider, den OCSP-Antwortsender oder eine lokal im Cache gespeicherte CRL oder OCSP-Antwort nicht zugegriffen werden kann, muss ein Sicherheitsereignis gemeldet werden (‚Warnung: Zertifikatsperrinformationen nicht verfügbar‘)“.*
- Absatz 4: *„Wie in IEC 62351-3:2018 vorgegeben, darf die Tatsache, dass die Sperrinformationen nicht abgerufen werden können, nicht die Beendigung der Sitzung nach sich ziehen.“*

Aus diesen vier Absätzen ergeben sich drei einzelne Anforderungen für die Analyse. Absatz 4 ist keine (technische) Anforderung im Sinne dieser Arbeit, da es sich dabei um eine Verhaltensbeschreibung handelt. Es liegt keine Anforderung, sondern vielmehr eine nichtfunktionale Anforderung vor, die typischerweise nicht konfigurierbar ist, sondern sich aus dem Gesamtsystem ergibt.

Anforderungskategorisierung

Anforderungen im Bereich der IT-Sicherheit können sich auf unterschiedliche Bereiche oder Komponenten beziehen. Im Rahmen der vorliegenden Arbeit wurden deshalb drei Kategorien gebildet, um abzubilden, an welchem Ort eine Anforderung umgesetzt werden muss. Die Kategorien wurden während der Sichtung der Anforderungen abgeleitet. Die erste Kategorie umfasst Anforderungen an Komponenten, die den typischen Bereich von IKT-Kommunikationsgeräten (z. B. Router, Switches) oder klassische Netzwerkbereiche adressieren. Sie werden in der Kategorie Netzwerk zusammengefasst. Dazu gehören auch Managementsysteme und Anwendungsserver, die ihre Dienste im Netzwerk bereitstellen. Beispiele hierfür sind Sicherheitsanforderungen an Dynamic Host Configuration Protocol (DHCP)-Server oder eine Zertifizierungsstelle für kryptografische Zertifikate. Die zweite Kategorie sind Prozesse. Hierunter fallen alle Aspekte, die keine technischen Anforderungen stellen, sondern primär auf Management- und Organisationsebene angesiedelt sind. Dazu gehören typische Prozessdefinitionen, Dokumentationsanforderungen, die Erstellung von Plänen (z. B. Backupstrategien) und allgemein strategische Vorgehensweisen. Die dritte Kategorie ist IED. Darin enthalten sind die Anforderungen, die sich an das

eigentliche „Endgerät“ richten. Je nach Norm werden andere Begriffe verwendet und es ist die Rede von IED (vgl. IEC 62351), IACS (vgl. IEC 62443), Speicherprogrammierbare Steuerung (SPS) oder eingebetteten Systemen. Anforderungen, die sich auf diese genannten Geräte beziehen, werden in dieser Arbeit der Kategorie IEDs zugeordnet.

Im nächsten Schritt wurde für jede Anforderung entschieden, welcher Kategorie sie zuzuordnen ist. Eine Anforderung kann zwei Kategorien angehören, da einige Anforderungen sowohl im Netzwerk als auch auf einem Endgerät bzw. IED umgesetzt werden können. Mit diesem validierenden Analyseschritt wurde sichergestellt, dass die ausgewählten Normen auch tatsächlich IT-Sicherheitsanforderungen beschreiben, die auf den Endgeräten bzw. IEDs umgesetzt werden können.

Wann ist eine Anforderung automatisiert überwachbar?

Als weiterer Teil der Analyse wurde beurteilt, ob eine Anforderung automatisierbar ist. Dazu wurde in dieser Arbeit definiert, dass eine IT-Sicherheitsanforderung automatisiert überwachbar ist, wenn ihre Konfiguration technisch kommuniziert werden kann. Für weitere Betrachtungen wurde angenommen, dass eine entsprechende Unterstützung durch Hersteller und Software gegeben ist.

Die Einschätzung, ob dies auf die Anforderungen zutrifft, wurde aus der Perspektive eines Softwareentwicklers vorgenommen. Kann eine Anforderung so umgesetzt werden, dass sie konfigurierbar ist und diese Konfiguration an eine Anwendung oder das Betriebssystem kommuniziert werden kann, wurde sie als automatisierbar eingeschätzt. Konnte dies eindeutig nicht erfüllt werden, so wurde die Anforderung als nicht automatisierbar eingeschätzt. Eine teilweise Automatisierbarkeit von Anforderungen wurde ebenfalls berücksichtigt. Die initiale Einschätzung wurde im Rahmen einer Masterarbeit durchgeführt [Fab21] und vom Autor der vorliegenden Arbeit überarbeitet, sodass die Einschätzung durch zwei Experten erfolgte.

3.5 Ergebnisse der Analyse

Bei der Auswertung der drei IT-Sicherheitsnormen sind insgesamt 348 Anforderungen identifiziert worden. Abbildung 3.5 zeigt die Verteilung der Sicherheitsanforderungen nach Norm. Für die IEC 62443-4-2 wurden mit insgesamt 112 Anforderungen (35 %) die meisten identifiziert. Für die IEC 62443-3-3 sind es 99 Anforderungen (31 %) und für den BSI-Grundschutzbaustein für industrielle Steuerungsanlagen

62 Anforderungen (19 %). 47 Anforderungen (15 %) wurden in den ausgewählten Teilen 3, 4, 6, 7 und 8 der IEC 62351 identifiziert.

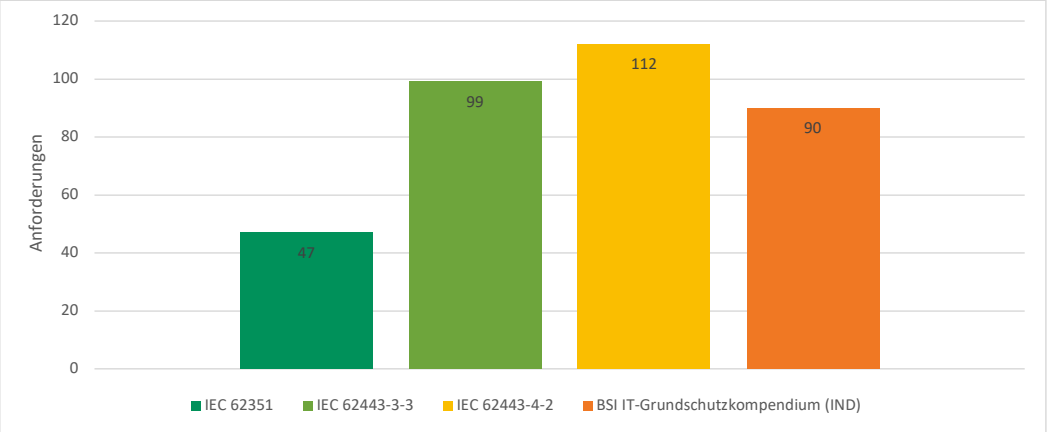

Abbildung 3.5.: Anzahl der identifizierten Anforderungen aufgeteilt nach Norm

Die IEC 62443 stellt mit den Teilen 3–3 (99 Anforderungen) und 4–2 (112 Anforderungen) 66 % der identifizierten Anforderungen und damit die meisten.

Kategorische Verteilung der Anforderungen

Die Verteilung der Anforderungen in den drei zuvor definierten Kategorien wird in Abbildung 3.6 dargestellt. Die Abbildung zeigt, dass 67 % der identifizierten Anforderungen auf den IEDs, 14 % der Anforderungen auf der Netzwerkebene umgesetzt werden und sich weitere 19 % an die Prozessebene richten. Es gibt Anforderungen, die im Bereich Netzwerk oder ebenfalls auf dem IED umgesetzt werden können. Da die Zuordnung zu den definierten Kategorien nicht immer präzise getrennt werden kann, kann eine Anforderung in mehreren Kategorien enthalten sein.

Kategorisierung der Anforderungen nach Herkunft

Im Rahmen der Untersuchung wurde somit festgestellt, dass die Normen die zuvor beschriebenen Kategorien unterschiedlich stark adressieren. Die Betrachtung der Menge der Anforderungen je Kategorie, aufgeschlüsselt nach den verschiedenen Normen, ist für die vorliegende Arbeit von Nutzen, um zu eruieren, ob eine Norm sich in besonderem Maße für das vorliegende Vorhaben eignet. Das Resultat dieser Auswertung ist in Abbildung 3.7 dargestellt. Sicherheitsanforderungen, die direkt auf einem IED umsetzbar sind, stammen mehrheitlich aus der Norm IEC 62443. Diese stellt mit den Teilen 3–3 und dem 4–2 allein 175 Anforderungen auf der

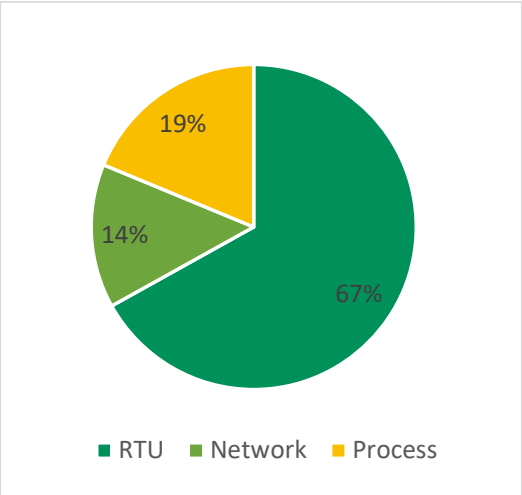

Abbildung 3.6.: Verteilung aller identifizierten Anforderungen gemäß den Kategorien

Ebene der IED. Die Norm IEC 62351 stellt hingegen 39 Anforderungen und der BSI-Grundschutzbaustein für Industrie 43 Anforderungen, die auf das IED abzielen.

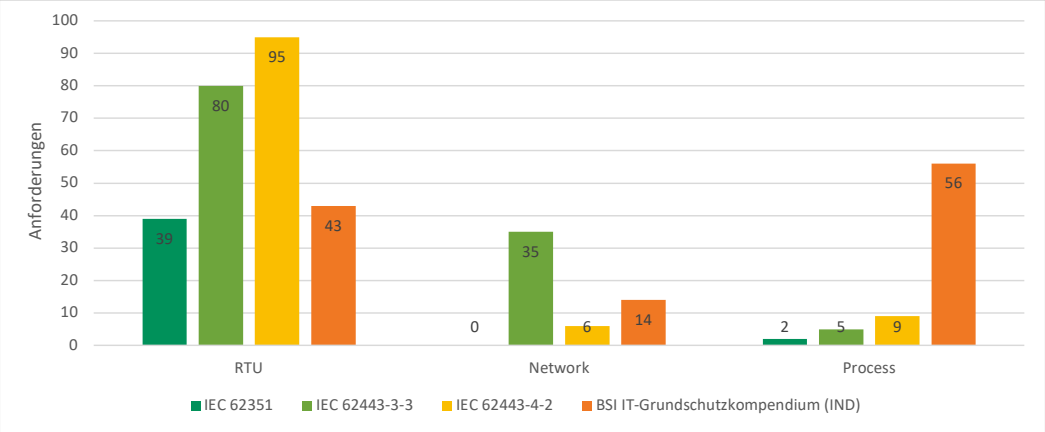

Abbildung 3.7.: Verteilung der kategorisierten Anforderungen, aufgeschlüsselt nach Normen

In der Abbildung ist ebenfalls ersichtlich, dass der IEC 62443-3-3 im Vergleich zu den anderen Normen ein Vielfaches an Anforderungen in der Kategorie Netzwerk aufweist. Dies ist insofern plausibel, als sich der Teil der Norm an die Betreiber des IED richtet und diese auch das Netzwerk absichern müssen, um das IED zu sichern. In der Kategorie Prozess stechen die Anforderungen des BSI-IT-Grundschutzkompendiums heraus, was den Zielen des Standards entspricht. Die in den jeweiligen Normen identifizierten IT-Sicherheitsanforderungen, die sich auf IEDs beziehen, übersteigen jeweils die Zahl von 30 Anforderungen und werden damit als ausreichend betrachtet. Dies verdeutlicht zudem, dass alle untersuchten Standards einen adäquaten Beitrag zu den Sicherheitsanforderungen an IEDs leisten und für die vorliegende Arbeit die

richtige Wahl darstellen, da die meisten darin beschriebenen Anforderungen für Endgeräte bzw. IEDs vorgesehen sind.

Automatisierte Abfragbarkeit

Neben der Quantität und der Verteilung der Sicherheitsanforderungen nach Wirkungsbereich ist zudem zu eruieren, inwiefern diese automatisierbar sind bzw. auf dem IED automatisiert abgefragt werden können. Von den insgesamt 348 identifizierten Anforderungen werden 257 der Kategorie IED zugeschrieben. Diese 257 Anforderungen wurden hinsichtlich der Automatisierbarkeit eingeschätzt. Die Abbildung 3.8 zeigt die Ergebnisse dieser Einschätzung. Die Abbildung veranschaulicht, dass 156 Anforderungen (61 %) in der Kategorie IED als automatisiert abfragbar bewertet wurden. Die Einschätzung einer teilweisen Automatisierbarkeit erfolgte für 79 Anforderungen (31 %). Die Einschätzung der Nicht-Automatisierbarkeit von 22 Anforderungen (8 %) bildet den Abschluss der Betrachtung. Die als automatisierbar

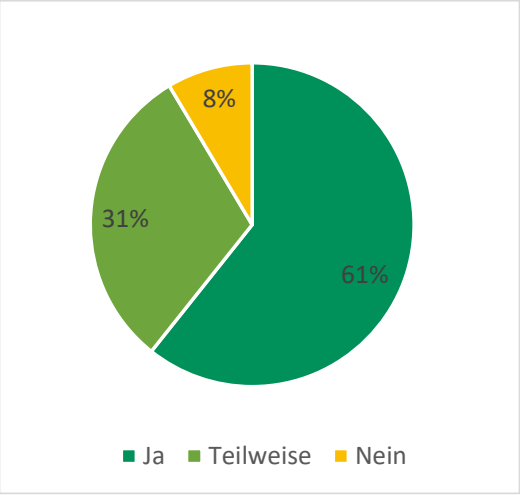

Abbildung 3.8.: Einschätzung der automatisierten Abfragbarkeit der Anforderungen

bewerteten Anforderungen lassen sich ebenfalls auf die betrachteten Standards verteilen. Die Verteilung dieser ist in Abbildung 3.9 dargestellt. Erkennbar ist, dass die meisten Anforderungen aus der IEC 62443 stammen, sowohl einzeln (Teil 3-3 und 4-2) als auch aggregiert betrachtet stellt der Standard fast zwei Drittel der Anforderungen, welche als auf Endgeräten automatisiert abfragbar eingeschätzt werden.

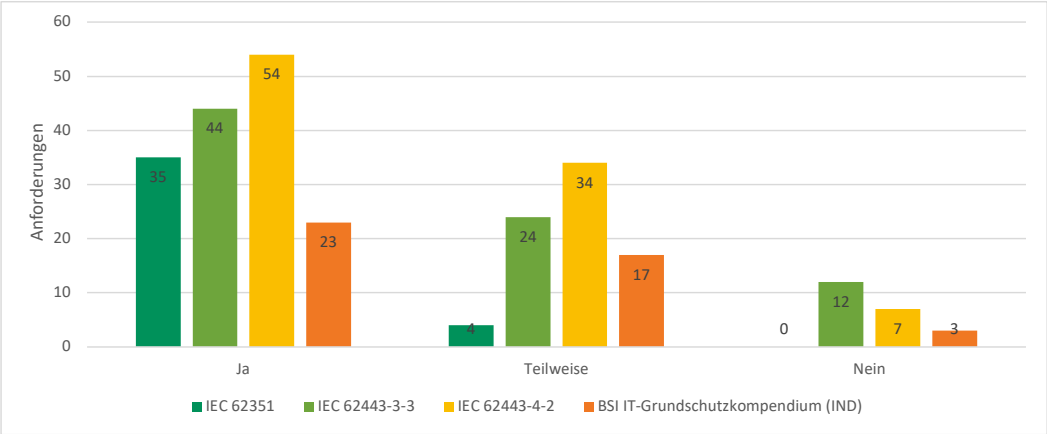

Abbildung 3.9.: Bewertung der Automatisierbarkeit der Anforderungen nach Norm aufgeschlüsselt

Kategorisierung der Sicherheitsanforderungen nach Grundanforderungen

Um thematische Schwerpunkte der Normen zu identifizieren und vergleichen zu können, wurden im weiteren Verlauf der Normenanalyse alle Anforderungen weiteren Sicherheitsbereichen zugeordnet. Dies ermöglicht die Identifikation von Schwerpunkten in den Sicherheitsbereichen der Normen und zeigt mögliche Unterschiede zwischen den Normen bzw. den quantitativ besonders adressierten Sicherheitsbereichen auf. Als Vorlage für die Kategorisierung wurden die sieben Grundanforderungen der IEC 62443-1-1 verwendet (FR, engl. Foundational Requirement), (siehe functional requirements in 3.3.1, IEC 62443). Die Teile IEC 62443-3-3 und IEC 62443-4-2 kategorisieren ihre Anforderungen bereits in diesen FRs. Dies erfolgt, da die FRs die Sicherheitsmerkmale der Informationssicherheit adäquat abdecken und mit der Norm bereits einem internationalen Konsens entsprechen. Im Anschluss erfolgt eine Zuordnung jeder Anforderung aus den anderen Normen und Standards zu einer FR.

Die Ergebnisse der Kategorisierung der Anforderungen in die FR der IEC 62443 sind in Abbildung 3.10 dargestellt. Auf der x-Achse sind die FR 1–7 und auf der y-Achse ist die jeweilige Anzahl der Anforderungen aufgetragen. Von den insgesamt 264 Anforderungen entfallen die meisten auf die Kategorie FR 3, Systemintegrität (74 Anforderungen). Die Kategorie FR 1, Identifikation und Authentisierung, stellt 56 Anforderungen. 55 Anforderungen sind der Kategorie FR 2, Nutzungskontrolle, zugeordnet. Wie die Abbildung ebenfalls zeigt, sind diese drei Kategorien am stärksten vertreten und stellen zusammen 185 von insgesamt 264 Anforderungen. Dies entspricht einer Gewichtung von 70 % und zeigt die Bedeutung dieser drei Kategorien. Die Kategorien FR 4–7 stellen insgesamt 79 Anforderungen, was 30 %

der Gesamtzahl entspricht. Dies sind im Einzelnen FR 4 (Vertraulichkeit der Daten) mit 12 Anforderungen, FR 5 (Eingeschränkter Datenfluss) mit 22 Anforderungen, FR 6 (Rechtzeitige Reaktion auf Ereignisse) mit 15 Anforderungen und FR 7 (Ressourcenverfügbarkeit) mit 30 Anforderungen.

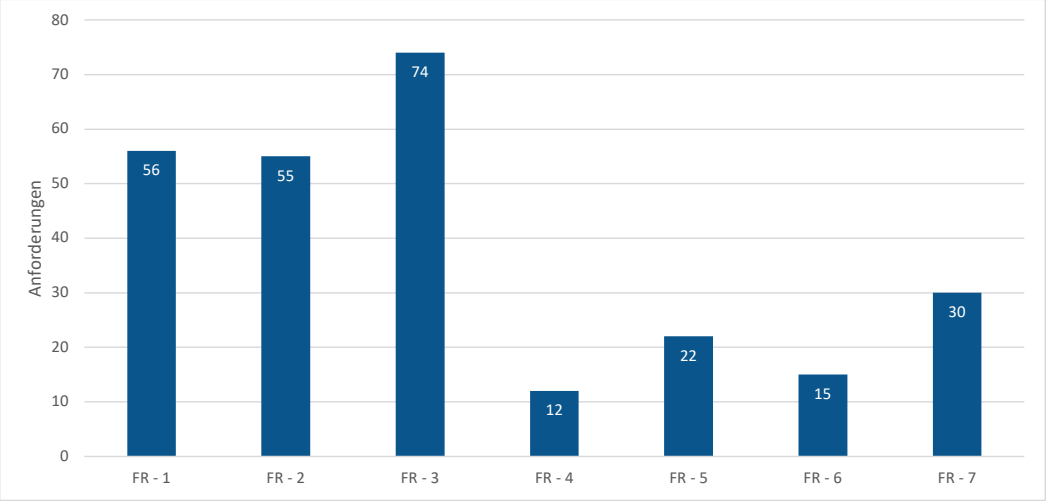

Abbildung 3.10.: Aggregation der automatisierbaren Anforderungen der Normen in Kategorien der funktionalen Anforderungen aus IEC 62443

Bei einer Betrachtung der kategorisierten Anforderungen nach ihrer jeweiligen Herkunft des Standards wird ersichtlich, dass alle Standards die Kategorie der Systemintegrität gleich hoch bewerten. Dort liegen die einzelnen Anforderungen nah beieinander. Die Abbildung 3.11 zeigt die Verteilung nach Standards. Darin ist erkennbar, dass die ausgewählten IEC-62443-Standards einen Fokus auf die Kategorien der Identifizierung und Authentifizierung sowie auf die Nutzungskontrolle legen und erst an dritter Stelle die Systemintegrität kommt. Ebenfalls stellt der IEC 62443 in den Kategorien FR 1 und FR 2 deutlich die meisten Anforderungen. Zwischen den Normen sind die Anforderungen bei der Systemintegrität ausgeglichen. Bei den ausgewählten Teilen des IEC 62351 konnten hingegen in den Kategorien der FR 4, 5 und 7 keine Anforderungen identifiziert werden.

3.6 Fazit und Diskussion

Im Rahmen der vorliegenden Untersuchung erfolgte die Vorstellung von drei IT-Sicherheitsnormen, welche im Rahmen von Recherchen identifiziert und ausgewählt wurden. Ein Auswahlkriterium war der internationale Konsens zu den Normen. Des

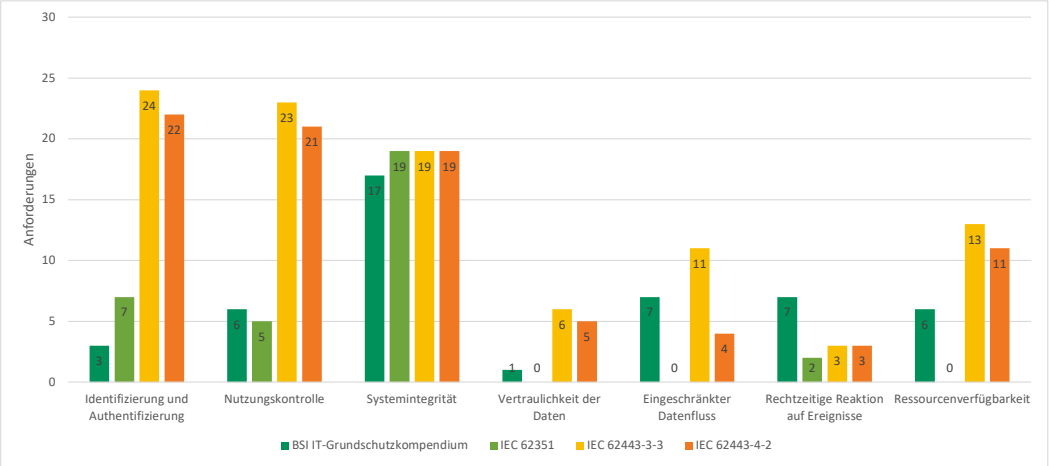

Abbildung 3.11.: Verteilung der Anforderungen aus den Normen auf die Kategorien der funktionalen Anforderungen (FR)

Weiteren wurden diese Normen ausgewählt, da sie in unterschiedlichen Publikationen als relevant für die Stromnetzarchitektur eingestuft wurden. Lokale Standards wurden aufgrund gesetzlicher Gegebenheiten dennoch berücksichtigt.

Zwischen den Normen sind Doppelungen hinsichtlich der Anforderungen oder der zu erreichenden Sicherheitsziele möglich. Diese wurden nicht näher identifiziert oder genauer betrachtet, da dazu ein inhaltlich tieferer und aufwendigerer Vergleich zwischen den Normen notwendig wäre. Für die vorliegende Arbeit hat dies keine Auswirkungen auf die weiteren Schritte, da mit der Identifikation der Anforderungen das Ziel für die vorliegende Arbeit bereits erreicht wurde.

Die quantitative Analyse hat ergeben, dass ausreichend viele IT-Sicherheitsanforderungen existieren, die sich technisch ausdrücken lassen und sich daher, nach Einschätzung zweier Experten, für die automatisierte Abfrage eignen können. Ein weiteres Ergebnis dieser Analyse ist, dass ein Großteil der Sicherheitsanforderungen der Kategorie Systemintegrität zuzuordnen ist (siehe Abbildung 3.10). Dieses Resultat unterstreicht und bekräftigt im Kontext der vorliegenden Arbeit die Relevanz der Plattformintegrität, was für die Integration von Trusted-Computing-Technologien spricht und bereits in der Einleitung motiviert wurde.

Aus der rein quantitativen Betrachtung der Anforderungen lassen sich weitere Aspekte ableiten, die im Gesamtkontext dieser Arbeit interessant sind. Diese werden in den folgenden Absätzen skizziert und diskutiert.

Anforderungen variieren quantitativ

Bei der Betrachtung der quantitativen Anforderungen wird ersichtlich, dass diese beim IEC 62443 deutlich umfangreicher sind als bei den anderen Normen. Dies kann zum einen darin begründet sein, dass die Normen jeweils nicht vollständig, sondern nur in den als relevant eingestuften Teilen analysiert wurden. Andererseits ist die IEC 62443 auch die jüngste IT-Sicherheitsnorm im Bereich der Automatisierungstechnik und spiegelt die Weiterentwicklung der Digitalisierung in diesem Bereich wider, wodurch sie neue Kommunikationsszenarien abdeckt. Als Beispiel dafür können die unterschiedlichen Sicherheitsmechanismen hinsichtlich der Authentifizierung bei Maschine-zu-Maschine-Kommunikation(M2M) und Mensch-zu-Maschine-Kommunikation angeführt werden. Außerdem scheinen im Rahmen der IEC 62443 die technisch verfügbaren Mittel deutlich weiter ausgeschöpft zu werden. So wird beispielsweise von Menschen eine 2-Faktor-Authentifizierung verlangt. Für die M2M-Kommunikation gelten hingegen andere Anforderungen. Ein weiteres Argument ist, dass die IEC 62351 rein für die Bedürfnisse des Energienetzes geschaffen wurde und auch Lösungen für spezifische Energienetzprotokolle bietet, die hier (mangels Relevanz) nicht abgebildet sind (z. B. Zustandsautomaten für GOOSE).

In der Betrachtung der Anforderungsdefinitionen zeigt sich, dass die IEC 62351, im Gegensatz zur IEC 62443, klare Forderungen an die konkrete technische Umsetzung bzw. Implementierungsanforderungen stellt. Die IEC 62443 und der BSI-IT-Grundschutz hingegen stellen Anforderungen auf einer abstrakteren Ebene dar. Daraus lassen sich zwei Schlussfolgerungen ableiten: Einerseits sind spezifisch-technische Anforderungen in Normen nur schwer mit der Realität vereinbar, wenn sie zu konkrete Anforderungen stellen. Dies ist darauf zurückzuführen, dass die Lebensdauer von Normen in der Regel deutlich länger ist als die von technischen Umsetzungen bzw. konkreten Sicherheitsmechanismen. Andererseits können diese konkreten Implementierungsanforderungen der IEC 62351 genutzt werden, um damit Anforderungen aus der IEC 62443 umzusetzen.

Ein letzter Aspekt bei der Betrachtung der Normen ist deren Anschlussfähigkeit an das aus der ISO 27001 geforderte ISMS. Die vorliegende Arbeit ist auch aus den Anforderungen der ISO 27001 motiviert, nämlich der Überwachung der IT-Sicherheitsmaßnahmen. Damit wird die Eignung der Anforderungen aus der IEC 62443 und dem BSI-IT-Grundschutz für die vorliegende Arbeit untermauert.

Zusammenfassung und nächste Schritte

Dieses Kapitel hat mit der quantitativen Analyse festgestellt, dass ausreichend Anforderungen an die IT-Sicherheit für IEDs vorliegen und diese als Konfiguration technisch umgesetzt werden können. Die durchgeführte Analyse hat damit das Ziel erreicht, für die vorliegende Arbeit Anforderungen an die IT-Sicherheit zu identifizieren, die als technische Konfiguration ausgedrückt und damit grundsätzlich automatisiert abgefragt werden können. Das Feststellen dieser Relevanz ist ein wichtiger Grundstein und Nachweis, auf dem die vorliegende Arbeit zur Beantwortung der Forschungsfrage weiter aufbauen kann.

Im folgenden Kapitel erfolgen eine Erweiterung der identifizierten Anforderungen zunächst um Plattformintegrität durch Trusted Computing sowie die Vorstellung eines Informationsmodells für das Energienetz, welches den Austausch der Sicherheitskonfigurationen im Energienetz ermöglicht. Damit wird die vorliegende Arbeit den in der Analyse identifizierten Schwerpunkt der Systemintegrität hinsichtlich der Forschungsfrage adressieren.

4 Informationsmodellelemente für Sicherheitskonfigurationsattribute in Stromnetzen

Anmerkung: Einige Teile dieses Kapitels, insb. die Modellierung der Remote Attestation in das IEC 61850, ist in der Publikation [Fra+23] bereits veröffentlicht worden. In diesem Kapitel wird auf den Erkenntnissen des vorherigen Kapitels aufgebaut und ein entsprechendes Informationsmodell erstellt, in dem die zuvor identifizierten Sicherheitsanforderungen strukturiert als Konfigurationen abgebildet werden. Dies ist die Voraussetzung für die ebenfalls in diesem Kapitel vorgestellte Modellierung dieses Informationsmodells im Stromnetz. Zusätzlich werden die Anforderungen der Remote Attestation (RA) beschrieben, um damit die Integration von Trusted-Computing-Technologien in das Energienetz zu berücksichtigen. Diese Anforderungen werden ebenfalls in ein Informationsmodell überführt, das mit der Referenzarchitektur des Energienetzes kompatibel ist bzw. eine nahtlose Integration ermöglicht. Damit werden die Erkenntnisse aus dem vorherigen Kapitel berücksichtigt und vertieft umgesetzt, da die Analyse einen Fokus der Anforderungen auf der Systemintegrität gezeigt hat.

Im Folgenden werden zunächst verwandte Arbeiten sowie der aktuelle Stand der Technik zum Thema Informationsmodelle zum Datenaustausch im Bereich der IT-Sicherheit vorgestellt. Im Anschluss erfolgt eine Betrachtung der Möglichkeit innerhalb der Referenzarchitektur zur Übertragung von Daten von einem IED in das Controlcenter, um darauf aufbauend ein Informationsmodell für die SKI aus dem vorigen Kapitel unter Verwendung vom Smart Grid Architecture Model (SGAM) zu erstellen.

Im weiteren Verlauf erfolgt eine Abbildung der Anforderungen in ein gemeinsames Informationsmodell, welches zunächst methodisch eruiert wird. Danach wird das Thema der Remote Attestation mittels Trusted-Computing-Methoden behandelt. Dabei wird insbesondere auf die Integration der Remote Attestation in die Referenzarchitektur des Stromnetzes und die daraus resultierenden Anforderungen eingegangen.

4.1 Informationsmodell für Sicherheitskonfigurationen

In dieser Sektion wird das eigens erstellte Informationsmodell für die SKI vorgestellt. Es basiert auf den Erkenntnissen aus dem vorherigen Kapitel. Das Informationsmodell für SKI dient dazu, die Informationen aus den Anforderungen zu strukturieren und als einheitliches und zentrales Modell bereitstellen zu können. Das Informationsmodell stellt damit die Grundlage für eine weitere Integration in die bestehenden Informations- und Datenstrukturen der Referenzarchitektur der TC57 Power System Architecture Model. Darauf aufbauend wird das Informationsmodell verwendet, um die Integration praktisch zu demonstrieren. Mit dem Informationsmodell für SKI wird eine Lücke geschlossen, da bisher kein Informations- oder Datenmodell für die Abbildung von Sicherheitskonfigurationen vorhanden war.

Eine grundsätzliche Schwierigkeit besteht darin, dass die Anforderungen aus den Normen zum einen in natürlicher Sprache geschrieben sind und die Normen zum anderen untereinander nicht auf demselben technischen Detaillevel arbeiten.

4.1.1 Anforderungen an das Informationsmodell

Das Informationsmodell hat zum Ziel, die potenziellen Konfigurationen einer Anforderung abzubilden und zudem eine eindeutige Referenzierung des Norm- bzw. Anforderungsgebers zu ermöglichen. Zu diesem Zweck soll eine Anforderung im Informationsmodell einen Metabereich und einen Konfigurationsbereich enthalten. Dies ist in Abbildung 4.1 dargestellt. Der Metabereich dient der eindeutigen Zuordnung der Anforderung zu einer Norm bzw. dem Anforderungsgeber. Im Konfigurationsbereich sollen die technischen Konfigurationen hinterlegt werden. Im Gegensatz zum Metabereich muss der Konfigurationsbereich des Informationsmodells mit komplexen Konfigurationsmöglichkeiten umgehen können und daher die Flexibilität aufweisen, unterschiedliche noch nicht bekannte technische Einstellungen abbilden zu können. Einige Anforderungen sind technisch bereits konkret spezifiziert, andere Anforderungen wiederum sind vage und offen formuliert und ermöglichen (bewusst) diverse technische Möglichkeiten zur Erfüllung einer Anforderung. Bei der IEC 62443 sind keine (direkten) technischen Anforderungen an die Konfigurationen genannt, sondern Anforderungen an die Sicherheitsfunktionen gestellt, deren Ausgestaltung nicht vorgegeben ist. Diese Anforderungen beziehen sich oft auf die Anwesenheit einer Sicherheitsfunktion, deren genaue Konfiguration oder technische Ausprägung nicht beschrieben ist. Die Anforderungen sind abstrakter und lassen unterschiedliche Lösungswege bzw. Lösungsmittel zu. Das Informationsmodell wird im Kontext der

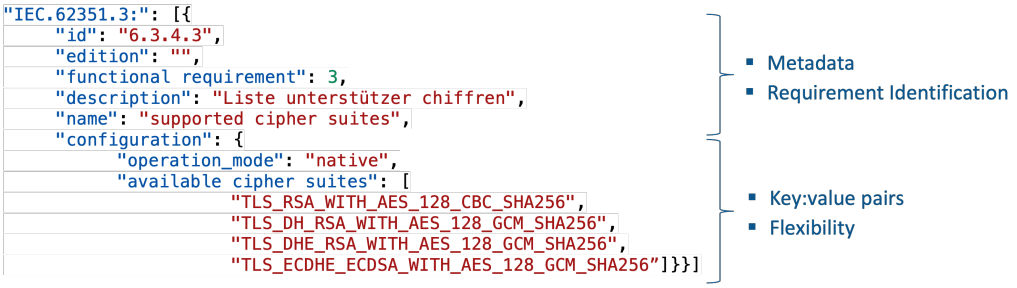

Abbildung 4.1.: Beispielhafte Abbildung der Anforderungen in JSON-Notation, eigene Darstellung

TC57 Power System Architecture Model-Referenzarchitektur bereitgestellt mit dem Ziel, Daten aus der Unterstation (Substation) in das Controlcenter zu transportieren. Um auch der Idee der nahtlosen Integrationsarchitektur (sog. seamless integration architecture) in der TC57 Power System Architecture Model gerecht zu werden, ist es erforderlich, das Informationsmodell mit den vorgesehenen Kommunikationsmitteln der TC57 zu übertragen. Dabei ist darauf zu achten, dass die Kompatibilität und Protokollunabhängigkeit gewährleistet bleiben.

4.1.2 Herausforderungen

Bei der Betrachtung der Normen sind zwei Herausforderungen hervorzuheben: Zum einen sind die Sicherheitsanforderungen (größtenteils) in natürlicher Sprache geschrieben und zum anderen beschreiben unterschiedliche Normen die Anforderungen in unterschiedlicher technischer Tiefe. Zudem beinhalten die betrachteten Normen auch keinerlei technisches Informationsmodell. Als Ausnahme ist zu erwähnen, dass in der Norm IEC 62351-7 im Rahmen der Netzwerkobjekte Management Information Bases (MIBs) definiert werden, die genutzt werden können, um beispielsweise physikalische Netzwerkunterbrechungen, das Erkennen unbefugten Zugriffs, Denial of Service (DOS)-Angriffe und andere, vor allem netzwerkspezifische Ereignisse übertragen zu können [Nor19b]. Es existiert daher kein Informationsmodell für eine maschinelle Verarbeitung der Sicherheitsinformationen. Um diese Lücke zu schließen, werden in der vorliegenden Arbeit einzelne Anforderungen aus den vorgestellten Normen exemplarisch betrachtet, über das vorgestellte Informationsmodell in greifbare Datenmodelle überführt und anhand der beiden folgenden Beispiele verdeutlicht.

Das erste Beispiel wurde so ausgewählt, dass die Problemstellung verständlich vorgestellt werden kann. Die Anforderung stammt aus der IEC 62351-3, diese be-

schreibt unter Punkt 6.3.4.3 technisch spezifische Anforderungen für die Chiffren der Verbindungen mit Transport Layer Security (dt. Transportschichtverschlüsselung) (TLS) im „nativen Betriebsmodus“ (IEC 62351-3). Der Betriebsmodus „nativ“ ist eine Eigenheit aus der IEC 62351 und gehört nicht unmittelbar zu TLS selbst. Vorgeschrieben werden an dieser Stelle vier unterschiedliche Chiffren. Eine Möglichkeit, wie diese genannte Sicherheitsanforderung als technische Konfiguration im Sinne der vorliegenden Arbeit ausgedrückt werden kann, ist in Skript 4.1 als JavaScript Object Notation (JSON) gezeigt. Das darin befindliche Konfigurations-Objekt (configuration) enthält zwei weitere Objekte, die den Betriebsmodus abbilden (operation_mode) und die vorhandenen Chiffren als Array darstellen.

```
{
"configuration": {
    "operation_mode": "native",
    "available_cipher_suites": [
        "TLS_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_DH_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
        ]
    }
}
```

Skript 4.1: Beispiel einer Sicherheitsanforderung als technische Konfiguration

Wenn es notwendig ist, kann das Konfigurations-Objekt um ein weiteres Schlüsselattribut erweitert werden. Soll zum Beispiel noch ergänzt werden, für welche TLS-Version oder Verbindung diese Konfiguration gilt, können diese Informationen angefügt werden.

Das zweite Beispiel stammt aus der IEC 62443-4-2 und wurde ausgewählt, um die Vielfältigkeit der Umsetzungsmöglichkeiten einer Anforderung zu zeigen, die durch flexible Konfiguration abgebildet werden muss. Dieses Beispiel beschreibt eine Sicherheitsfunktionalität, die fordert, dass die Komponenten die Fähigkeit aufweisen, menschliche Nutzer eindeutig zu identifizieren und zu authentifizieren. Diese Anforderung lässt viel Spielraum in ihrer Auslegung. Hierbei könnten biometrische Authentifizierungsverfahren verwendet werden, bei denen es wiederum unterschiedliche Möglichkeiten gibt, bspw. retinabasierte, bei denen eine spezielle Kamera die Retina im Auge des Nutzers scannt und dieses als biometrisches Merkmal verwendet. Eine weitere Möglichkeit der Umsetzung besteht über einen Fingerabdrucksensor, welcher Fingerabdrücke als biometrisches Merkmal nutzt. In Skript 4.2 wird eine mögliche Beispielkonfiguration für die retinabasierte Umsetzung gezeigt, wobei auch gleichzeitig die Möglichkeit weiterer Einstellungen der retinabasierten Konfiguration

vorhanden sein muss. Um dies zu erreichen, wurde hier beispielhaft in Zeile 7 ein weiteres Array eingefügt. Mit diesem Beispiel soll verdeutlicht werden, dass eine Anforderung mit unterschiedlichen Varianten umgesetzt werden kann und daher divergente Konfigurationen möglich sind. Um genau diese Breite an Umsetzungs- und Konfigurationsmöglichkeiten in einem Informationsmodell abzubilden, wird im folgenden Abschnitt ein dafür passendes Informationsmodell vorgestellt.

```
1  ...
2      {
3          "configuration": {
4              "has identification": true,
5              "method": "biometric",
6              "type": "retina",
7              "settings": [
8                  "key": "value",
9                  ...
10             ]
11         }
12     }
```

Skript 4.2: Beispiel einer Sicherheitsanforderung für biometrische Authentifizierung

4.1.3 Informationsmodell für Sicherheitskonfigurationsinformationen

Um die Anforderungen aus den Normen abzubilden, wurde ein Informationsmodell als UML-Diagramm modelliert. Die Abbildung 4.2 zeigt den Aufbau. Eine Sicherheitsanforderung setzt sich aus verschiedenen eigenen deskriptiven Attributen zusammen. Die unterschiedlichen Attribute dienen der Identifikation einer Anforderung innerhalb eines Standards und verfügen darüber hinaus über weitere Metainformationen. Die technischen Konfigurationsattribute werden als Array eingefügt und bestehen aus Key-Value-Paaren. Die Attribute werden im Folgenden erläutert. Ausgehend von der (Klasse) Sicherheitsanforderung werden die wichtigsten Attribute im Folgenden kurz beschrieben:

- **Standard_Identifikator:** Referenziert die Norm, aus der die Sicherheitsanforderung stammt. Der Aufbau dieses Attributs ist in der Klasse „Standard“ definiert. Eine Norm oder ein Standard lässt sich in der Regel klar identifizieren durch folgende Attribute: Name (oder Bezeichner), Titel, Untertitel, Version sowie Herausgeber des Standards bzw. im Falle einer Norm die Institution, die die Norm angenommen hat (z. B. IEC), eine Bezeichnung (z. B. 62443) und das Erscheinungsdatum. Die Klasse Standard kann ebenfalls um weitere Attribute ergänzt werden.

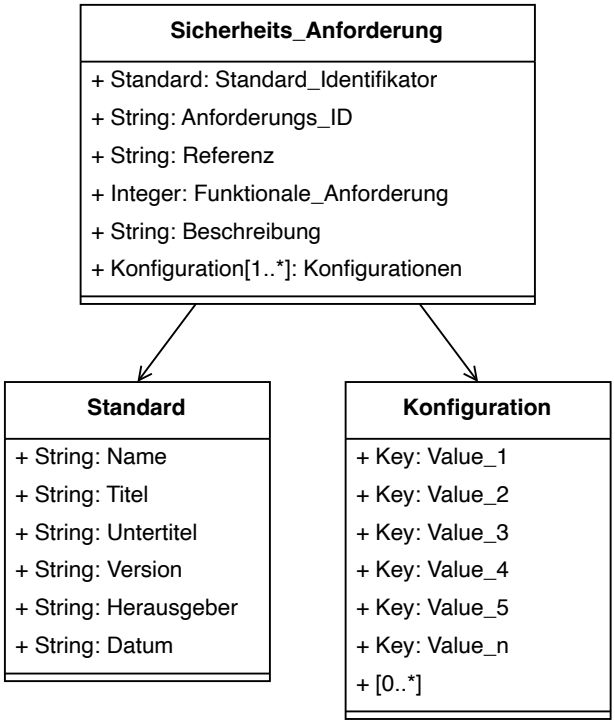

Abbildung 4.2.: UML-Darstellung des neuen Informationsmodells für Sicherheitskonfigurationsinformationen (SKI)

- **Referenz**: Referenziert die Anforderung innerhalb der Norm durch die Kapitelnummer. Bei Bedarf kann diese durch die Angabe der Absatznummer erweitert werden. Dies ist insbesondere dann von Vorteil, wenn unter einer Kapitelnummer mehrere Anforderungen definiert werden. Das Zählen der Absätze beginnt bei eins. Die Referenz soll es ermöglichen, die jeweilige Anforderung innerhalb der Norm / des Standards zu identifizieren.

- **Funktionale Anforderung**: Beschreibt, zu welcher Sicherheitsfunktionsklasse eine Anforderung gehört. Als Vorgabe gelten die sogenannten Functional Requirements der Norm IEC 62443-3-3 (siehe Kapitel IEC 62443). Das Attribut stellt sicher, dass Sicherheitsanforderungen kategorisiert werden können.

- **Beschreibung**: Soll die eigentliche Anforderung beschreiben, so wie sie in der Norm / dem Standard gefasst ist. Da dies aus urheberrechtlichen Gründen nicht immer möglich ist oder die Anforderungsbeschreibung zu umfangreich ist, kann sie auch gekürzt hinterlegt werden. Es wird das Ziel verfolgt, Hintergrundinformationen zur besseren Einordnung verfügbar zu machen.

- **Konfiguration:** Das Attribut „Konfiguration“ bildet die technischen Konfigurationen ab. Daher sind diese als Array definiert und können mehrere Konfigurationsobjekte beinhalten. Ein Konfigurationsobjekt wird in der Klasse „Konfigurationen“ als Key-Value-Paar beschrieben und ermöglicht ebenfalls Arrays und Datentypen wie int, string, date, number. Auch Verschachtelungen sind zulässig und ermöglichen es, technische Konfigurationen als Unified Modelling Language, dt. einheitliche Modellierungssprache (UML) zu modellieren, darzustellen und beispielsweise als JSON umzusetzen. An dieser Stelle ist die Integration der Sicherheitsanforderungen der Standards am unterschiedlichsten, weil nicht jede Norm in gleicher technischer Tiefe die Sicherheitsanforderungen beschreibt.

4.2 Informationsmodellierung im Smart Grid

Um das zuvor vorgestellte Informationsmodell in das Smart Grid bzw. in die Kommunikationsarchitektur der Referenzarchitektur der TC57 Power System Architecture Model zu integrieren, ist ein Architekturmodell hilfreich. Der Informations- und Datenaustausch im Energienetz ist ein komplexes und vielschichtiges Umfeld, da eine Vielzahl von Akteuren, Systemen und Geräten und verschiedene Datenprozesse von kritischen Informationen wie z. B. Schutzabschaltungen bis hin zur Rechnungsstellung beteiligt sind. Daher ist die Daten- und Informationsübertragung trotz Referenzarchitektur eine komplexe Herausforderung. Es gilt unterschiedliche Anforderungen zu berücksichtigen, da eine Vielzahl von Akteuren beteiligt ist. Zudem sind neue Anwendungsfälle in der Regel nicht oder nur abstrakt in die Referenzarchitektur eingebettet. Ein methodischer Ansatz zur Modellierung von Kommunikationswegen zum Daten- und Informationsaustausch in der Systemarchitektur des Energienetzes ist das sogenannte SGAM. Dieses wird im Folgenden vorgestellt und der für vorliegende Arbeit benötigte Daten- und Informationsaustausch damit modelliert. Mit SGAM leiten sich Kommunikationsstrecken und Protokolle ab, die präsentiert werden, zum vorherigen Informationsmodell passen und für die Ziele dieser Arbeit geeignet sind.

4.2.1 Smart Grid Architecture Model (SGAM)

Das vom Europäisches Komitee für elektrotechnische Normung, französisch: Comité Européen de Normalisation Électrotechnique (CENELEC) herausgegebene und im

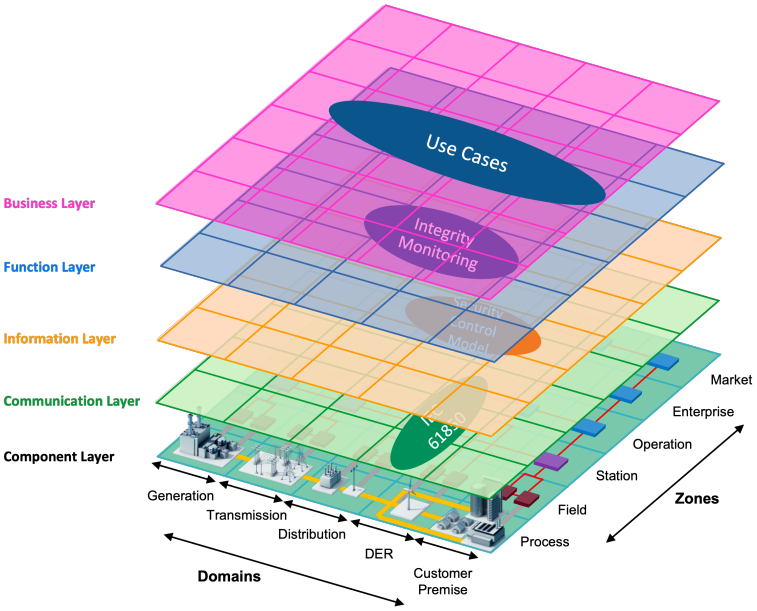

Abbildung 4.3.: Smart Grid Architecture Model mit Projektion der Anwendungsfälle, Ursprungsquelle: [Leh22]

SGAM-Handbuch [GG14] beschriebene SGAM ist eine Zonenabbildung der hierarchischen Ebenen des Netzmanagements. Diese Zonen spiegeln ein hierarchisches Modell wider, das das Konzept der Aggregation und der funktionalen Trennung im Energieversorgungsmanagement berücksichtigt. SGAM wurde ursprünglich mit dem Ziel entwickelt, Standardisierungslücken in Smart-Grid-Architekturen [GG14] zu identifizieren. Mittlerweile hat es sich etabliert, damit Anwendungsfälle zu modellieren, um zu überprüfen, wo welche Lücken in der Informationskette bestehen. Für diesen Fall wird SGAM in der vorliegenden Arbeit verwendet und darauf abgebildet. Die Abbildung 4.3 zeigt die verschiedenen Ebenen und Zonen. Diese werden im Folgenden zusammen mit einer Einordnung der einzelnen Aspekte der vorliegenden Arbeit beschrieben.

Die mehrdimensionalen Ebenen stellen die hierarchischen Netzübergänge dar. Auf der x-Achse befinden sich die verschiedenen Domänen, also Energieerzeugung (Generation), das Übertragungsnetz (Transmission), das Verteilnetz (Distribution) sowie die verteilten Energieerzeuger (DER) und schließlich die Kunden bzw. die Prosumer-Domäne.

Entlang der y-Achse befinden sich die beteiligten Zonen, hervorzuheben ist oberste Ebene (Business-Layer), wo die bereits vorgestellten Anwendungsfälle (Use Cases) verortet sind (siehe Abschnitt 1.1). Auf dem Function-Layer befindet sich das technische Monitoring, welches die Sicherheitskonfigurationsinformationen verarbeiten

und aufbereiten kann, um z. B. die Daten weiterleiten, visualisieren oder auch direkt mit den geforderten Sicherheitseinstellungen aus den Standards abgleichen zu können.

Die vorliegende Arbeit konzentriert sich auf den Bereich der darunter liegenden Informationsschicht (Information-Layer), da es für die Anwendungsfälle primär um die Bereitstellung von Informationen geht. Auf dieser Schicht wird das notwendige Informationsmodell abgebildet, um für die vorliegende Arbeit Sicherheitskonfigurationsinformationen abstrahiert, strukturiert und einheitlich bereitstellen zu können. Auch die Abbildung der dafür notwendigen Strukturen wird auf dieser Schicht definiert.

Darunter befindet sich die Kommunikationsschicht (Communication-Layer), welche die Modellierung und Identifikation der Kommunikationsprotokolle abbildet, die einerseits das Informationsmodell praktisch instanziieren können (Datenmodell) und andererseits auch mit der darunter liegenden Komponentenschicht (Component-Layer) kompatibel sind.

Hier befindet sich die „Hardware“ (sog. Primärtechnik) des Stromnetzes, die Informationen von Sensoren und Aktoren zur Verfügung stellt. Auf der Komponentenschicht sind auch die unterschiedlichen Domänen (Domains) abgebildet und können über das SGAM auf die jeweiligen Zonen (Zones) abgebildet werden. Dies ist ein wichtiger Aspekt, da dies auf jeder Schicht unterschiedlich dargestellt wird und sich daraus verschiedene Anforderungen ergeben können.

Für den allgemeinen Anwendungsfall zur Abfrage von Sicherheitskonfigurationen werden zwei Informationsobjekte benötigt: Das erste Objekt dient der Remote Attestation und das zweite stellt die eigentlichen Sicherheitskonfigurationen zur Verfügung.

Auf der Informationsschicht wurde das Datenmodell erstellt, da für die benötigten Informationsobjekte kein passendes Datenmodell gefunden werden musste. Auf der Kommunikationsschicht (Communication-Layer) wurde die IEC 61850 definiert. Die IEC 61850 wurde in einem Suchprozess herauskristallisiert, um sowohl auf der Komponentenschicht als auch mit dem Datenmodell interagieren zu können. Dies wird in einem späteren Abschnitt erläutert.

Die für die Anwendungsfälle (siehe Abschnitt 1.1) notwendigen Informationen auf der Funktionsschicht konnten innerhalb der Architektur der TC57 Power System Architecture Model nicht identifiziert werden und werden deshalb für die vorliegende Arbeit entwickelt und in einem Demonstrator umgesetzt. Dies ist zum einen ein Datenmodell, um den Informationsaustausch für die Remote Attestation zu

ermöglichen. Zum anderen handelt es sich um Datenobjekte, die die Informationen der Sicherheitskonfigurationen bereitstellen können.

4.2.2 Protokollauswahl

Die weitere Modellierung der vorliegenden Arbeit mittels SGAM betrachtet vorrangig die Kommunikationsstrecke und ist in Abbildung 4.4 dargestellt. Diese Abbildung zeigt den Kommunikationspfad, der für die Ziele der vorliegenden Arbeit benötigt wird. Der eingezeichnete grüne Pfeil zeigt auf, über bzw. zwischen welchen Bereichen die Kommunikation stattfinden muss. Der Fokus liegt auf der Fernwirktechnik im Verteilnetz. Dezentrale Energieerzeugungsanlagen sind ebenfalls eingezeichnet, da diese teilweise Protokollüberschneidungen aufweisen und zeigen, dass die Anwendungsfälle und der Ansatz der vorliegenden Arbeit auf andere Bereiche übertragbar sind.

Das Kommunikationsprotokoll nimmt eine wichtige Rolle ein, da es in der Lage sein muss, objektorientierte bzw. hierarchische Datenstrukturen abzubilden und zu erweitern. Gleichzeitig soll die Realisierung der Kommunikationsverbindung mit bestehenden Protokollen der Referenzarchitektur der TC57 Power System Architecture Model erfolgen. Auf der Prozessebene (unten) ist als Kommunikationseinheit für die Fernwirktechnik eine IED vorgesehen, die ein Informationsmodell bereitstellen soll, sodass auf Betriebs- und Unternehmensebene (Operations- und Enterpriseebene) die Sicherheitskonfigurationsinformationen und Datenobjekte bereitgestellt werden können. Der Fokus liegt primär auf dem Verteilnetz, da die zur Verfügung stehenden Kommunikationsprotokolle teilweise auch für dezentrale Erzeugungsanlagen eingesetzt werden können. Daher wurde auch deren Kommunikationsstrecke dargestellt. Die Referenzarchitektur der TC57 bietet für die Kommunikationsverbindung zwischen Substation (Schichten Prozess bis Station) und Controlcenter (Schichten Operation bis Markt) unterschiedliche Kommunikationsprotokolle an, die bereits in der Abbildung 2.2 (siehe Kapitel Intelligentes Stromnetz) gezeigt wurden. Für diese Arbeit wurden zwei Kommunikationswege in Betracht gezogen:

1. Der Informationsaustausch und die Datenübertragung mit der Norm IEC 61850, da es eine hierarchische Datenmodellierung ermöglicht und im SGAM von der Prozesstechnik bis zum Controlcenter kompatibel ist. Über das CIM ist auch eine Schnittstelle zur Enterprise-Schicht vorhanden.

2. Der Informationsaustausch aus der Perspektive des IT-Netzwerkmanagements: Die Möglichkeiten der IEC 62351 wurden betrachtet und der Einsatz vom Simple Network Management Protocol (SNMP) wurde untersucht.

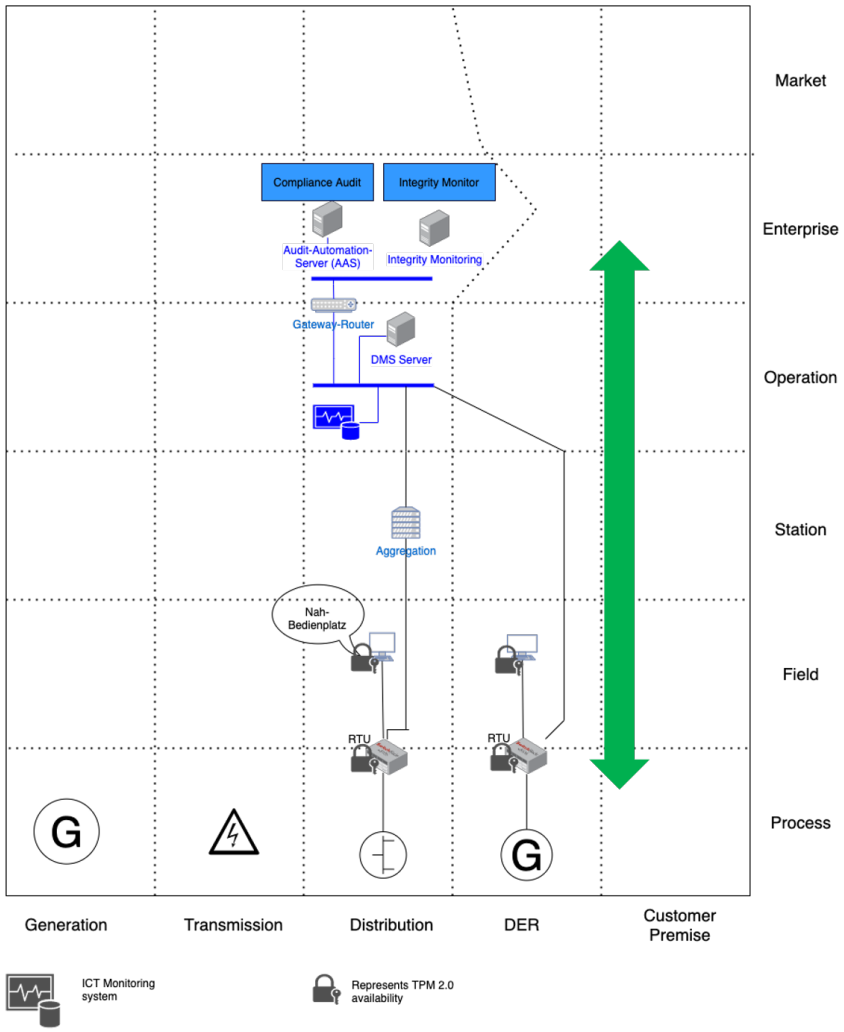

Abbildung 4.4.: Vorgesehene Kommunikationsstrecke in SGAM-Darstellung

4.2.3 Betrachtung der IEC 61850

Die Betrachtung der Norm IEC 61850 für die definierten Anwendungsfälle ist naheliegend. Die dort spezifizierten Informations- und Datenmodelle sowie Kommunikationsprotokolle sind im Bereich der SCADA bzw. OT angesiedelt. Ursprünglich für die Kommunikation zwischen IED in Unterstationen (via GOOSE) entwickelt, wurde der Anwendungsbereich stetig erweitert. Inzwischen kann die IEC 61850 auch für die Fernwirktechnik eingesetzt werden und verwendet für die Kommunikation auf den Schichten der Open Systems Interconnection (OSI) das MMS-Protokoll. Die IEC 61850 definiert auch Informations- und Datenmodelle, wie sie bereits in Kapitel IEC 61850 vorgestellt wurden. Dieses hierarchische, an die Objektorientierung angelehnte Informationsmodell ist erweiterbar, CIM-kompatibel und ermöglicht

somit die Datenbereitstellung auf Unternehmensebene. Dies ist für die Realisierung der Anwendungsfälle der vorliegenden Arbeit von Vorteil, da die Informationen auf direktem Weg bereitgestellt, weiterverarbeitet und übertragen werden können und die Anwendungsfälle die Daten bzw. Informationen auf der Enterprise- bzw. Geschäftsebene benötigen (siehe Abbildung 4.3 und 4.4).

Ein weiterer Punkt, der für die Verwendung der IEC 61850 in diesem Zusammenhang spricht, ist die Anbindung an die DER, wodurch die Anwendungsfälle dieser Arbeit direkt auf andere Bereiche übertragbar sind und nicht nur für den Bereich der Unterstationen im Verteilnetz gelten. Darüber hinaus zählt die IEC 61850 zu den Kernprotokollen innerhalb des TC57 Power System Architecture Model und wird für zukünftige Szenarien genutzt, wie zum Beispiel die Einbindung von elektrisch betriebenen Autos (E-Autos) in die aktive Laststeuerung [US19].

Die IEC 61850 ist, wie bereits erwähnt, primär für die Kommunikation und Datenübertragung des SCADA-Bereichs entwickelt worden und dafür ausgelegt, Messdaten und OT-spezifische Informationen zu übertragen. Aus dem Blickwinkel des IKT-Netzwerkmanagements ist eine Betrachtung des Protokolls Simple Network Management Protocol (SNMP) als Übertragungsprotokoll samt der existierenden Datenmodelle interessant und wird im nächsten Abschnitt behandelt.

4.2.4 Betrachtung des Simple Network Management Protocols

Die Umsetzung von Sicherheitsmaßnahmen wird in der TC57-Referenzarchitektur als Querschnittsaufgabe entlang einer Vielzahl grundlegend unterschiedlicher Ebenen und Bereiche dargestellt. Die Norm IEC 62351 beschreibt die IT-Sicherheit in Energiemanagementsystemen und den damit verbundenen Datenaustausch. Sie legt Maßnahmen und Anforderungen an die Kommunikation fest, mit denen die Grundsätze der Informationssicherheit (u. a. Vertraulichkeit, Datenintegrität, Authentifizierung und Nichtabstreitbarkeit) umgesetzt werden. Die IEC 62351 bietet auch typische Möglichkeiten aus dem Bereich der IKT-Überwachung (Monitoring) an, um sicherheitsrelevante Informationen zu übertragen und auszutauschen. Dieser Informationsaustausch findet allerdings primär im Bereich des IKT-Netzwerkmanagements statt und wird grundsätzlich für den Betrieb des IKT-Netzwerks genutzt und nicht auf der Applikationsebene der Energienetzleittechnik bzw. Fernwirktechnik. Dies wird auch in der Abbildung der bereits in Kapitel 2.1.1 vorgestellten Referenzarchitektur der Kommunikationsprotokolle deutlich. Dort ist auf der rechten Seite die IEC 62351 parallel zur OT dargestellt (siehe Abbildung 2.2). Neben den SCADA-typischen

Kommunikationsprotokollen der Referenzarchitektur des TC57 Power System Architecture Model werden in der IEC 62351 auch Kommunikationsprotokolle aus dem Bereich des (IKT-)Netzwerk- und Systemmanagements (NSM) verwendet. Beispielsweise werden in Teil 7 der IEC 62351 Datenmodelle für NSM definiert, mit dem Ziel, eine informationstechnische Struktur für SCADA-Systeme in der Energieversorgung zu erhalten, die den Gesundheitszustand von allen Netzwerkkomponenten – auch IEDs – erfasst und damit einen ganzheitlichen (IKT-Netzwerk-)Überwachungsansatz schafft. Die Norm bezieht sich dabei auf das SNMP, ohne dieses als obligatorisch zu bezeichnen.

Das Simple Network Management Protocol (SNMP), das primär für das Netzwerkmanagement erfunden wurde, hat bereits eine lange Historie. Ursprünglich wurde das Protokoll auch für die Fernkonfiguration von Routern und Switches verwendet, wird allerdings heutzutage unter anderem aufgrund der als unsicher geltenden Protokolle kaum noch für diese Zwecke verwendet. Obwohl die Übertragungssicherheit in verschiedenen Versionen verbessert wurde, wird SNMP hauptsächlich zur Überwachung von IKT-Netzen und deren Komponenten eingesetzt [DH08, S. 98]. Hier dient es vor allem zur Überwachung der Funktionsfähigkeit von Netzwerken, beispielsweise durch die Erkennung von Portausfällen, Lüfterausfällen und anderen Störungen an IKT-Netzwerkkomponenten.

Aufgrund der Fähigkeiten und der Historie von SNMP wurde vermutet, dass Informationen über allgemeine Konfigurationsanforderungen für IT-Sicherheit möglicherweise bereits in großem Umfang vorhanden sind und über SNMP direkt genutzt werden können. Ein Vorteil von SNMP wären bestehende, international standardisierte Daten- und Informationsstrukturen und der Zugriff darauf. Damit wäre der Zugriff auf die Informationsobjekte bereits gegeben bzw. teilweise vorhanden, und diese Synergien hätten für die vorliegende Arbeit genutzt werden können, um die Bereitstellung dieser Informationen zu realisieren. An dieser Stelle ist anzumerken, dass die Referenzarchitektur des TC57 Power System Architecture Model nicht alle Kommunikationsprotokolle enthält, sondern hauptsächlich den Daten- und Informationsaustausch des OT-Bereichs betrachtet. Eine Realisierung mittels SNMP wurde im Rahmen einer Masterarbeit untersucht [Fab21]. Dabei wurde betrachtet, welche Anforderungen an technische Konfigurationen der genannten Normen als Informationsobjekte für SNMP verfügbar sind. Im Ergebnis konnten nur wenige Informationen über SNMP bezogen werden. Dies liegt darin begründet, dass sich die Suche nach Informationsobjekten für SNMP schwieriger gestaltet, als zunächst vermutet wurde. Zwar ist eine Vielzahl von Informationen über die ISO standardisiert, jedoch entweder schwer recherchierbar oder möglicherweise herstellerspezifisch und daher nicht mehr in öffentlich zugänglichen Verzeichnissen enthalten. Die Abschlussarbeit

hat damit einmal mehr den Mangel an (standardisierten) Informationsobjekten für Sicherheitskonfigurationen aufgezeigt.

Unabhängig vom Ergebnis kann zusammenfassend festgehalten werden, dass eine SNMP-Datenübertragung den Nachteil hat, dass die Daten für die vorgestellten, weitreichenden Anwendungsfälle nicht optimal gewesen wären. Dies liegt vor allem daran, dass die Informationen zu sehr auf der Ebene des (IKT-)Netzwerkmanagements liegen. Dies kann auch als Vorteil gesehen werden, wenn man die Fähigkeiten von existierenden Monitoring-Systemen betrachtet. Diese wurden für die Überwachung von Komponentenzuständen entwickelt, verfügen über Soll-Ist-Vergleichsmethoden, können bei Abweichungen alarmieren und werden ohnehin von den Unternehmen eingesetzt. Allerdings ist keine Möglichkeit bekannt, die Informationen und Daten der Monitoring-Systeme im Sinne der Anwendungsfälle auf der Ebene des Controlcenters verfügbar zu machen. Eine Möglichkeit wäre vermutlich durch CIM realisierbar. Insgesamt hätte dies jedoch den Nachteil, dass die Daten nicht Teil der OT und SCADA wären. Der Vorteil, dass die Datenattribute für Sicherheitskonfigurationen bereits in großem Umfang vorhanden sind, hat sich nicht gezeigt. Aus dem Grund wurde ein Ansatz über SNMP nicht weiter verfolgt.

4.3 Modellierung in IEC 61850

Das erste Informationsmodell ist das im vorherigen Abschnitt entwickelte Modell, das die SKI darstellt. Dieses wird in der IEC 61850 modelliert. Dabei handelt es sich im Wesentlichen um eine High-Level-Modellierung, um die Zuordnung der jeweiligen Attribute zu zeigen. Diese Integration ist notwendig, da für die SKI innerhalb der Architektur des TC57 Power System Architecture Model kein entsprechendes Informationsmodell existiert.

Das zweite Informationsmodell, das in die IEC 61850 integriert wird, ist das Informationsmodell der Fernattestierung. Da hierfür bereits ein konkretes Informations- und Datenmodell von der TCG vorliegt, erfolgt eine wesentlich tiefergehende Modellierung, die im übernächsten Abschnitt näher erläutert wird. Diese Vertiefung geht zudem auf zwei wesentliche Aspekte der vorliegenden Arbeit ein: Erstens ist die Remote Attestation eine notwendige Voraussetzung, um einem IED vertrauen zu können. Zum anderen handelt es sich bei der Fernattestierung um eine Funktion, die die Integrität der Plattform gegenüber Dritten nachweisen kann. Die Ergebnisse aus der Standardanalyse haben gezeigt, dass die Plattformintegrität in den Normen und Standards mit besonderem Fokus adressiert wird.

Integration der Sicherheitskonfigurationsinformationen

Um eine Integration in die Protokolle und Strukturen des Energienetzes zu erreichen, wurde das zuvor erarbeitete Informationsmodell auf das der IEC 61850 abgebildet. Die Zuordnung der Klassen und Attribute der SKI ist in Abbildung 4.5 grafisch dargestellt. Die Sicherheitskonfigurationen werden als *Logical Device* dargestellt. Dieses *Logical Device* verkörpert im Innen- und Außenverhältnis eines IED den zentralen Zugriff auf die SKI. Auf der Ebene der *Logical Node* sind die einzelnen Sicherheitsstandards verortet und referenzieren über den *Standard Identifier* die jeweilige Norm. Auf der darunterliegenden Ebene, den *Data Objects*, wird der eigentliche Inhalt einer Anforderung zugeordnet. Dies sind neben der Beschreibung, Namen und der funktionalen Anforderung vor allem die Konfigurationen. Die übergeordnete Ebene des Servers wird hier nicht betrachtet, da es sich um die Abbildung der SKI handelt und diese sich unterhalb der Serverinstanz befinden.

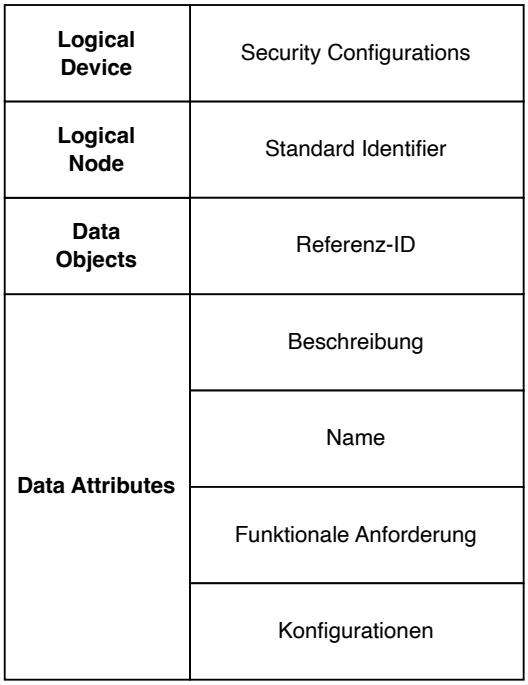

Abbildung 4.5.: Abstrakte Abbildung des Informationsmodells auf IEC-61850-Informationsmodell

4.4 Informationsmodell für Remote Attestation

In diesem Abschnitt erfolgt eine Beschreibung der Integration der Remote-Attestation-Funktionalität in das Informationsmodell der IEC 61850. Im Gegensatz zu den

Sicherheitskonfigurationen aus dem vorherigen Abschnitt kann ein bereits vorhandenes Informationsmodell verwendet werden. Das bestehende Informationsmodell der Remote Attestation wurde von der Trusted Computing Group (TCG) entwickelt und als Ausgangspunkt verwendet. Dieses wird im Folgenden kurz beschrieben und der Integrationsprozess sowie die Zuordnung der Attribute in die IEC-61850-Strukturen werden präsentiert.

Für ein besseres Verständnis wird das modellierte Ergebnis zuerst vorgestellt. Danach erfolgt eine detaillierte und schrittweise Erläuterung der Integration der Remote Attestation sowie des dazugehörigen Datenmodellierungsansatzes und dessen Anwendungsfall. Im Anschluss werden die Attribute der Remote Attestation auf die IEC-61850-Attribute abgebildet und die daraus resultierenden Datenobjekte, logischen Knoten und Modellierungstabellen nach IEC 61850 erläutert.

4.4.1 Remote-Attestation-Zielkonzept

Das Ziel der Remote Attestation ist wie bei den SKI die Abfragbarkeit aus dem Controlcenter. Im Falle der Remote Attestation kommt dem Controlcenter dabei die Rolle des Verifizierers zu, die IED hat die Rolle des Attestees. Folgend dem hierarchischen Aufbau des IEC-61850-Informationsmodells (siehe Kapitel IEC 61850, Abbildung 2.3) wird das Konzept der Attribute in Abbildung 4.6 gezeigt. Die unterste Ebene stellt die vorgeschlagene *TPM2Quote-Klasse* („TQC“) mit drei Beispielattributen dar. Die zweite Schicht enthält die Datenobjekte, die sich in der TPM2-Klasse widerspiegeln, unter anderem das Attribut TPM2Quote2, das für den Prozess der Remote Attestation von wesentlicher Bedeutung ist, da es die erforderlichen Bescheinigungsinformationen als Attribute enthält. Die Logical Node wird definiert, um das TPM2 innerhalb des logischen Geräts zu repräsentieren, welches wiederum Teil des Servers auf einem IED ist. Da das TPM2 als logischer Knoten dargestellt wird, eröffnet sich die Möglichkeit, mehrere Datenobjekte für verschiedene TPM2-Anwendungsfälle und Funktionen zu erstellen.

Zu Veranschaulichung wurden die Datenobjekte *TPM2Quote2* und *VendorInformation* definiert und in dieser Abbildung dargestellt.

4.4.2 Trusted Attestation Protocol

Die von der TCG entwickelte Spezifikation Trusted Attestation Protocol (TAP) definiert das Informationsmodell für Remote Attestation in unterschiedlichen An-

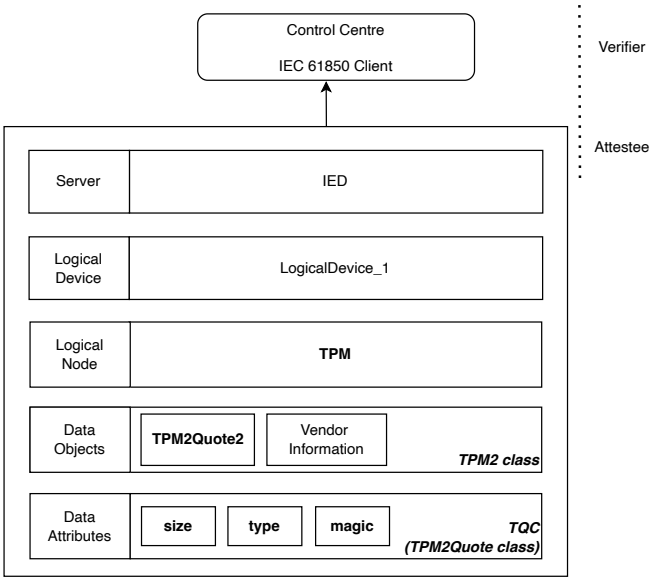

Abbildung 4.6.: Die erzeugten Datenklassen für die Attribute, Objekte und logischen Knoten. Eigene Darstellung aus [Fra+23]

wendungsfällen. Des Weiteren werden für die diversen Anwendungsfälle die entsprechenden Informations- und Datenmodelle aufgezeigt [Tru19d]. Die dortigen Anwendungsfälle unterscheiden sich hauptsächlich in der Implementierung des sogenannten „Frischheitsnachweises“ (proof-of-freshness, sog. nonce oder magic). Zur Reduktion der Komplexität wird in dieser Publikation der Anwendungsfall „Explicit Attestation using TPM2_Quote“ als Implementierungsbeispiel gewählt. Dieser Anwendungsfall ist in der Lage, ohne Unterstützung Dritter auszukommen, da der anfragende „Verifier“ den Frischenachweis erstellt und diesen mit der Anfrage an den Attester mitsendet.

Gemäß der TAP-Spezifikation ist dieser Anwendungsfall durch den Bescheinigungsuntertyp (Attestation subtype) 0x04 definiert und verwendet den Befehl TPM2_Quote zur Bescheinigung von PCR-Werten. Der Befehl generiert eine signierte TPMS_ATTEST-Struktur. Diese Struktur enthält die Attribute des TPM2-Befehls gemäß der Definition in der *Trusted Platform Module Library Part 2* [Gro16]. Die TPMS_ATTEST-Struktur ist in Tabelle 4.1 dargestellt. Darin ist ersichtlich, dass die Struktur verschiedene Parameter und Typen enthält. Jeder Typ steht für eine TPM2-spezifische Datenstruktur, die ein oder mehrere Attribute enthält, deren Bedeutung im nachfolgenden Abschnitt erläutert wird. Die Datenstrukturen selbst sind Teil der TPM2-Spezifikation und in [Tru19d] spezifiziert.

Vor der Erstellung neuer Attribute ist gemäß der IEC 61850 zu prüfen, ob bereits vordefinierte gemeinsame Datenklassen (engl. common data classes, CDC) mit entsprechenden Attributen existieren. Dies ist für die TAP-Integration nicht der Fall, daher werden benutzerdefinierte Klassen erstellt, welche in den folgenden Abschnitten erläutert werden.

4.4.3 Zuordnung der Attribute und Datenstrukturen

Die in der TAP-Spezifikation definierten Datenstrukturen und Attribute müssen durch Datenattribute und Datentypen dargestellt werden, die in der Norm IEC 61850 enthalten sind. Ein anschauliches Beispiel für die Abbildung der Spezifikation der TPM2-Bibliothek auf die IEC-61850-Attribute ist in Abbildung 4.7 dargestellt. Die Abbildung zeigt die TPMS_ATTEST-Struktur der Tabelle 4.1 und die ausgewählten entsprechenden Datentypen aus der Norm IEC 61850. Allgemein können die Datenstrukturen aus dem Bereich der TAP-Spezifikation auch verschachtelt sein.

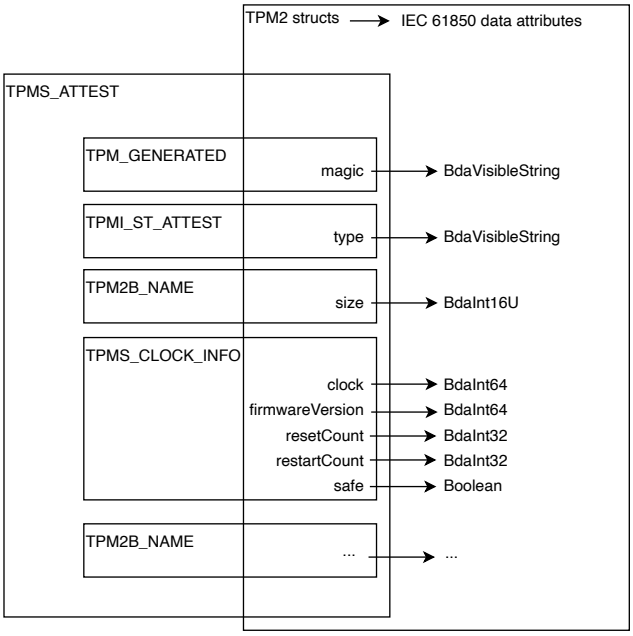

Abbildung 4.7.: Beispielhafte Zuordnung von ausgewählten Attributen aus den Informationsmodellen. Eigene Darstellung aus [Fra+23]

Tabelle 4.1.: Definition der TPMS_ATTEST-Struktur des Trusted Attestation Protocol, Quelle: [Tru19d]

Parameter	Typ	Beschreibung
magic	TPM_GENERATED	Die Angabe, dass diese Struktur von einem TPM erstellt wurde (immer TPM_GENERATED_VALUE)
type	TPMI_ST_ATTEST	Typ der Bescheinigungsstruktur
qualifiedSigner	TPM2B_NAME	Qualifizierter Name des Signierschlüssels
extraData	TPM2B_DATA	Externe Informationen, die vom Aufrufer bereitgestellt werden. Hinweis: Eine TPM2B_DATA-Struktur bietet Platz für einen Digest und einen Methodenindikator zur Angabe der Komponenten des Digests. Die Definition dieses Methodenindikators liegt außerhalb des Anwendungsbereichs dieser [TAP] Spezifikation.
clockInfo	TPMS_CLOCK_INFO	Clock, resetCount, restartCount und Safe Attribute
firmwareVersion	UINT64	Herstellerspezifischer Wert, der die Versionsnummer der Firmware des TPM2 angibt
[type]attested	TPMU_ATTEST	Typspezifische Bescheinigungsinformationen

4.4.4 Datenattribute

Die zugeordneten Datenattribute für den beschriebenen Anwendungsfall der Remote Attestation sind in Tabelle 4.2 aufgeführt. Die Tabelle beinhaltet die Attributnamen, welche die Bezeichnungen der TPMS_ATTEST-Strukturen aus dem TAP-Informationsmodell widerspiegeln. Die Spalte „Typ“ in der Tabelle definiert die Basisdatentypen (BDA). Zum Beispiel steht *BdaInt16U* für ein *16-bit integer ohne Vorzeichen*. Neben dem Attributtyp befindet sich die Spalte, die die funktionale Beschränkung (engl. functional constraint, FC) für jedes Attribut definiert. In Bezug auf den vorliegenden Anwendungsfall ist die FC als operational received (OR) (dt. operationell erhalten) definiert. Die Spalte daneben enthält die Beschreibung und die letzte Spalte definiert das Vorkommen des Attributs. Dieses kann mandatory (M, dt. obligatorisch), optional (O) oder complementary (C, dt. komplementär) sein. Im vorliegenden Anwendungsfall sind alle Attribute notwendig und deshalb als mandatory gekennzeichnet.

Tabelle 4.2.: TPM2-Quote-Klasse (TQC) Attributtypen gemäß dem Anwendungsfall TAP

TPM2-QUOTE-Klasse				
Attributname	Typ	FC	Wert / Bereich / Beschreibung	M/O/C
Datenattribut				
Status				
size	BdaInt16U	OR	Größe der Attestdatenstruktur.	M
TPMS_ATTEST				
magic	BdaVisibleString	OR	Die Angabe, dass diese Struktur von einem TPM erstellt wurde (immer TPM_GENERATED_VALUE).	M
type	BdaVisibleString	OR	Typ der Attestdaten-struktur. In diesem Fall „TPM_ST_ATTEST_QUOTE“.	M
qualifiedSigner	BdaInt16U[]	OR	Qualifizierter Name des Signier-schlüssels.	M
extraData	byte[]/ TPM2B_DATA	OR	Vom Aufrufenden bereitgestellte Informationen.	M
TPMS_CLOCK_INFO				
clock	BdaInt64	OR	Clock, resetCount, restartCount and safe	M
firmwareVersion	BdaInt64	OR	Herstellerspezifischer Wert, der die Versionsnummer der Firmwa-re des TPMs angibt.	M
resetCount	BdaInt32	OR	Anzahl der TPM-Resets seit dem letzten TPM2_Clear()-Aufruf.	M
restartCount	BdaInt32	OR	Anzahl der Fälle, in denen TPM2_Shutdown() oder _TPM_Hash_Start seit dem letz-ten TPM Reset oder TPM2_Clear() aufgerufen wurden.	M
safe	BOOLEAN	OR	Das TPM hat bisher keinen grö-ßeren Wert als den aktuellen Wert der Uhr gemeldet. Wird bei TPM2_Clear() auf YES gesetzt.	M
TPMS_PCR_SELECTION				
pcrSelectAlgHash	BdaVisibleString	OR	Der ausgewählte Hash-Algorithmus.	M
sizeofSelect	BdaInt8	OR	Die Größe des pcrSelect-Arrays in Oktetten.	M
pcrSelect	BdaInt8U (rep. byte)	OR	Die Bitmap der ausgewählten PCR.	M
pcrDigest	BdaInt8U (rep. byte)	OR	Digest der ausgewählten PCRs un-ter Verwendung des Hashs des Si-gnierschlüssels.	M
pcrUdpateCounter	BdaInt32	OR	Anzahl der Selektionsstrukturen. Ein Wert von null ist zulässig.	M
pcrs	BdaInt8U[] (rep. byte)	OR		M

4.4.5 Datenobjekte

Um den Zugriff auf den TPM2 ganzheitlich zu integrieren und instanziieren zu können, werden seine Funktionen als IEC-61850-basierte Datenobjekte bereitgestellt. Diese Objekte sind in der Abbildung 4.6 dargestellt. Der IEC-61850-Server wird innerhalb der physischen IED bereitgestellt und enthält ein Logical Device (dt. logisches Gerät). Die definierte Logical Node (dt. logischer Knoten) stellt den TPM2 selbst dar. Die darunterliegende Schicht enthält zwei Datenobjekte: Das *TPM2Quote2* und das *VendorInformation*. Diese Datenobjekte verweisen auf Datenattribute, die als eigene IEC-61850-Klasse definiert wurden. Diese Klasse ist die *TPM2 class* und beinhaltet diese beiden Datenobjekte. In der Tabelle 4.3 ist diese Klasse genauer dargestellt und enthält das Datenobjekt *TPM2Quote2*. Die Datenobjekte beziehen sich auf die zuvor definierte gemeinsame Datenklasse *TQC*. Die Tabelle ist nach den Vorgaben der Norm IEC 61850 erstellt worden und definiert das Datenobjekt *TPM2Quote*, welches als Beispiel für die Implementierung der vorliegenden Arbeit dient. Die Datenobjekte greifen auf die Datenattribute zu und machen diese zugänglich. Diese Datenattribute sind vom Typ Basic Data Attributes (BDAs) nach der Norm IEC 61850. Diese Attribute liefern die Zuordnung zu den erforderlichen Datenattributen für den Anwendungsfall der Remote Attestation von TPM2Quote2.

Tabelle 4.3.: Datenobjekt der Klasse TPM2 für den Anwendungsfall TAP

TPM2-Klasse			
Name	Allg. Datenklasse	Erläuterung	M/O/C
Datenobjekte			
Attestinformation			
TPM2Quote2	TQC	Enthält die Attribute des Anwendungsfalls der expliziten Attestierung mittel TPM2_Quote-Befehl. Der TPM2.0-Anwendungsfall ist in der TAP-Spezifikation beschrieben [Tru19d]	O

4.4.6 Logical Node

Obwohl es sich bei dem TPM2 um einen physischen Chip handelt, wird dieser im ACSI-Modell auf der Ebene der Logical Node verortet und repräsentiert somit die logischen Funktionen und nicht seine physikalischen Eigenschaften. Dies ist für die Modellierung insofern wichtig, als man davon ausgehen könnte, dass der TPM2 selbst als Logical Device dargestellt wird. Außerdem kann ein TPM2 auch als

Software-TPM2 innerhalb einer CPU oder als virtualisierter Software-TPM existieren. Für die Logical Node wurde die bereits bestehende IEC-61850-Klasse *Generic process I/O* (GGIO) verwendet. Gemäß IEC 61850 kann diese Klasse für Anwendungsfälle genutzt werden, die von den anderen Klassen nicht abgedeckt werden, und ihr Inhalt kann sicherheitsrelevant sein. Dieser logische Knoten ist in erster Linie dazu gedacht, TPM2-Funktionen anzubieten, die für interne und externe Zwecke oder Kommunikation verwendet werden. Die Klasse GGIO hat auch vordefinierte Datenobjekte, deren Implementierung jedoch optional ist.

4.5 Zusammenfassung

Durch die Modellierung mittels SGAM wurde das Informationsmodell der Norm IEC 61850 als Lösung für die Übertragung in der Referenzarchitektur des TC57 Power System Architecture Model erarbeitet. Im Ergebnis wurde das Informationsmodell der IEC 61850 um zwei Informationsmodelle erweitert. Das erste ermöglicht eine Abbildung der SKI aus dem vorherigen Kapitel. Das zweite Informationsmodell bildet die Remote Attestation im IEC-61850-Informationsmodell ab. Die Integration der Remote Attestation wird exemplarisch vertieft. Dafür wurden eigene Datenklassen und Objekte nach IEC 61850 modelliert und in der Tiefe dargestellt und umgesetzt. Die beiden Informationsmodelle des SKI und die Remote Attestation stellen die Grundlage für die Implementierung im Demonstrator, welche im folgenden Kapitel beschrieben wird.

5 Demonstrator / Proof of Concept

5.1 Einleitung

In diesem Kapitel wird die Implementierung des praktischen Demonstrators beschrieben. Aufbauend auf dem vorherigen Kapitel werden die zuvor dargelegten Informationsmodelle in einem praktischen Demonstrator implementiert und instanziiert. Eine theoretische Umsetzung bzw. Integration in die Norm IEC 61850 erfolgte bereits im vorherigen Kapitel, die praktische Integration wird in diesem Kapitel gezeigt und stellt die Voraussetzung für die Evaluation dar. Das Ziel des Demonstrators ist es, die zuvor vorgestellten Konzepte praktisch umzusetzen, um die Funktionsfähigkeit zu zeigen und darauf basierend zu evaluieren. Um dies zu erreichen, wird die Umsetzung des Demonstrators zunächst in einer isolierten Entwicklungsumgebung eingebettet und im nachfolgenden Evaluationskapitel in die Evaluationsumgebung überführt. Die Entwicklungsumgebung und die Architektur sowie die minimal notwendigen Anforderungen werden zunächst vorgestellt und in einem Gesamtkonzept verortet. Darin enthalten sind auch die notwendigen Softwarebibliotheken und Werkzeuge sowie die dafür benötigte Entwicklungsumgebung.

5.2 Konzeption

Das Ziel des Demonstrators ist es, die beiden Informationsmodelle der Remote Attestation und der SKI praktisch zu instanziieren und innerhalb des Stromnetzes zur Verfügung zu stellen, sodass das Controlcenter sie abrufen kann. Mittels SGAM wurde im vorigen Kapitel bereits das Kommunikationsprotokoll erarbeitet, das für diesen Demonstrator verwendet wird. Für eine realistische, aber vereinfachte Einbettung in die Referenzarchitektur des TC57 Power System Architecture Model wird ein Gerät benötigt, das die Daten über IEC 61850 bereitstellt, und ein weiteres Gerät, welches das Controlcenter verkörpert und die Daten abrufen kann. Im Hinblick auf die Integration in die TC57-Referenzarchitektur ist daher eine Einbettung der Geräte als Ortsnetzstation und Controlcenter (Control Centre A) vorgesehen. Dies ist in

Abbildung 5.1 dargestellt, die rot markierten Elemente zeigen die ausgewählten Protokolle, Komponenten und Bereiche. Der Demonstrator wird so angelegt, dass das

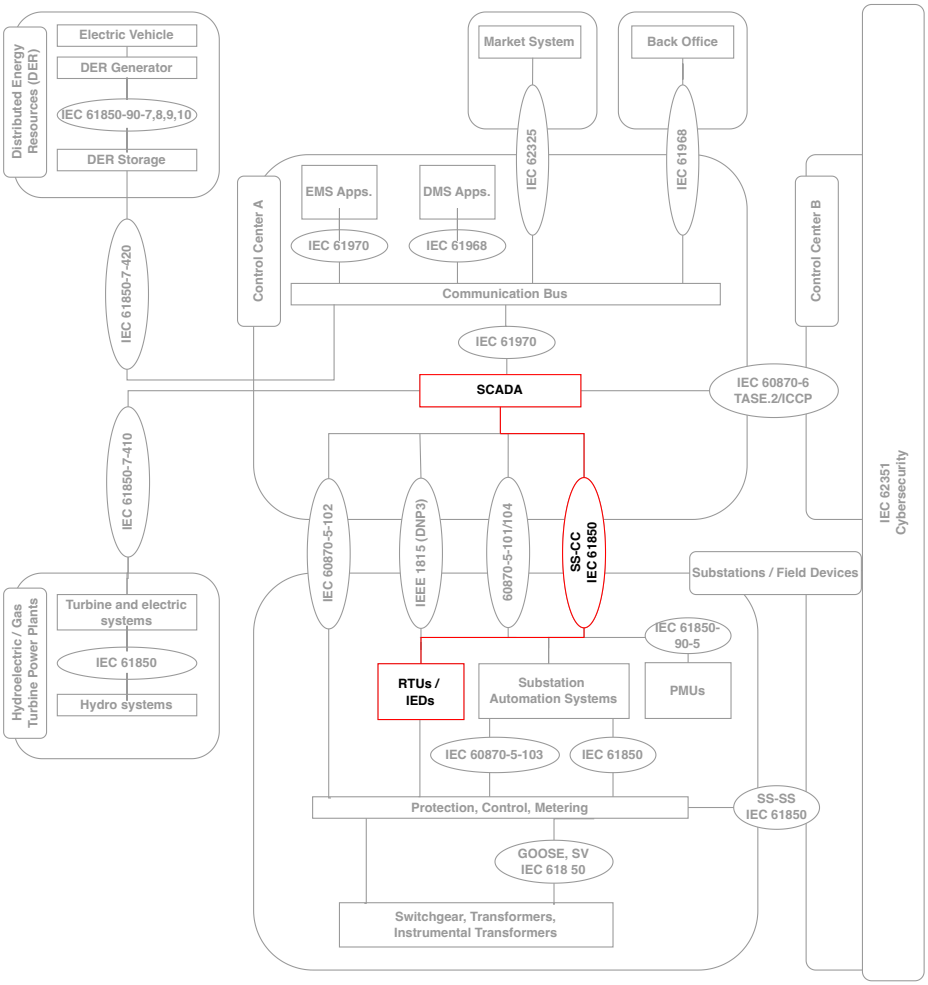

Abbildung 5.1.: Fokussierter Kommunikationsweg: RTU/IED der Unterstation über IEC 61850 in das Controlcenter A, Abbildung in Anlehnung an [Cle14]

Controlcenter die Informationen aus einer in Ortsnetzstationen typischen IED abruft. Dazu wird eine IED die Ortsnetzstation abbilden und für den Demonstrator vereinfachen, weil für die Umsetzung der Anwendungsfälle die Sekundärtechnik (IKT) benötigt wird und die entsprechenden Informationsmodelle als konkrete Datenmodelle über die Kommunikationsschnittstellen bereitstellen soll. Auf Umsetzungen der Primärtechnik wird daher bewusst verzichtet, da diese für die Anwendungsfälle von nachrangiger Bedeutung sind. Das im Controlcenter befindliche SCADA-System wird ebenfalls vereinfacht und als Client in einer eigenen Implementierung so umgesetzt, dass diese über die Kommunikationsstrecke mit dem IEC 61850 die Daten von der

IED der Ortsnetzstation abrufen kann. Auch an dieser Stelle werden für den Demonstrator aufgrund der Anwendungsszenarien selektiv die Funktionen des IKT-Bereichs dargestellt und umgesetzt. Diese Umsetzung im Rahmen eines Demonstrators erfolgt

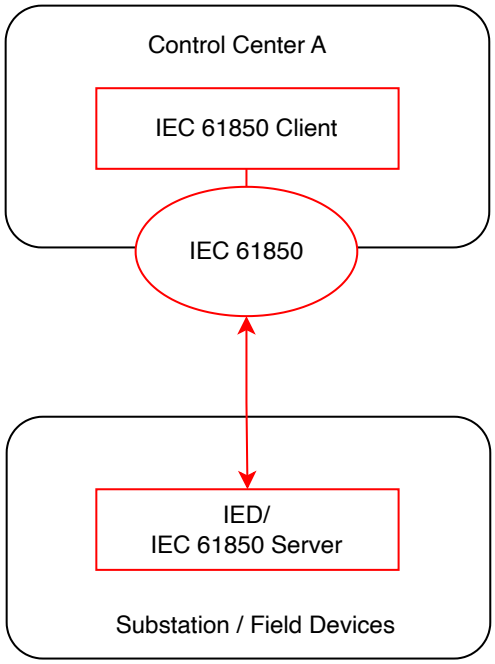

Abbildung 5.2.: Client-Server-Komponenten des Demonstrators als Architekturdarstellung

als Client-Server-Architektur und ist in Abbildung 5.2 gezeigt. Dargestellt ist ein vereinfachter Ausschnitt der Referenzarchitektur des TC57 Power System Architecture Model, der das Controlcenter und die Kommunikationsverbindung zu einer Unterstation (Substation) zeigt. Für den Demonstrator der vorliegenden Arbeit wird die Unterstation als eine IED vereinfacht, welche einen IEC-61850-Server abbildet. Das Controlcenter wird so beschränkt, dass es eine Kommunikationsstrecke in Form eines Local Area Network, dt. lokales Netzwerk (LAN) zur Unterstation hat und der dort befindliche Client die Daten vom Server aus der Unterstation abfragt.

In den folgenden Abschnitten wird die iterative Vorgehensweise zur Umsetzung erläutert, beginnend mit der Auswahl der Bibliotheken zur Implementierung einer IEC-61850-basierten Client-Server-Architektur. Weiterhin werden die Anforderungen an die Entwicklungsumgebung sowie der Aufbau der Bibliotheken vorgestellt.

Anschließend wird die IEC-61850-basierte Client-Server-Architektur schrittweise um die Informationsmodelle erweitert und auch deren Implementierung beschrieben.

5.2.1 Werkzeuge und Systeme

Die Identifikation und Festlegung von benötigten Bibliotheken und Werkzeugen sind ein wichtiger Schritt, da weitere Design- und Implementierungsentscheidungen davon abhängen. Dabei werden vor allem die Bibliotheken betrachtet, die die benötigten Kernfunktionalitäten bereitstellen können. Diese sind die Anbindung des TPM2 zur Bereitstellung der Remote-Attestation-Funktionalitäten. Eine zweite Bibliothek stellt die aus der IEC 61850 benötigten Funktionen und Datenmodelle bereit. Im Rahmen einer Online-Recherche haben sich jeweils zwei Bibliotheken herauskristallisiert, die für die TPM2-Anbindung infrage kommen, und zwei Bibliotheken, die eine IEC-61850-basierte Umsetzung ermöglichen. Diese Bibliotheken werden im folgenden Abschnitt näher betrachtet und verglichen.

TCG Software Stack 2.0

Für die Anbindung des TPM2 wird eine Bibliothek benötigt, die den Kommunikationsstack für den TPM2 zur Verfügung stellt. Dieser sogenannte TCG Software Stack 2.0 (TCG) ist von der Trusted Computing Group (TCG) in verschiedenen Standards definiert und frei verfügbar [Tru19a]. Die derzeit wichtigsten Teile dieser Spezifikationen bzw. Stacks sind auf Github.com als Open Source Software (OSS) von einer offenen Entwickler-Community[1] implementiert und können unter Einhaltung der *BSD-2-Clause*-Lizenz verwendet werden. Der dortige TSS-Stack besteht aus verschiedenen Repositorien und implementiert die unterschiedlichen, aufeinander aufbauenden Application Programming Interface (dt. Anwendungsschnittstelle) (API)-Level der TCG. Eine Übersicht der Bibliotheken und der darin umgesetzten Spezifikation ist in Tabelle 5.1 gezeigt (übernommen aus dem TPM2-TSS-Repository auf Github [@Lin]).

[1] Linux TPM2 & TSS2 Software: https://github.com/tpm2-software.

Tabelle 5.1.: Umgesetzte TSS2-Bibliotheken entsprechend den Spezifikationen der TCG

Name	Bibliothek	Beschreibung	Spezifikationen
Feature API (FAPI)	libtss2-fapi	High-Level API für einfache TPM2-Nutzung	TCG Feature API (FAPI) Specification[Tru20a] TCG TSS 2.0 JSON Data Types and Policy Language Specification [Tru20c]
Enhanced System API (ESAPI)	libtss2-esys	1:1 Abbildung der TPM2-Befehle	TCG TSS 2.0 Enhanced System API (ESAPI) Specification [Tru20b]
System API (SAPI)	libtss2-sys	1:1-Abbildung von TPM2-Befehlen	TCG TSS 2.0 System Level API (SAPI) Specification [Tru19c]
Marshaling/ Unmarshaling (MU)	libtss2-mu	(Un)marshaling all data types in the TPM library specification	TCG TSS 2.0 Marshaling/Unmarshaling API Specification [Trub]
TPM Command Transmission Interface (TCTI)	libtss2-tcti-device libtss2-tcti-tbs libtss2-tctildr libtss2-tcti-swtpm ...	Standard-API zum Senden/Empfangen von TPM-Befehlen und -Antworten	TCG TSS 2.0 TPM Command Transmission Interface (TCTI) API Specification [Tru24b]
		Basis für alle Implementierungen	TCG TSS 2.0 Overview and Common Structures Specification [Tru19a]

Tabelle 5.2.: Übersicht der TPM2-Bibliotheken und -Stacks

Bibliothek/ Stack	Programmiersprachen	Besonderheiten
TSS.MSR	C#, C++, Java, JavaScript, Python	Verfügbar auf Github, Microsoft Research
TrouSerS	-	Unterstützt kein TPM2, veraltet
Urchin	-	Bezieht sich auf Windows 10
libIEC61850	C	Aktuelle und umfangreiche Dokumentation, kommerzielle Verwertung durch MZ Automation, Unterstützung für TLS 1.2[5]

Bei der Recherche nach weiteren Bibliotheken für den TSS wurde der Microsoft *TSS.MSR* betrachtet. Dabei handelt es sich um die TSS-Implementierung von Microsoft Research, die auf Github[2] verfügbar ist. Dort werden Stacks für die Programmiersprachen C# (.NET), C++, Java (>SE 8), JavaScript (mit Node.js >4.8.4) und Python (2.7 und >3.5) angeboten. Weitere TSS-Implementierungen wie zum Beispiel *TrouSerS*[3] unterstützen entweder nicht den TPM2, sind veraltet (lange keine Commits bei Github) oder beziehen sich auf Windows 10, wie zum Beispiel das Paket namens *Urchin*[4]. Die Dokumentation der Bibliotheken war ebenfalls ein wichtiges Kriterium für den Auswahlprozess.

IEC-61850-Bibliotheken im Vergleich

Die erste Bibliothek ist die in C geschriebene *libIEC61850* unter der Lizenz GNU General Public License version 3 (GPLv3) der Firma MZ Automation GmbH [@MZ 23]. Die zweite Bibliothek ist die Java-basierte Open-Source-Bibliothek IEC61850bean/OpenIEC61850 unter Apache-2.0-Lizenz, die im Rahmen von Forschungsprojekten entwickelt wurde und heute von der beanit GmbH kommerziell unterstützt wird [@Ste]. Beide erfüllen eine Liste von Kriterien: kostenfrei verfügbar, Open Source, anpassbar bzw. veränderbar und funktional erfüllen sie die folgenden Voraussetzungen:

- OSI-Anbindung via Manufacturing Messaging Specification (MMS)
- Datensätze lesen, schreiben und konfigurieren
- MMS-Unterstützung für die Kommunikation zum Controlcenter
- Praktische Erweiterbarkeit des Daten- und Informationsmodells

[2]Microsoft auf Github.com: https://github.com/microsoft/TSS.MSR.
[3]TrouSerS: Open-Source-Software Stack: https://trousers.sourceforge.net.
[4]Repository ms-iot/security: https://github.com/ms-iot/security/tree/master/Urchin.

- Konfiguration über Substation Configuration Description Language (SCL)
- ReportControlBlocks (RCB) konfigurieren
- Reporting erstellen und spontan senden
- Verschlüsselung zwischen IED und Controlcenter mittels TLS-Version 1.3
- Bereitstellung eines dokumentierten IEC-61850-kompatiblen Clients (im IEC 61850 wird lediglich ein Server spezifiziert, jedoch kein Client).

Bewertung der Bibliotheken

In der Gesamtschau stehen zur Wahl eine Implementierung in Java mit dem Microsoft-TSS und der Implementierung Java beanit IEC61850. Dem steht eine Realisierung mit den C-basierten Bibliotheken gegenüber. Dies wäre die Kombination aus der libIEC61850 von MZ Automation und den zuvor vorgestellten TSS-Bibliotheken der Linux TPM2 & TSS2 Software Community. Zwei wichtige Kriterien sprechen für die C-basierte Implementierungsvariante: Erstens ist C in der Automatisierungstechnik aufgrund der besseren Echtzeitfähigkeiten angesehener als Java. Das zweite und entscheidende Kriterium für den Demonstrator in der vorliegenden Arbeit ist jedoch die Dokumentation der Bibliotheken.

Bei dem TCG TSS ist durch die aktive Entwicklergemeinschaft eine umfangreiche Dokumentation entstanden, welche durch Tests und Beispiele untermauert wird. Der TSS-Ableger von Microsoft enthält keine Dokumentation, sondern lediglich teilweise funktionierenden Beispielcode. Auch die Dokumentation der libIEC61850 ist deutlich aktueller und umfangreicher, was vermutlich durch die kommerzielle Verwertung seitens MZ Automation begünstigt wird. Darüber hinaus stellt die libIEC61850 eine Dokumentation für eine verschlüsselte Verbindung zwischen Client und Server über TLS Version 1.2 zur Verfügung und beschreibt den genauen Aufbau ihrer Bibliothek. Nicht vollständig erfüllt ist allerdings das Kriterium, TLS Version 1.3 zu unterstützen. Im Rahmen der vorliegenden Arbeit kann diese Abweichung akzeptiert werden, da für sie die Verbindungssicherheit nicht im Fokus steht und es Möglichkeiten gibt, die Nachteile gegenüber Version 1.3 zu mitigieren. Für den Schwerpunkt dieser Arbeit ergeben sich daraus keine weiteren Risiken. Zusammenfassend resultieren damit zwei Möglichkeiten:

[5] Die libIEC61850 unterstützt TLS 1.3 erst seit der Version 1.6.0, welche im August 2023 erschienen ist.

- Java-basierte Entwicklung mit dem Microsoft-TSS und der Bibliothek beanit IEC61850.
- C-basierte Entwicklung mit der libIEC61850 von MZ Automation und den TSS-Bibliotheken der Linux TPM2 & TSS2 Software Community.

Für den Demonstrator wurde der Variante mit C-Bibliotheken der Vorzug gegeben und die Entwicklung des Servers in C realisiert. Die einzelnen Komponenten und der Aufbau werden in den folgenden Abschnitten erläutert.

5.2.2 Client-Server-Architektur der libIEC61850

Dieser Abschnitt beschreibt den Aufbau des IEC-61850-Servers und Clients, so wie er von der libIEC61850 zur Verfügung gestellt wird, um die entsprechenden Erweiterungen und den Gesamtaufbau nachvollziehen zu können. Der Client wird zuerst vorgestellt, weil im Kontext der vorliegenden Arbeit eine deutlich höhere Komplexität auf der Serverseite besteht und die Serverseite in den folgenden Kapiteln wesentlich tiefer erläutert wird und so das Gesamtverständnis über den Aufbau und Ablauf besser gegeben ist.

Aufbau IEC-61850-Client-API

Obwohl in der offiziellen Normenreihe der IEC 61850 kein expliziter Client definiert ist, wird zur Kommunikation mit dem IEC-61850-Server ein Client benötigt. Die Bibliothek libIEC61850 stellt diesen Client zur Verfügung und er wird in der vorliegenden Arbeit verwendet, um das Controlcenter zu repräsentieren bzw. die Kommunikation dorthin zu verkörpern, und ist damit Bestandteil der SCADA-Umgebung. Der Aufbau des Clients ist in Abbildung 5.4 dargestellt. Gezeigt wird ein Schichtenmodell, welches auf der untersten Ebene die Hardware abstrahiert und diese damit dem MMS-Client-Stack zur Verfügung stellt. Die darüber liegenden Schichten stellen IEC-61850-basierte Services für den Client bereit. Dieser kann über den benutzerdefinierten Bereich (*user provided c application*) mit eigener Programmlogik genutzt werden.

Im benutzerdefinierten Bereich befindet sich der eigene Programmcode der vorliegenden Arbeit, in welchem die Initialisierung der Remote Attestation, deren Auswertung (Rolle des *Verifiers*) sowie die Abfrage der Sicherheitskonfigurationen angesiedelt sind. Auch die Ergebnisse der Abfragen werden dort ausgewertet, wobei

sich diese Arbeit auf einen Soll-Ist-Vergleich beschränkt, ohne die Machbarkeit einzuschränken. Der Client stellt zudem die Schnittstelle zur Datenhaltung und zu den damit verbundenen Referenzdaten bereit, die für den Soll-Ist-Abgleich notwendig sind.

Erweiterung des Clients

Der Client wurde entsprechend erweitert, sodass dieser in der Lage ist, die Remote Attestation anzustoßen, deren Quote-Informationen abzurufen und auszuwerten. Für die SKI gibt es keinen Prozessablauf und die Informationen werden direkt als *Dataset* vom Server abgefragt. Außerdem wird der Client so umgesetzt, dass dieser die jeweiligen Referenzwerte von einem oder mehreren Servern abfragen und auswerten kann. Dafür werden dem Client die Soll-Referenzwerte in Form einer Gerätekonfiguration für jeden Server zur Verfügung gestellt.

Eine beispielhafte Abbildung einer solchen Gerätekonfiguration ist in Skript 5.1 dargestellt. Ein Konfigurationsobjekt enthält ein oder mehrere Geräteobjekte (device_x), bestehend aus Gerätenamen (name), Gerätetyp (Type), IP-Adresse (ip), Port (port), Pfad zum öffentlichen Signierschlüssel (public_signing_key) sowie einem Array der Soll-PCR-Werte (plattform_configurations_expected) und einem Objekt mit den Soll-Einstellungen der Sicherheitskonfigurationsinformationen (security_configurations_expected). Der öffentliche Signierschlüssel eines Geräts wird benötigt, damit der Client die Signatur des *Quotes* überprüfen kann (die Quote-Struktur wird vom TPM2 im Server mit dessen privatem und eingeschränktem Signierschlüssel signiert).

Skript 5.1: Abbildung einer Gerätekonfiguration ohne PCR-Werte und Sicherheitskonfigurationsinformationen

```
{
    "device_1": {
        "name": "IED 1",
        "type": "Rpi4_TPM2",
        "ip": "172.17.0.2",
        "port": 102,
        "public_signing_key": "/path/to/keyfile",
        "plattform_configurations_expected": [],
        "security_configurations_expected": []
    }
}
```

Die Gerätekonfiguration kann um zusätzliche Geräte erweitert werden, sodass der Client mehrere Server abfragen und auswerten kann. Die vollständige Übersicht der Geräteliste findet sich im Anhang in Skript A.4.

Aufbau IEC-61850-Server-API

Die Struktur der IEC61850-Server-Bibliothek ist in Abbildung 5.3 dargestellt. Daran orientiert sich auch der Aufbau des Demonstrators, dessen Code sich an oberster Stelle im Bereich *User provided server application* (dt. vom Benutzer bereitgestellte Serveranwendung) befindet. Diese kommuniziert über die bereitgestellte IEC-61850-Server-API mit der darunter liegenden Service-Ebene, über die der Zugriff auf den MMS-Server-Stack, das IEC-61850-Datenmodell (engl. Data Model) und die Publish-/Subscribe-Methoden der IEC-61850-GOOSE-Objekte erfolgt.

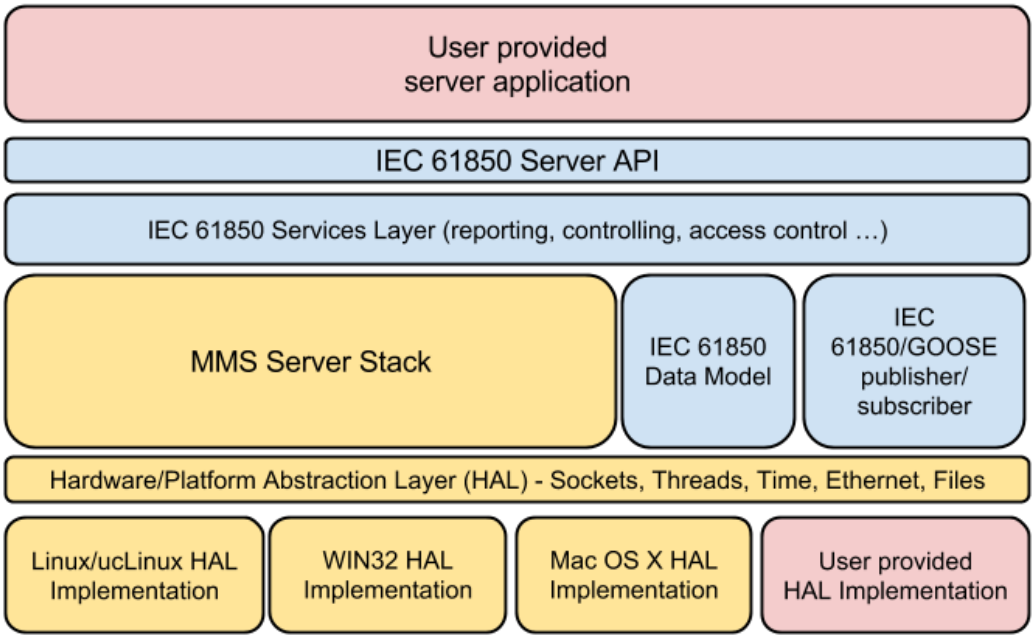

Abbildung 5.3.: Aufbau der libIEC61850-Server-Bibliothek, Quelle [@MZ]

Für den in dieser Arbeit realisierten Demonstrator werden hauptsächlich der MMS-Server-Stack sowie das IEC-61850-Datenmodell verwendet. Die darunter liegenden Schichten dienen der weiteren Abstraktion von der Hardware und sind im Entwicklungsprozess für diese Arbeit nicht weiter relevant. Sie unterstreichen allerdings die Vielseitigkeit der libIEC61850 für unterschiedliche Zielplattformen.

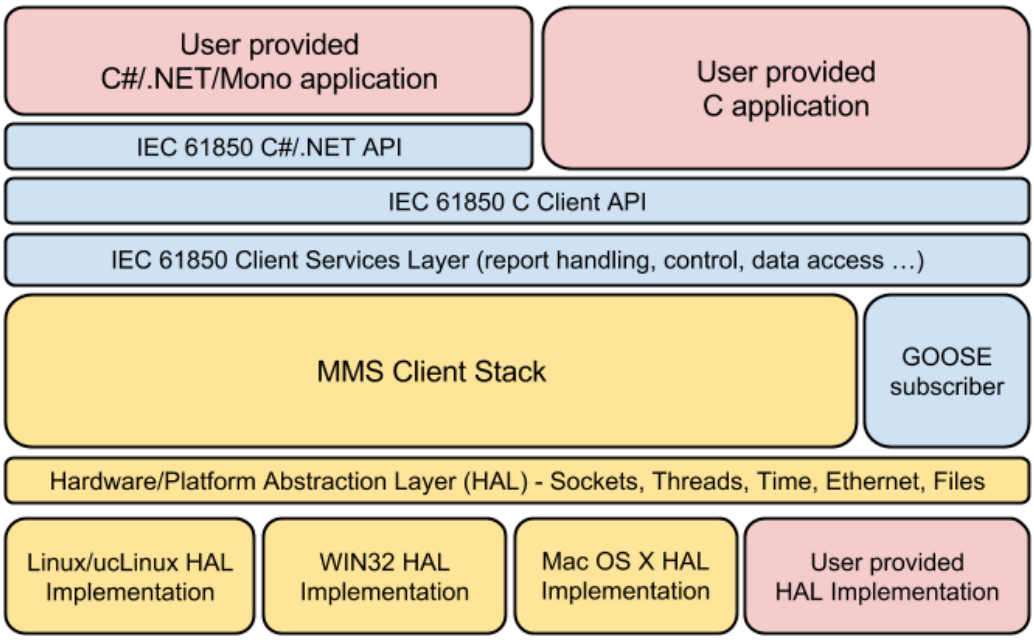

Abbildung 5.4.: Client-API-Architektur der libIEC61850-Bibliothek, Quelle [@MZ]

Benötigte Softwarekomponenten

Die Serverarchitektur wurde als Schichtenmodell entworfen, um die benötigten Komponenten zu identifizieren und den logischen bzw. hierarchischen Aufbau der Serverkomponente zu beschreiben. Das Schichtenmodell ist in Abbildung 5.5 dargestellt und stellt die Ausgangslage für die benötigten Komponenten der Serverentwicklung dar. Seine Aufgaben werden im Folgenden erläutert:

1. **TPM2-Chip:** Dieser zielt darauf ab, als Hardware-Sicherheitsmodul (HSM) die Plattformintegrität sicherzustellen, kryptografisches Schlüsselmaterial sicher zu verwahren, als RoT zu dienen sowie die Integration von der darüber liegenden Schicht des Measured Boot zu ermöglichen.

2. **Measured Boot:** Measured Boot ist eine wesentliche konzeptionelle Komponente, welche einen messbaren Bootvorgang beschreibt. Dies gewährleistet, dass das geladene Betriebssystem oder Kernel eines IED (je nach Auslegung) sowie die darunter liegenden initialen Bootkomponenten kryptografisch gemessen werden.

3. **IED/IEC-61850-Anwendung:** Diese Schicht beinhaltet das Betriebssystem, die Businesslogik der Client- und Server-Anwendung sowie die Kommunikationsschnittstellen, welche durch IEC 61850 spezifiziert wurden. Somit stellt diese

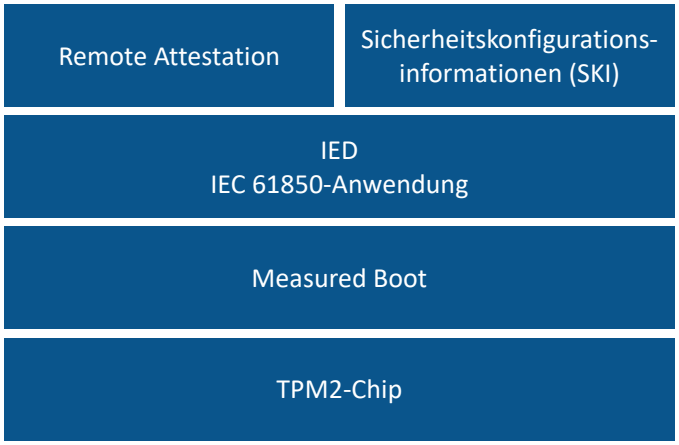

Abbildung 5.5.: Logische Schichtenarchitektur der geplanten Komponenten

Schicht die eigentliche logische Softwarekomponente des IED dar und integriert an dieser Stelle die folgenden Datenmodelle für die Remote Attestation und die SKI.

4. **Remote Attestation:** Die Funktionalität der Remote Attestation wird auf dieser Schicht umgesetzt. Diese Schicht befindet sich logisch innerhalb der IEC-61850-Anwendung, stellt funktional allerdings eine eigene Komponente dar.

5. **Sicherheitskonfigurationsinformationen (SKI)** stellen ebenfalls eine eigene Funktionalität bereit, nämlich deren Abfragbarkeit. Diese befindet sich, wie auch die Remote Attestation, logisch innerhalb der IEC-61850-Serveranwendung, welche die SKI als Datenmodell abbildet, sodass diese abgefragt werden können.

Die detaillierte Beschreibung der genauen Umsetzungskonzeption sowie der darauf folgenden Implementierung geschieht im nachfolgenden Abschnitt *Integrationskonzept*.

5.2.3 Entwicklungsumgebung

Aus den vorgestellten Bibliotheken, APIs und TPM2-Simulatoren wird eine Entwicklungsumgebung aufgebaut, wie in Abbildung 5.6 dargestellt. Dort ist eine Instanziierung der zuvor beschriebenen Komponenten gezeigt und diese dient als Ausgangslage für die weiteren Implementierungen der RA und der SKIs. Deren Umsetzung findet hauptsächlich im *Client-Application-Code* bzw. im *Server-Application-Code* statt. In den folgenden Abschnitten werden die darunter liegenden Komponenten vorgestellt,

die in der Entwicklungsumgebung benötigt wurden. Dies sind die Bereitstellung des TPM2 als Simulator und ein eigens entwickelter Measured-Boot-Emulator als Mock für Messwerte eines Bootvorgangs.

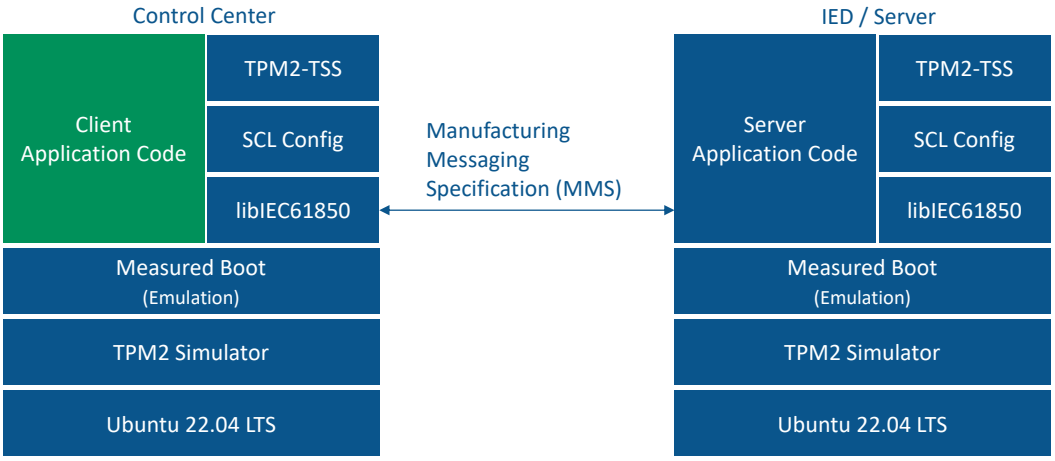

Abbildung 5.6.: Client-Server-Schichten in der Entwicklungsumgebung

Die zu implementierenden Komponenten wurden in mehreren Iterationen umgesetzt, wobei im ersten Schritt die Entwicklungsumgebung definiert wurde. Um einen flexiblen Entwicklungsprozess zu erreichen, wurde für den Client und den Server jeweils ein eigener Docker-Container erstellt. Dadurch sind beide Anwendungen im Entwicklungsprozess voneinander isoliert und werden nicht durch z. B. nebenläufige Prozesse beeinträchtigt, wobei dennoch die Portabilität bestehen bleibt. Der Einsatz von Docker-Containern ermöglicht es, die IEC-61850-basierten Client- und Serversysteme auf beliebigen Hosts zu betreiben und zu entwickeln. Somit konnte auf einem Notebook entwickelt werden. Die Anwendung solcher Virtualisierungskonzepte in der Stromnetzdomäne wurde von Krüger et al. in [KKL23] bereits gezeigt und stellt für den Demonstrator in der vorliegenden Arbeit die Entwicklungsumgebung dar. Die Beschreibungsdatei für den Docker-Container findet sich in Anhang A.1. Die einzelnen Komponenten zur Integration in den Container werden im Folgenden vorgestellt und sind in Abbildung 5.6 dargestellt.

Docker-Umgebung und Betriebssystem

Auf der untersten Ebene ist das Betriebssystem innerhalb des Docker-Containers. Hier wurde das kostenfreie Linux-basierende Betriebssystem vom Hersteller Canonical Ubuntu 22.04 LTS (Long-Term-Support) präferiert. LTS-Versionen zeichnen sich durch eine besonders hohe Stabilität aus und werden über einen langen Zeitraum mit Updates unterstützt. Des Weiteren sind bereits zahlreiche benötigte Bibliotheken

vorinstalliert. Auf den Einsatz spezifischer Unix-Varianten für eingebettete Systeme, wie beispielsweise BusyBox, wurde bewusst verzichtet, da diese die Entwicklung kaum beschleunigen und eine Portierbarkeit in der Regel möglich ist.

TPM2-Simulator

Die Schicht TPM2-Simulator ersetzt speziell im Entwicklungsprozess den physischen TPM2 durch Software. Sie ermöglicht die Bereitstellung von TPM2-Funktionen und den Schnittstellen in isolierten Umgebungen und Containern zwecks Entwicklung. Die Nutzung eines TPM2-Simulators ist in der Entwicklungsphase üblich, da dieser den Prozess unabhängig vom Endgerät macht und gleichzeitig verhindert, dass ein physisch verbauter TPM2 beschädigt wird. Zudem ermöglicht dies automatisiertes Testen von Anwendungen, die einen TPM2 verwenden. Der Simulator bietet allerdings keine echten TPM2-Funktionen und somit auch keine Sicherheit. Er darf deshalb nur in Entwicklungsumgebungen verwendet werden.

Measured Boot

Die Schicht Measured Boot vertritt die Funktion des messbaren Bootvorganges, der als Measured Boot bezeichnet wird. Da Measured Boot während der Entwicklungsphasen nicht im Docker-Container verfügbar ist, wurde eigens ein Measured-Boot-Emulator entwickelt. Dieser Emulator stellt das Ergebnis von Measured Boot in den PCR des TPM2 dar. Somit ist es im Entwicklungsprozess möglich, im Container PCR-Werte abzufragen, die bei jedem Start des Containers identisch sind und nicht vom Hostsystem abhängen. Der Emulator besteht aus festen Dateien, deren Inhalte von einem Bash-Skript gemessen werden. Die Ergebnisse der Messungen werden anschließend dazu verwendet, die PCR-Werte zu erweitern. Der Vorteil von dem Emulator ist die Reproduzierbarkeit und auch die einfache Möglichkeit, die gemessenen Dateien zu Test- und Evaluationszwecken zu manipulieren. Dadurch können manipulierte Bootvorgänge vereinfacht nachgestellt werden. Das Skript wird am Ende des Startvorgangs des Docker-Containers automatisch ausgeführt und die Messungen werden vorgenommen. Eine Auflistung der Dateien, ihrer Repräsentationen und der Referenzwerte für die Messungen ist in Tabelle 5.3 abgebildet. Das dazugehörige Bash-Skript ist in Anhang Skript A.3 hinterlegt.

Tabelle 5.3.: Referenzwerte der Hashes, die der Simulator erzeugt

PCR Bank	Referenz SHA-256 Referenz-Hash
1	biosfile (repräsentiert BIOS-Konfigurationen und Hash-Wert) *0x72AA59B7798C6A6203930673FAC56DE* \ *F8E4FCC2628E4FBABB8291E8F0872E062*
2	fitfile (repräsentiert fit-Dateien des ARM-Bootprozesses) *0x8932B65D01BCDB9F82088C9E5171FC* \ *4B7141B99D6ECEE77E42365E1D5FA9ED6*
5	uboot (uboot Bootloader) *0x99129AA7857ECC3CFCA15221B30ADA8* \ *3FE445B51B22785D29DB324B23C53C9B4*
7	main_kernel (die Kernel-Dateien des Betriebssystems) *0x992AEC5EBB61E1AFE7ED0313E63DEF7* \ *5D994D5E3C5106E8E9B7153EEB36598BB*
9	Hauptanwendung IEC 61850 Server *0xAA9A8F7EE75D1DA343FE7D68762284C* \ *F19EB18E327E5DE4E884F7A0E3DF506A3*
10	Konfigurationen der Hauptanwendung *0x8C28A85B9F66EC8C696A06503E5F5DC* \ *B54AA7CE9983D2ED8951D16E175E92763*

5.3 Integration Remote Attestation

Dieser Abschnitt beschreibt die praktische Konzeption und Implementierung von RA in den Demonstrator mittels des IEC 61850 als Übertragungskanal. Dazu wird das zuvor definierte Informationsmodell als Datenmodell umgesetzt. Für die Implementierung wird das IEC-61850-basierte Client-Server-System der zuvor vorgestellten Entwicklungsumgebung genutzt und die Funktionen der RA werden integriert. Der dazu notwendige Prozessablauf der RA und die wesentlichen Implementierungsdetails werden im Folgenden erläutert und beschrieben.

5.3.1 Integrationskonzept

Ein erster Schritt vor der eigentlichen Integration ist die Abbildung des Prozesses der Remote Attestation mittels des IEC 61850 zwischen Client und Server. Anschließend wird das Informationsmodell zu einem konkreten Datenmodell implementiert. Im Zuge dessen wird auch vorgestellt, wie auf die Quote-Daten des TPM2 zugegriffen wird.

Client-Server-Prozessablauf Remote Attestation in IEC 61850

Zur besseren Nachvollziehbarkeit erfolgt an dieser Stelle eine kurze Wiederholung des Ablaufs einer RA, welcher bereits im Abschnitt *2.2.5 Remote Attestation* ausführlicher behandelt wurde. Der RA-Prozess muss vom Client (Verifier) initiiert werden und beginnt mit dem Senden des Number Used Once (nonce) sowie der gewünschten PCR-Bänke an den Server (Attester). Der Server übermittelt daraufhin den empfangenen nonce und die PCR an den TPM2 und erhält einen *Quote* zurück. Dieser wird anschließend an den Client gesendet und dort validiert.

Um diesen RA-Prozess innerhalb der IEC 61850 umzusetzen, ist eine detaillierte Betrachtung der bereitgestellten Sende- und Empfangsmöglichkeiten erforderlich. In der Norm des IEC 61850 sind drei unterschiedliche Varianten beschrieben, die geeignet sein könnten, diesen Prozess umzusetzen:

1. Der Server ist in der Lage, mittels einer sogenannten *Spontanmeldung* einen Bericht über die Informationsobjekte an den Client zu senden [Int10]. Aufseiten des Clients besteht an dieser Stelle jedoch kein direkter logischer Zusammenhang, da die Spontanmeldung der IEC 61850 dafür gedacht ist, bei ungeplanten Ereignissen eine Meldung über bestimmte Informationen und Parameter zu übermitteln. Diese Vorgehensweise ist in erster Linie auf Ereignisse der Primärtechnik ausgerichtet und wird durch ein zuvor definiertes Ereignis ausgelöst. Um im RA-Prozess das Erstellen und Versenden des Quotes auf dem Server auszulösen, bedarf es der vorherigen Übermittlung der nonce und der PCR-Bänke vom Client an den Server. Es wäre möglich, diese Attribute auf dem Server zu überwachen und bei einer Änderung einen Quote auszulösen und zu übermitteln. Die Übermittlung der Quote-Daten über den Weg der Spontanmeldung könnte mit dem Nachteil verbunden sein, dass die Spontanmeldung bereits Attribute an den Client übermittelt, bevor diese überhaupt im Datenmodell des Servers gesetzt wurden. In diesen Fall ist eine Verzögerung einzuplanen, um sicherzustellen, dass die TPM2-generierten Quote-Daten bereits als Objekt-Attribute auf dem IEC-61850-Datenmodell bereitstehen, bevor die eigentliche Spontanmeldung ausgelöst wird. Diese Umsetzung widerspricht nicht nur der Idee der Spontanmeldung, sondern scheint auch eine unnötig komplexe Lösung zu sein.

2. Der Server überwacht die PCR-Bänke und den nonce. Wird eine Veränderung erkannt, wird ein Quote ausgelöst und die generierten Quote-Daten werden als Objekt-Attribute auf dem IEC-61850-Datenmodell bereitgestellt. In diesem

Prozess kann der Client den Quote auch indirekt auslösen, indem er die PCR-Bänke und den nonce setzt. Im Gegensatz zum vorherigen Prozess ruft der Client diese Objektattribute zu einem späteren Zeitpunkt ab. Dies bringt den Vorteil, dass der Client zwischen dem Setzen der Objektattribute und der Abfrage der Quote-Attribute die Wartezeit selbst definieren und dadurch den Prozess genauer steuern kann.

3. Die dritte Möglichkeit folgt dem Prozess aus Punkt 2, jedoch stellt der Server die Quote-Daten zusätzlich als Datei zum Download zur Verfügung. Der Client kann die Daten nach dem Setzen der nonce und der PCR-Bänke mit einer kurzen Verzögerung als Datei abrufen und geht dabei nicht über die Objekt-Attribute. Diese Variante bietet den Vorteil, dass der Client ebenfalls die Kontrolle über den Prozess hat, eine aufwendige Abbildung der Remote-Attestation-Daten auf das IEC-61850-Informationsmodell und dessen Objektattribute ist aber nicht unbedingt erforderlich, da bei einem Dateitransfer das Datenformat nicht den BDA entsprechen muss, sondern mehr Freiheit bringt. Dies könnte im Fall von RA vorteilhaft sein, wenn der TPM2-Quote eine JSON-Struktur zurückgibt und der Client eine JSON-Struktur erwartet, um den Quote zu verifizieren. Eine fehleranfällige Konvertierung der Datentypen von JSON zu IEC-61850-basierten BDA würde entfallen.

Die Umsetzung erfolgte nach dem Konzept der dritten Variante und wird in den folgenden Abschnitten näher erläutert.

5.3.2 Implementierungsaufbau Server

Wie bereits im allgemeinen Abschnitt beschrieben, stellt der Server-Application-Code (Serverapplikation) die Basis und Businesslogik für die Implementierung und Integration des Datenmodells inklusive der Remote Attestation in das Kommunikationsprotokoll der IEC 61850 dar und ist als Schichtenmodell in Abbildung 5.7 wiedergegeben. Parallel zum Server-Application-Code sind die beiden C-Bibliotheken (TPM2-TSS und libIEC61850) sowie die für die libIEC61850 notwendige SCL-Konfigurationsdatei dargestellt. Die IEC-61850-Serveranwendung wird über eine eigene Extensible Markup Language, dt. erweiterte Auszeichnungssprache (XML)-Datei konfiguriert, die als Substation Configuration Description Language (SCL) bezeichnet wird. Diese Datei enthält Konfigurationsanweisungen für z. B. Berichte (Reports) sowie die darin enthaltenen Attribute und Klassen und die dem Server zur Verfügung stehenden

Klassen, Datenobjekte und deren Attributdefinitionen. Außerdem werden die verfügbaren *Logical Nodes* darüber definiert und die angebotenen Services, die in der IEC 61850 definiert sind, aktiviert bzw. konfiguriert.

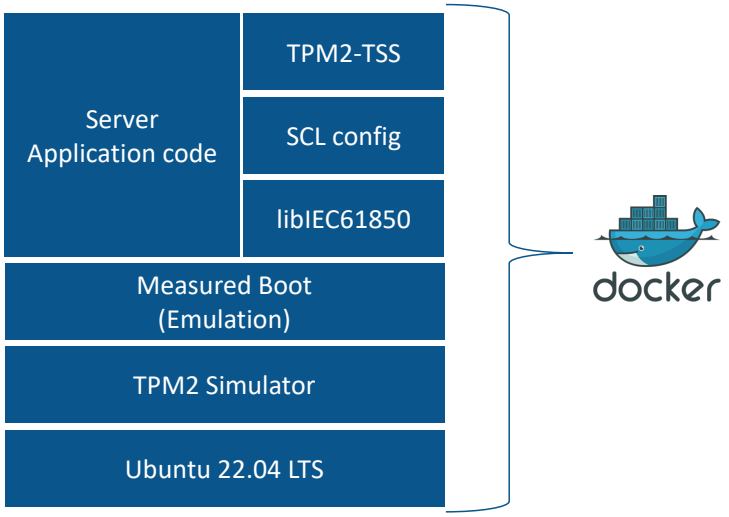

Abbildung 5.7.: Schichtenmodell der Komponenten und Implementierungen

RA-Datenmodell-Mapping auf IEC-61850-Objektattribute

Um die Daten für die Remote Attestation auf die IEC-61850-Objektattribute und -Datensätze abzubilden, müssen sie über die TSS-Schnittstelle abgefragt werden. Für diese Kommunikationsschnittstelle zwischen der IEC-61850-Anwendungslogik und dem TSS wurde die Feature API (FAPI) gewählt. Die FAPI ist die empfohlene Form der Interaktion mit dem TPM2, da die Komplexität für API-Benutzer reduziert ist und es ausreicht, Profile vorab zu definieren und zu laden. Ein weiterer Vorteil gegenüber niedrigeren API-Leveln ist die JSON-basierte Ein- und Ausgabe der FAPI. Diesem Vorteil steht auf der Programmierebene in C mit einem Mapping der IEC-61850-basierten Serverattribute ein gravierender Nachteil gegenüber: Alle Key-Value-Objekte müssen zunächst einem JSON-Objekt entnommen werden, auf passende Datentypen in C konvertiert werden und anschließend in die entsprechenden MMS-Attribute bzw. über IEC-61850-spezifische Basic Data Attribute (BDA) konvertiert werden. Auf diese Weise können die Objektattribute als genau definierte Klasse, wie im Datenmodell beschrieben, zur Verfügung gestellt werden. Dabei sind Abweichungen von der zuvor definierten Klasse notwendig, da beispielsweise bei dynamischen Arrays immer die aktuelle Länge der Daten bekannt sein muss. Client-seitig muss dieser fehleranfällige und unverhältnismäßig komplizierte Konvertierungsvorgang in die umgekehrte Richtung zu einem JSON erfolgen. Diese

Vorgehensweise funktioniert prinzipiell, verursacht aber einen erheblichen Aufwand in der Codebasis beim Client und Server.

5.3.3 Abbildung der Quote-Informationen als IEC-61850-Datensatz

Die IEC 61850 ermöglicht es, Datenattribute unterschiedlicher Datenobjekte zu einem definierten Datensatz zusammenzufassen und diesen Datensatz von einem Client abzufragen. Für die Bereitstellung der Remote-Attestation-Objektdaten und die Umsetzung des Informationsmodells wurde in dieser Arbeit ein eigener Datensatz erstellt, damit die entsprechenden Quote-Daten als solche abgerufen bzw. ausgelesen werden können. Das Skript 5.2 zeigt einen Ausschnitt der Konfiguration dieses Datensatzes. Das vollständige Skript ist im Anhang unter Skript A.13 dokumentiert.

Skript 5.2: Serverseitige Datensatzkonfiguration für die Remote-Attestation-Informationen

```
1 <DataSet name="QuoteDS" desc="TPM Quote Data Set">
2     ...
3     <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
          doName="TpmQuote2" daName="sigScheme"/>
4     <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
          doName="TpmQuote2" daName="sigSchemeHashAlg"/>
5     <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
          doName="TpmQuote2" daName="magic"/>
6     <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
7     ...
8 </DataSet>
```

In dem Skript ist ebenfalls die Zuordnung zur Klasse der *Logical Node GGIO* erkennbar. Dieses stellt gegenüber der in Kapitel Informationsmodell für Remote Attestation definierten Integration eine Abweichung dar, die unabdingbar war, weil das Erstellen einer eigenen *Logical Node* nicht dokumentiert ist und sich aus den Codebeispielen nicht ausreichend ableiten ließ. Für den Zweck des Demonstrators stellt diese Abweichung keinen Nachteil dar.

Das Skript 5.3 zeigt die Deklaration des IEC-61850-Datenobjekts (*DOType*) sowie die *common data class* (cdc) *TQC* und die vorgesehenen Datenattribute, die Datentypen (*btypes*) einschließlich der *functional constraint (FC)* (dt. funktionale Einschränkung). Um auch Arrays abdecken zu können, wird in der Zeile 6 des Skript 5.3 ein *structured data object (SDO)* erstellt, das auf ein weiteres angelegtes Attribut verweist. Das vollständige Skript ist im Anhang dokumentiert (siehe Skript A.14).

Skript 5.3: Ausschnitt der Deklaration der Datenobjekte und Datenattribute in der SCL-Datei

```
<DOType id="TPM_2_Quote_2" cdc="TQC">
  ...
  <DA name="sigScheme" bType="VisString255" fc="OR"/>
  <DA name="sigSchemeHashAlg" bType="VisString255" fc="OR" />
  <DA name="magic" bType="VisString255" fc="DC" />
  <SDO name="pcrSelectArr" type="pcrSelectionArr" count="32"/>
  ...
</DOType>
```

Mit Beginn der Implementierungsarbeiten wurde in iterativer Vorgehensweise nach der optimalen Implementierungslösung gestrebt. In der ersten Iteration ist das Informationsmodell der RA als Datenmodell im IEC-61850-Server implementiert worden. Als erster Schritt wurden die Datenattribute der RA auf die BDA der IEC 61850 abgebildet. Während der Implementierungsarbeiten hat sich gezeigt, dass die Konvertierung des vorliegenden JSON-Strings mit den Quote-Informationen der Remote Attestation in die in der IEC 61850 definierten Datenprimitiven, Basic Data Attribute (BDA), aufwendig, kompliziert und dadurch fehleranfällig ist. Hinzu kommen zur Laufzeit wechselnde Arraylängen, die serverseitig aufwendig zu implementieren sind und zusätzlich zuvor als Objektattribute in der SCL-Datei definiert werden müssen. Außerdem musste das Informationsmodell erweitert werden, um für jedes Array ein weiteres Feld für die tatsächliche Länge zu schaffen, damit der Client diese wieder in eine JSON-Struktur zurückführen kann. Da der Quote mit dem TSS auf der FAPI-Ebene erzeugt wird, wird eine JSON-Struktur auf das IEC-61850-Datenmodell abgebildet. Client und Server tauschen ihre Daten über dieses Datenmodell aus und der Client wandelt dieses Datenmodell wieder in einen JSON-String um, damit er es validieren und weiterverarbeiten kann. Damit sind die Voraussetzungen für die vorgestellte Variante 1 und 2 implementiert, in Tests jedoch nicht zuverlässig genug, um den Anforderungen der vorliegenden Arbeit zu genügen. Deshalb wird im nächsten Abschnitt die Umsetzung der dritten Prozessvariante vorgestellt.

Prozessergebnis aus Implementierungsarbeiten

Mit dem neuen Wissen aus der praktischen Implementierung der Quote-Attribute in die Objektattribute und Datensätze des IEC 61850 wurde entschieden, den Aufwand und die Fehler- und Störanfälligkeit zu reduzieren. Dazu wurde im Sinne der FAPI-Idee gehandelt und auf die IEC-61850-Funktion des Dateitransfers zurückgegriffen. Daraus resultiert die Implementierung der vorgestellten Prozessvariante 3, die im Detail in Abbildung 5.8 als Sequenzdiagramm gezeigt wird.

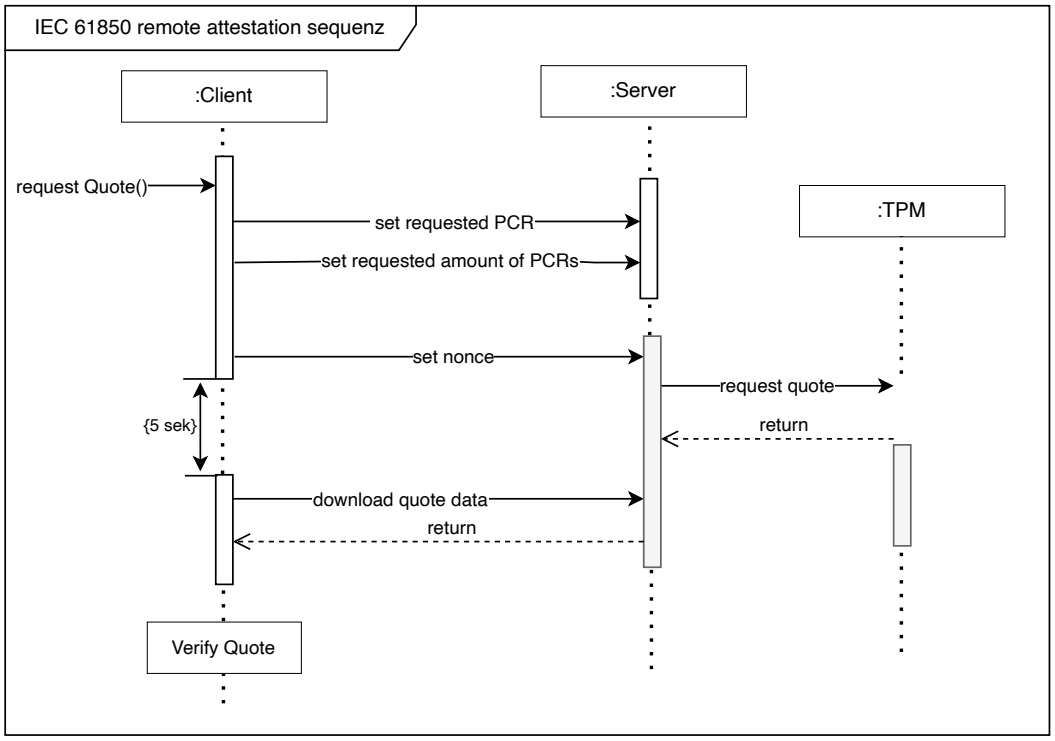

Abbildung 5.8.: Remote-Attestation-Ablauf mittels IEC-61850-Client und -Server

Der Client setzt auf dem Server zuerst die PCRs-Informationen in die dafür vorgesehenen Objektattribute des zuvor definierten Informationsmodells. Danach wird der nonce auf demselben Weg gesetzt. Der Server überwacht dieses Objektattribut und initiiert bei einer Veränderung einen TPM2-Quote-Befehl. Der zurückgegebene Quote wird danach von der Serveranwendung in das IEC-61850-Datenmodell überführt und zusätzlich als JSON-Datei bereitgestellt. Der Client nutzt den in der IEC 61850 spezifizierten Dateiaustausch, um die JSON-Datei herunterzuladen. Damit stehen die Quote-Informationen als Objektattribute auf dem Server zur Verfügung und können über IEC 61850 abgerufen oder empfangen werden. Das Skript 5.4 zeigt eine gekürzte Quote als JSON-Datei sowie die zugehörigen Beschreibungen bzw. Datentypen der jeweiligen Attribute und deren Werte, wie sie nun auf dem Server zum Download bereitgestellt werden.

Skript 5.4: Abbildung einer Quote2-Struktur mit Erklärung der Schlüssel-Werte (key-value) im JSON-Format

```
1 {
2   "success": true,
3   "responseCode": "TSS2_RC_SUCCESS",
4   "quoted": {
5     "magic": "TPM_GENERATED_VALUE",
6     "type": "TPM_ST_ATTEST_QUOTE",
```

```
    "qualifiedSigner": "Signierender Schluessel",
    "extraData": "Vom Aufrufer bereitgestellte Nonce",
    "clockInfo": {
      "clock": "Zeit seit TPM-Initialisierung",
      "resetCount": "Anzahl der TPM-Resets",
      "restartCount": "Anzahl der TPM-Neustarts",
      "safe": "Sicherheitsstatus der TPM-Uhr"
    },
    "firmwareVersion": "Firmware-Version des TPM",
    "attested": {
      "quote": {
      "pcrSelect": "Ausgewaehlte PCR-Indizes",
      "pcrDigest": "Digest der ausgewaehlten PCR-Werte"
      }
    }
  },
  "signature": {
    "sigAlg": "Signaturalgorithmus",
    "sig": "Signaturdaten"
  }
}
```

5.4 Integration der Sicherheitskonfigurationsinformationen

In diesem Abschnitt werden die praktische Konzeption und Implementierung der Sicherheitskonfigurationsinformationen (SKI) beschrieben. Dazu wird das zuvor vorgestellte Informationsmodell im IEC-61850-basierten Server praktisch umgesetzt, sodass es vom Client (Controlcenter) abgefragt werden kann. Dafür wird ebenfalls das IEC-61850-basierte Client-Server-System erweitert und die SKI werden praktisch integriert. Die wesentlichen Implementierungsdetails und Konzeptbestandteile werden dazu erläutert.

5.4.1 Integrationskonzept Remote-Attestation

Im Gegensatz zur Integration der Remote Attestation gibt es für die Integration der Sicherheitskonfigurationsinformationen (SKI) keine API, die die notwendigen Informationen zur Verfügung stellen würde. Um diese Lücke zu schließen, wurde eine

Möglichkeit entwickelt, mit der die verschiedenen Anwendungen ihre jeweiligen Sicherheitskonfigurationen mitteilen können. Solche Anwendungen sind zum Beispiel das Betriebssystem, die IEC-61850-Anwendung oder andere Softwarekomponenten, die auf dem IED ihre Sicherheitskonfigurationen mitteilen. Dabei wurde bewusst bedacht, dass es sich um mehrere Anwendungen bzw. unabhängige Softwaremodule handeln kann. Obwohl der Fokus dieser Arbeit die Übertragung, Bereitstellung und Integration in die Protokolle und Datenmodelle innerhalb der TC57-Architektur sind, wird dieser Punkt konzeptionell betrachtet werden, da er die Basis für die Bereitstellung der Daten darstellt. Im Rahmen der vorliegenden Arbeit wird dieser wichtige Punkt in Form einer ersten Konzeptidee adressiert.

Um die Komplexität nachzuvollziehen, muss zunächst die zukünftige Entwicklung berücksichtigt werden, nach der ein IED über eine Vielzahl an Softwarekomponenten verfügen kann, die über ein Betriebssystem und eine eingebettete Anwendung zur Prozesssteuerung hinausgehen und durch virtuelle Systeme auf einem IED bereitgestellt werden [KKL23]. Dies kann im Kontext dieser Arbeit beispielsweise eine eigenständige Software zum Aufbau von Verbindungen vom Typ Virtual Private Network (dt. virtuelles privates Netzwerk) (VPN) oder ein Softwaremodul zur biometrischen Authentifizierung sein. Außerdem wird davon ausgegangen, dass zukünftig moderne IEDs zum Einsatz kommen werden, bei denen mit unterschiedlichen Softwaremodulen und eher offenen Betriebssystemen zu rechnen ist. Diese ermöglichen die Installation beliebiger Softwarekomponenten und Module. Um ein IED aus der Ferne abfragen zu können, ist ein zentrales Interface erforderlich, welches diese Funktion nach außen bereitstellt und intern auf die SKI bzw. die dafür benötigten Datenkomponenten zugreifen kann. Beim SNMP beispielsweise wird dies von einem Agenten übernommen. Eine Softwareanwendung kann sich bei dem Agenten registrieren und diesem seine Informationen bereitstellen oder beim Agenten verfügbare Informationen abfragen. Anschließend bietet der Agent diese Informationen zentral nach außen an.

Um die Komplexität im Rahmen der vorliegenden Arbeit zu reduzieren und eine leichtgewichtige Möglichkeit für die Abfrage der SKI bereitzustellen, wurde auf ein komplexes Agentensystem wie beispielsweise bei SNMP verzichtet. Wie vorgesehen, stellt die IEC-61850-Serveranwendung deshalb über ihre Datenmodelle die Schnittstelle zur Abfrage der SKI dar. Um die Fähigkeit zur Integration weiterer Datenquellen zu ermöglichen, werden diese als JSON-Datei an einem festen Ort abgelegt und von der Server-Anwendung eingelesen. Ein wesentlicher Vorteil dieses Verfahrens besteht darin, dass die Dateien und Verzeichnisse kryptografisch gemessen und als PCR im TPM2 erfasst werden können. Des Weiteren erlaubt diese

Methode die Verwendung der Konfigurationsdateien als Konfigurationen für weitere auf dem IED befindliche Softwares und Systemkomponenten.

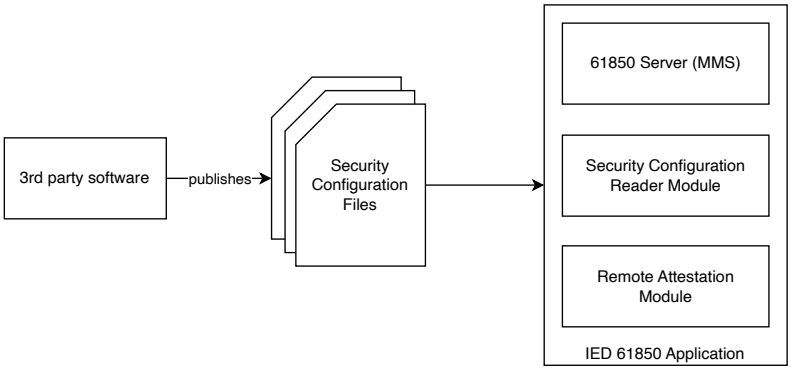

Abbildung 5.9.: Prozess der Entstehung der Sicherheitskonfigurationseinstellungen

Für den Demonstrator in der vorliegenden Arbeit wird die Vorgehensweise als Push-Variante bezeichnet und umgesetzt. Abbildung 5.9 visualisiert den Prozess zusammenfassend. Bestehende Software publiziert ihre jeweiligen Sicherheitskonfigurationen als JSON-Datei, welche von der IEC-61850-Server-Anwendung eingelesen und vom Sicherheitskonfigurationsmodul in das Datenmodell integriert wird. Das Sicherheitskonfigurationsmodul verarbeitet die Informationen weiter und bildet diese, wie in Kapitel 4.3 (Modellierung in IEC 61850, S. 68) beschrieben, auf das IEC-61850-Datenmodell ab.

5.4.2 Server-Implementierung des Konzepts

Die Implementierung der SKI in den Demonstrator erfolgte exemplarisch und dient der Demonstration des Integrationskonzepts und der Evaluation. Die Prozessschritte der Implementierung werden schrittweise erläutert. Im ersten Schritt wurden die SKI als JSON-Datei händisch erzeugt, damit diese von der IEC-61850-Serveranwendung eingelesen werden kann.

Für die in der JSON-Datei enthaltenen SKI wurde auf dem IEC-61850-Server über die SCL-Datei ein IEC-61850-Datensatz (dataset) erstellt, damit die SKI einheitlich abgefragt werden können. Um alle im Kapitel Ergebnisse der Analyse identifizierten Sicherheitsanforderungen abzubilden, müssten diese jeweils einzeln deklariert werden. Aufgrund der Menge dieser und des demonstrativen Charakters dieses Kapitels sind sieben ausgewählte SKI in dem Datensatz angelegt. Jedes Datenobjekt (DO), dessen Attribute (DA) über den Datensatz abgefragt werden sollen, ist jeweils in der SCL-Datei deklariert worden. Das Skript 5.5 zeigt die Datensatzdeklaration des

Demonstrators der vorliegenden Arbeit. Darin ist zu erkennen, dass es sich um funktionsbeschränkte Attribute (*FCDA, functional constraint data attribute*) handelt, die mit der funktionalen Beschränkung (fc) DC (Description, dt. Beschreibung) belegt sind. Die Bezeichnung des jeweiligen Datenobjekts (doName) leitet sich aus dem Informationsmodell für die SKI ab (siehe Kapitel 4.1, S. 56). Auch muss deklariert sein, in welcher *Logical Node* (LN) das Objektattribut zu finden ist. Dies wird mit den Bezeichnern *lnClass* (Klasse der Logical Node) und *lnInst* (Instanz der Logical Node) definiert.

Skript 5.5: Exemplarisch definiertes Dataset für Sicherheitskonfigurationsinformationen (SKI)

```
1
2  <DataSet name="SecurityConfigurations">
3      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
           doName="CR_1_1_RE_2" daName="available"/>
4      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
           doName="CR_1_1_RE_2" daName="activated"/>
5      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="2"
           doName="6_3_4_3" daName="operationMode" />
6      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="2"
           doName="6_3_4_3" daName="available_cipher_suites" />
7      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="2"
           doName="7_2" daName="ldapVersion"/>
8      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="2"
           doName="7_2" daName="ldapUnavailLog"/>
9      <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="2"
           doName="7_2" daName="jwtUnavailLog"/>
10 </DataSet>
```

Damit das beschriebene Dataset mit den SKI auch als Bericht (Report) abgefragt werden kann, ist wie in Skript 5.6 ein *ReportControlBlock* (RCB) definiert. Dieser ermöglicht den Abruf des zuvor definierten Datensatzes durch einen Client und konfiguriert weitere Eigenschaften für den Datensatz und dessen Attribute. Beispielsweise wird eine Report-ID (*rptID*) festgelegt und ebenfalls bestimmt, ob der Datensatz bzw. dessen Attribute aus dem Zwischenspeicher gelesen werden dürfen. Zudem können Trigger (*TrgOps*) festgelegt werden, die den Datensatz z. B. im Rahmen einer Spontanmeldung an einen Client senden.

Skript 5.6: Konfigurationen des Report-Control-Blocks

```
1  <ReportControl name="SecurityConfigurationsRCB" confRev="0" datSet=
       "SecurityConfigurations" rptID="SecConfDS1" intgPd="10011"
       buffered="false">
2      <TrgOps period="true"/>
```

```
3       <OptFields dataSet="true" bufOvfl="false" configRef="true"
            dataRef="false" entryID="true" reasonCode="true" timeStamp="
            true" seqNum="true"/>
4       <RptEnabled max="1"/>
5   </ReportControl>
```

Im nächsten Schritt erfolgte die Implementierung der Objekt-Attribute im IEC-61850-Server. Dies ist in Skript 5.7 dargestellt. Dort werden die aktuellen Attribute bzw. Zustände in die sieben SKI gesetzt. Da es sich in diesem Beispiel um lediglich sieben SKI handelt, wurde auf ein Einlesen externer JSON-Dateien mit den hinterlegten SKI verzichtet. Zusätzlich ist im Rahmen dessen eine Unflexibilität der SCL-Datei für diesen Prozess festgestellt worden. Die SCL-Datei dient der Konfiguration eines IEDs und insbesondere der daran angeschlossenen Primärtechnik. Dabei wird davon ausgegangen, dass Datenobjekte und deren Attribute fix sind und sich nicht zur Laufzeit bzw. während des laufenden Betriebs verändern (können). Außerdem müssen die möglichen Attribute eines Datenobjekts für SKI zuvor bekannt sein.

Als praktisches Beispiel ist Zeile 16 in Skript 5.7 geeignet. Dort soll die Anforderung der Multi-Faktor-Authentifizierung (MFA) abgebildet werden. Wenn eine MFA aktiviert ist, kann dies mittels true oder false bestätigt werden. Da die genauen Konfigurationen und Einstellungsmöglichkeiten sowie der Geltungsbereich dieser nicht genauer in den Normen spezifiziert sind, kann dies mittels IEC 61850 nicht generalistisch gelöst werden. Denn die entsprechenden Objektattribute müssen vorab definiert bzw. in der SCL hinterlegt sein, um innerhalb des IEC-61850-Servers mit diesen Objektattributen arbeiten zu können. Dies ist ein weiteres Beispiel, das zeigt, wie wichtig ein standardisiertes Datenmodell für SKI ist, denn dann könnte die SCL zumindest dafür modelliert werden. Der sequenzielle Ablauf zur Abfrage der SKI durch den Client ist in Abbildung 5.10 dargestellt. Die Befehle zur serverseitigen Initialisierung sind im Anhang unter Skript A.15 aufgeführt.

Skript 5.7: Abfragbare Sicherheitskonfigurationseinstellungen, exemplarisch

```
1
2   IedServer_updateVisibleStringAttributeValue(iedServer,
3   IEDMODEL_GenericIO_GGIO2_6_3_4_3_operationMode, &tls_operation_mode
        );
4
5   IedServer_updateVisibleStringAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO2_7_2_ldapVersion, ldapVersion);
6
7   IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO2_7_2_ldapUnavailLog, true);
8   IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO2_7_2_jwtUnavailLog, true);
```

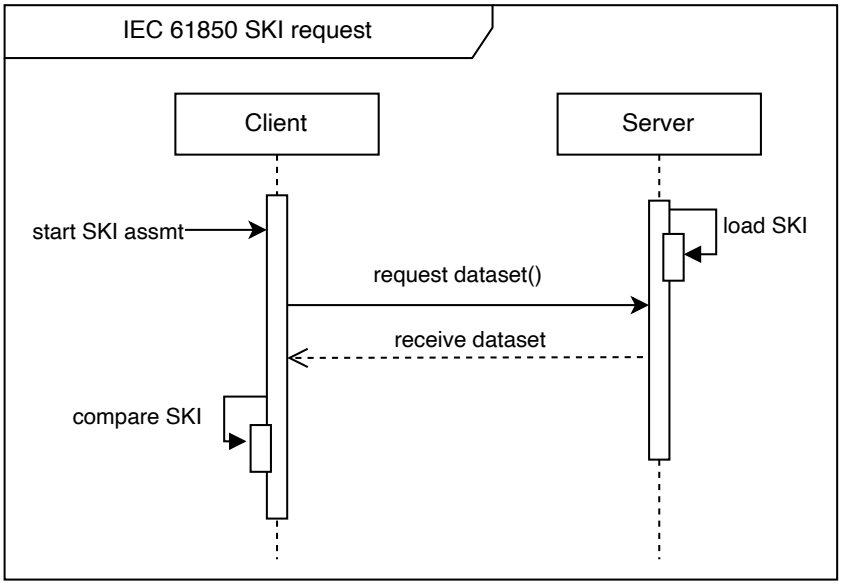

Abbildung 5.10.: Sequenzieller Ablauf der SKI-Abfrage

```
9
10  // keyProtHsm
11  IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO4_CR_1_1_RE_2_activated, true);
12
13  IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO4_CR_1_1_RE_2_activated, true);
14
15  // mfaHumans
16  IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO4_CR_1_9_RE_1_available, true);
17
18  IedServer_updateBooleanAttributeValue(iedServer,
        IEDMODEL_GenericIO_GGIO4_CR_1_9_RE_1_activated, true);
```

5.5 Gesamtaufbau Demonstrator

In diesem Abschnitt wird der Gesamtaufbau des Demonstrators beschrieben. Hierbei wird neben dem bisher ausführlich dargelegten Serveraufbau insbesondere auf den Client und dessen Umsetzung eingegangen. Wie eingangs im Kapitel beschrieben, vertritt der Client die Rolle des Controlcenters, um SKI und RA-Informationen von dem IEC-61850-Server bzw. einer IED abzurufen und auswerten zu können. Dazu muss der Client in der Lage sein, über ein LAN/Netzwerk mittels IEC-61850-basierten MMS-Protokolls die Datensätze abzurufen. Neben den IP-Adressen und

den Ports der abzufragenden Server benötigt der Client außerdem die jeweiligen Referenzwerte. Die Referenzwerte ermöglichen dem Client, die Serverinformationen zu vergleichen und dadurch Auskunft über das Vertrauen einer IED zu liefern. Die

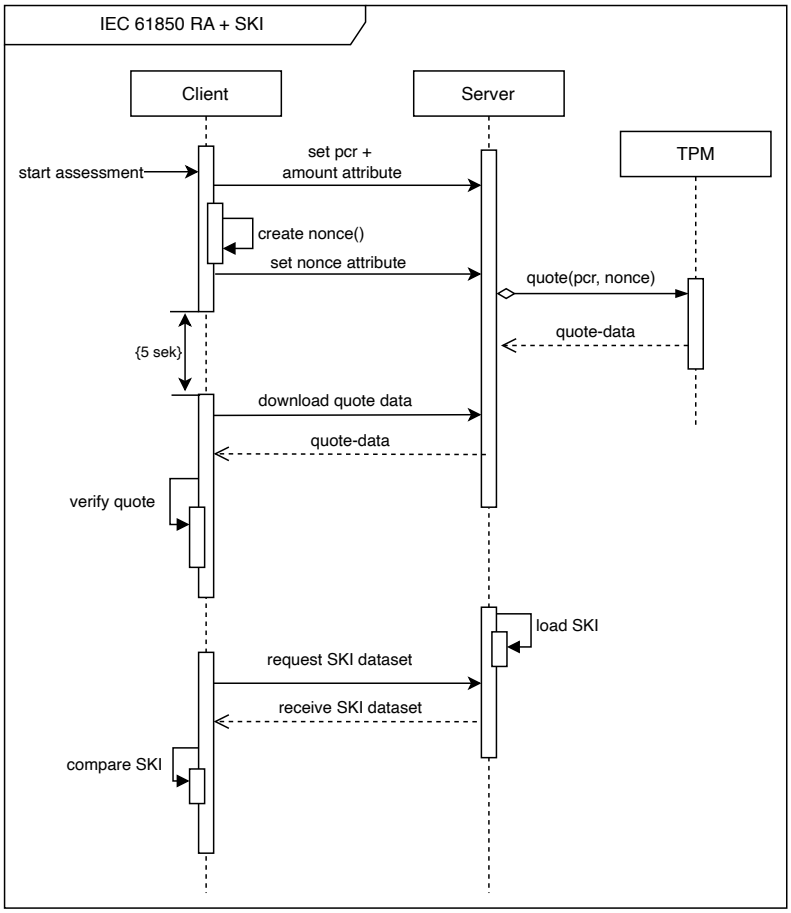

Abbildung 5.11.: Gesamtablauf Abfrage Remote Attestation und SKI als Prozessdiagramm

Ausgangslage für den Aufbau des IEC-61850-Clients wurde bereits im Rahmen der Entwicklungsumgebung unter Punkt 5.2.2 vorgestellt. Der gesamte Ablauf zwischen Client und Server ist als Sequenzdiagramm in Abbildung 5.11 dargestellt. Zusammengesetzt ergeben RA und die Abfrage der SKI den Gesamtaufbau. Zuerst wird die Remote Attestation durchgeführt und ausgewertet, daran anschließend die Abfrage der SKI.

5.6 Zusammenfassung

In diesem Kapitel wurden die Konzeption, Architektur und Umsetzung des Demonstrators gezeigt. Die Umsetzung erfolgte aufbauend auf den vorherigen Kapiteln,

sodass die Informationsmodelle für die Remote Attestation und die SKI instanziiert werden konnten. Dazu wurden zunächst wichtige Bibliotheken für die Kommunikation mit dem TPM2 und Kommunikationsstacks identifiziert und erläutert. Darauf basierend ist eine Client-Server-Architektur implementiert und vorgestellt worden. Anschließend wurde diese schrittweise erweitert, um die Funktionalitäten der Remote Attestation und der Abfrage der SKI zu integrieren. Dabei wurden spezifische Herausforderungen beschrieben und im Lösungskonzept berücksichtigt. Zusätzlich sind die Kommunikationsabläufe zwischen Client und Server als Prozessdiagramm aufgezeigt worden. Diese Implementierung stellt die praktische Umsetzung der Datenmodelle aus dem vorherigen Kapitel dar und bildet damit die Basis für die Evaluation im folgenden Kapitel.

6 Evaluation

Die Evaluation zielt darauf ab, die vorgestellten Konzepte und deren Umsetzung einer systematischen und empirischen Analyse zu unterziehen. In diesem Kapitel wird zunächst die Vorgehensweise vorgestellt, darauf folgend die Evaluationsumgebung sowie die Funktionstests des Demonstrators. Abschließend werden die Evaluationsergebnisse präsentiert und diskutiert.

6.1 Vorgehensweise

Für die vorliegende Arbeit wurde der Design Science Research Process (DSRP) als grundlegende wissenschaftliche Forschungsmethodik für Informationssysteme angewendet (siehe Kapitel 1.3). Zur Umsetzung der Methodik werden die implementierten Funktionen der Remote Attestation sowie die Abfrage von SKI anhand von Funktionstests evaluiert. Diese Tests stellen sicher, dass die implementierten Funktionen aus dem vorigen Kapitel innerhalb der Evaluationsumgebung funktionieren und der Demonstrator mitsamt der einzelnen Forschungsartefakte sowie des Datenaustauschs zwischen Client und Server korrekt arbeitet. Darauf aufbauend werden weitere Tests durchgeführt, mit denen aufgezeigt wird, dass Manipulationen erkannt werden können.

Diese Funktions- und Manipulationstests werden anschließend dazu verwendet, die Fähigkeiten des Demonstrators in Bezug auf die vorgestellte Trust-Pyramide (siehe Kapitel 1.1) darzulegen. Darüber wird gezeigt, dass die Remote Attestation und die SKI geeignet sind, das Vertrauen von IEDs zu bewerten. Dazu wird eine sogenannte Trust-Matrix in Form einer Transformationsfunktion eingeführt und vorgestellt, anhand derer das Vertrauen evaluiert werden kann.

Im Anschluss an die Funktionstests erfolgt die Evaluierung gegen die bereits in Kapitel 1.2.2 beschriebenen nichtfunktionalen Anforderungen. Diese nichtfunktionalen Anforderungen stellen die Bedingungen, unter denen der Lösungsansatz bzw. der Demonstrator seine Funktionen erfüllen muss. Auf der Grundlage des Demonstrators sowie unter Berücksichtigung der während der Design- und Entwicklungsphase gewonnenen Erfahrungen und der Umsetzung der Szenarien erfolgt eine qualitative

Beurteilung der nichtfunktionalen Anforderungen. Zusammenfassend besteht die Evaluation aus den folgenden Schritten:

1. Funktionstests: SKI und Remote Attestation
2. Ableiten und Testen der Trust-Matrix
3. Evaluation der nichtfunktionalen Anforderungen

Eine Übersicht der Anforderungen sowie der Art der Evaluation ist in Tabelle 6.1 gezeigt.

Tabelle 6.1.: Anforderungen und Art der Evaluation

Name	Anforderung	Art
Funktionale Korrektheit	Die Ergebnisse aus unterschiedlichen Abfragen des Servers übermitteln die korrekten Werte und die Analyse der Ergebnisse ist ebenfalls korrekt.	quantitativ
IT-Sicherheitsstandards	Im Gesamtkonzept sollen Anforderungen aus IT-Sicherheitsstandards berücksichtigt werden.	argumentativ
OT-Sicherheitsstandards	Im Gesamtkonzept sollen Anforderungen aus OT-Sicherheitsstandards berücksichtigt werden, die auf die Energienetzdomäne angewendet werden können.	argumentativ
Plattformintegrität	Die Plattformintegrität soll mittels Remote Attestation berücksichtigt werden.	argumentativ
Interoperabilität	Die Lösung und das Konzept sollen in die Referenzarchitektur der TC57 integrierbar sein (Seamless integration architecture)	argumentativ
Abfragbarkeit	Beschreibt, wie Sicherheitskonfigurationen auf OT-Ebene von einer RTU eingesammelt werden.	argumentativ
Vorschlag eines Standards	Es soll ein technisches Vorgehen zum Erfassen von SKI vorgeschlagen werden	argumentativ / Funktionstest

In Bezug auf die Evaluationsmethode wird zwischen qualitativer und argumentativer Evaluierung differenziert. Die funktionale Korrektheit wird anhand definierter Funktionstests evaluiert. Die Tests werden in den jeweiligen Abschnitten vorgestellt. Die erfolgreiche Umsetzung der Funktionstests bildet die Voraussetzung für die argumentative Evaluation der nichtfunktionalen Anforderungen. Da die nichtfunktionalen Anforderungen im Wesentlichen auf argumentativer Basis evaluiert werden, stellen die Umsetzung und Funktionalität des Demonstrators eine grundlegende Voraussetzung hierfür dar.

6.2 Evaluationsumgebung

Die Evaluationsumgebung ist in die bereits vorgestellte Referenzarchitektur der TC57 Power System Architecture Model eingebettet bzw. in für die vorliegende Arbeit notwendigen Bestandteilen eingebettet. In diesem Zusammenhang werden die minimal notwendigen Kommunikationskomponenten nachgestellt, wobei die Primärtechnik unberücksichtigt bleibt. Der Aufbau der Evaluationsumgebung ist in Abbildung 6.1 gezeigt und besteht aus einem Controlcenter sowie zwei demonstrativen Unterstationen (Substation 1 und 2). Diese sind über TCP/IP mit einem Layer-3-Switch in einem Klasse-C-Netzwerk verbunden. Das Controlcenter wurde als

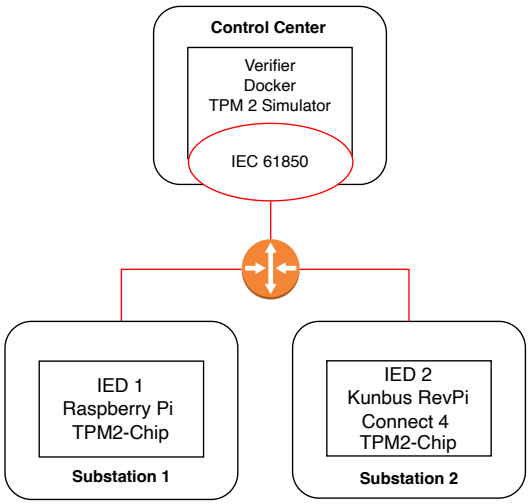

Abbildung 6.1.: Instanziierung der Client-Server-Komponenten als Laboraufbau

Docker-Container instanziiert, die Unterstationen enthalten jeweils ein IED, welches durch einen Raspberry Pi und ein Kunbus RevPi repräsentiert wird. Beide Geräte sind mit einem TPM2 ausgestattet. Der Kunbus Revolution Pi Connect 4 wurde für industrielle Anwendungen und Einsätze entwickelt [Kun] und repräsentiert ein modernes IED-Industrial-IoT-Gateway, welches auf einem Linux-basierten Open-Source-Betriebssystem basiert (standardmäßig ein angepasstes Raspberry Pi OS). Bei dem Raspberry Pi handelt es sich um das Modell 4b, welches mit einem TPM2-Evaluationsboard ausgestattet ist. Bei dem Evaluationsboard handelt es sich um das Infineon Optiga SLB 9670, welches auf die GPIO des Raspberry Pi aufgesteckt wird. Dadurch verfügt der Raspberry Pi ebenfalls über einen echten TPM2-Chip. Auf den beiden Geräten ist der zuvor entwickelte IEC-61850-Server installiert und fungiert dort als IEC-61850-Applikation.

Die Implementierung des Servers auf die echte Hardware unterstreicht die Funktionalität auf realer Hardware. Im Gegensatz zur (isolierten) Entwicklungsumgebung

ist hierbei mit anderen Störeinflüssen zu rechnen und dies schafft somit beispielsweise durch nebenläufige Prozesse des Betriebssystems realistischere Bedingungen. Zudem stehen auf der echten Hardware deutlich geringere Systemressourcen zur Verfügung. Der Raspberry Pi unterstützt nativ kein Measured Boot, daher sind beide IEDs für die Evaluation mit dem Measured-Boot-Simulator ausgestattet, der in diesem Falle jedoch mit dem echten TPM2-Chip interagiert. Das Controlcenter bzw. der IEC-61850-Client wurde als Docker-Container instanziiert. Als Docker-Host wurde ein Apple MacBook Pro M1 (2021) mit macOS 14.4.1 (Sonoma) eingesetzt. Die folgende Tabelle 6.2 zeigt die Geräteliste, die IP-Adresse sowie die Funktionen der Geräte und den Gerätetyp.

Tabelle 6.2.: Geräteliste mit IP-Adressen und Gerätetyp des Demonstratoraufbaus

Ort	IP-Adresse	Funktion	Gerätetyp
Controlcenter	192.168.188.41	Client	Apple MacBook Pro M1, Docker, TPM2-Simulator
Substation 1	192.168.188.40	IEC 61850-Server	Raspberry Pi 4b, Infineon Optiga TPM29670_Raspberry
Substation 2	192.168.188.25	IEC 61850-Server	Kunbus RevPi Connect 4, integrierter TPM2

6.3 Funktionstests

Die Funktionsfähigkeit und Korrektheit des Demonstrators wurden durch die Ausführung von Anwendungstestfällen evaluiert. Im Rahmen der Evaluierung werden jeweils Anwendungstestfälle für Funktionen der Remote Attestation und für die SKI beschrieben. Diese praktischen Anwendungstestfälle stellen sicher, dass jedes IED in der Evaluationsumgebung wie vorgesehen arbeitet und die Verbindung zum Client ebenfalls steht. Die Testfälle der Funktionstests bilden die Grundlage für eine Abbildung auf die Trust-Pyramide und sind im Folgenden beschrieben.

6.3.1 Testfälle zur Abfrage von Sicherheitskonfigurationen

Die folgenden Testfälle adressieren die Integration der SKI-Abfrage. Mit diesen Tests wird die Funktionsfähigkeit der Integration und des Konzepts in der Evaluationsumgebung evaluiert. Wie bereits im vorherigen Kapitel dargelegt, wurde ein exemplarischer Teil der identifizierten SKI implementiert. Im Rahmen dieses Tests werden aus jedem der in Kapitel 3 beschriebenen IT-Sicherheitsstandards zwei SKI

abgefragt und in der Tabelle 6.3 zusammenfassend dargestellt. Die hinterlegten Konfigurationen sind von exemplarischem Charakter und haben keine Auswirkungen auf die tatsächliche Konfiguration des IEC-61850-Servers. Ein Konfigurationsbeispiel ist in Skript 6.1 gezeigt und repräsentiert die unterstützten Cipher-Suites in JSON-Notation. Diese Anforderung stammt aus der Norm IEC 62351-3 und definiert die erlaubten Cipher-Suites.

Der Testablauf wurde in der Evaluationsumgebung durchgeführt. Für den Anwendungstestfall der Abfrage der SKI wurde durch den Client eine Verbindung zum Server in der Substation 1 über das IEC-61850-Protokoll initiiert. Der Client fragt die Datenattribute auf den Logical Nodes des Servers ab. Nach erfolgreicher Abfrage wurden aufseiten des Clients die Datenattribute gegen die hinterlegten Soll-Werte automatisiert abgeglichen und die Konformität wurde bewertet. Der Ablauf und die Ergebnisse sind im Konsolenfenster der IDE ausgegeben worden. Mit dem Funktionstest wurde sichergestellt, dass die Implementierung korrekt funktioniert. Aus dem Grund wurde auch ein negativer Test durchgeführt, bei dem die in den Servern hinterlegten Konfigurationen Abweichungen vom Soll enthielten und entsprechend nicht konform waren. Für die jeweiligen Tests wurden die Server in den Substations mit korrekten und vom Soll abweichenden SKI-Konfigurationen gestartet. Die dazugehörigen Tests (ID-1, ID-2) werden im Folgenden kurz beschrieben.

Skript 6.1: Ausgewählte SKI der IEC-61850-Server in Substation 1 und Substation 2 als JSON-Objekt

```
{
"logical-node-name": "IEC_62351_3",
"logical-node": "GGIO2",
"data-objects": [
{
  "id": "6_3_4_3",
  "name": "supported cipher suites",
  "configuration": {
    "available_cipher_suites": [
      "TLS_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_DH_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
    ]}}]}
```

Die detaillierte Repräsentation der gesamten SKI als JSON-Objekt ist in Anhang A.5 hinterlegt.

Test-ID 1: Korrekte Auswertung der SKI-Informationen

Dieser Funktionstest stellt sicher, dass die korrekte Übertragung und Auswertung im Controlcenter (Clientseite) sichergestellt sind. Dazu sind die beiden IEC-61850-Server der Substation 1 und Substation 2 mit der korrekten Konfiguration gestartet worden. Der Client wurde ebenfalls mit der korrekten Konfiguration der Sollwerte gestartet und fragte beide Server in den Substations ab. Anschließend wertete der Client die von den Servern abgefragten Informationen aus, indem er sie gegen die Sollwerte verglich. Die Konfiguration dieses Tests ist im Anhang A.4 als Testprotokoll beschrieben.

Test-ID 2: Erkennung von SKI-Abweichungen

Dieser Funktionstest stellt sicher, dass manipulierte bzw. falsche Sicherheitseinstellungen entdeckt werden. Die Gefahren durch falsche oder unzureichende Sicherheitseinstellungen wurden eingangs bereits motiviert (siehe Kapitel 1.1). Für die Umsetzung wurde in der Evaluationsumgebung eine vom Soll abweichende Konfiguration auf dem Kunbus-System hinterlegt. Bei der Abfrage der SKI durch die Leitstelle wurde erwartet, dass die Abweichung entdeckt würde. Zu diesem Zweck sind aus jeder Sicherheitsnorm zwei exemplarische Beispiele gewählt worden. Die folgende Tabelle 6.3 listet die gewählten Sicherheitsanforderungen auf.

Tabelle 6.3.: Übersicht der ausgewählten SKI für die Evaluation

Norm / Standard	ID	Kurzbeschreibung (Bezeichnung)
IEC 62351-2	6-3-4-3	Supported Cipher Suites (TlsCipherSupported)
IEC 62351-2	7-2	LDAP[1] Konfigurationsanforderungen (LdapKonfInfo)
IEC 62443-4-2	CR-1-1-RE-2	Multi-Faktor-Authentifizung für menschliche Nutzer (mfaHumans)
IEC 62443-4-2	CR-1-9-RE-1	Komponente muss die Fähigkeit besitzen, private Schlüssel mittels Hardware zu schützen (keyProtHsm)
BSI IND-1-2023	A9-02	Deaktivieren nicht benötigter Schnittstellen. Kommunikation aktiver Schnittstellen auf bestimmte Geräte oder Medien beschränken (intfUnused)
BSI IND-1-2023	A21	Dokumentation der Systeme, mit denen Daten ausgetauscht werden (extSystemExchange)

6.3.2 Testfälle der Remote Attestation

Zur Überprüfung der Funktionen der Remote Attestation wurden ebenfalls Testfälle definiert. Die Funktionstests stellen im Rahmen der Evaluation hauptsächlich die Funktionsfähigkeit der Lösung auf echter Hardware dar. Ein vollständiger Test mit dem Ziel, den Nachweis einer korrekten Implementierung (der Quote-Funktion) zu führen, ist in diesem Zusammenhang nicht vorgesehen, da die korrekte Funktionalität der eingesetzten Bibliotheken vorausgesetzt wird. Die für die Tests benötigten Referenzwerte werden auf beiden Geräten mit denen des Measured-Boot-Simulators dargestellt bzw. definiert und dienen als Soll-Werte. Die Funktionsweise und der Prozessablauf wurden bereits im vorherigen Kapitel vorgestellt (siehe 5.3.3). Die Tests wurden durch Anpassungen in den Konfigurationen durchgeführt und sind im Anhang A.3 dokumentiert, sowie in die Test-ID 3-5 aufgeteilt.

Test-ID 3: Korrekte Quote-Verifikation

Dieser Funktionstest stellt sicher, dass ein erwartet korrektes Testergebnis als solches auf der Clientseite korrekt erkannt wird. Das bedeutet in diesem Fall, dass keine Abweichung in den PCRs, den Public Keys sowie dem nonce vorliegt und die Auswertung aufseiten des Clients korrekt abläuft. Daraus resultiert ein korrekter Quote mit den Soll-Werten des Clients. Die genauen Testkonfigurationen sind im Anhang A.3.1 beschrieben.

Test-ID 4: Erkennung nicht verifizierter Quotes

Dieser Funktionstest stellt sicher, dass ein Quote, dessen Signatur nicht dem Soll entspricht, erkannt wird. Um dies zu testen, wurden die hinterlegten Soll—Werte verändert, sodass es keine Übereinstimmung geben darf und eine entsprechende Fehlermeldung angezeigt wird. Bei den veränderten Soll-Werten handelt es sich um manipulierte Zertifikate auf dem Client im Controlcenter. Eine Manipulation des Zertifikats im TPM2 oder der Zertifikate auf dem Server kommt hierfür nicht in Betracht, da sie einen unverhältnismäßigen Aufwand erzeugen würde. Der genaue Testablauf ist im Anhang A.3.2 als Szenario 1 beschrieben.

[1] LDAP = Lightweight Directory Access Protocol, Protokoll zum Zugriff auf Verzeichnisdienste.

Test-ID 5: Erkennung von PCR-Abweichungen

Dieser Funktionstest stellt sicher, dass vom Soll abweichende PCRs vom Client erkannt werden. Ein korrektes Testergebnis ist dann erzielt, wenn der Client die Abweichung erkennt. Um diese Funktion zu testen, ist in der Evaluationsumgebung aufseiten des Clients eine abweichende Konfiguration hinterlegt, welche nicht den tatsächlichen PCR-Konfigurationen der Server in den Substations entspricht. Die daraus resultierende Abweichung wurde vom Client erkannt. Dazu wurden beide Substations abgefragt und die Auswertung hat die Abweichung erfolgreich benannt. Die genaue Testkonfiguration und der Ablauf sind im Anhang A.3.2 hinterlegt und dort im Szenario 2 beschrieben.

Test-ID 6: Erkennung von Firmware-Manipulation

Die Manipulation der Firmware wird in der Trust-Matrix berücksichtigt und zielt darauf ab, bewusste oder unbewusste Veränderungen an Komponenten der Firmware nachzustellen. Durch die Funktion der Remote Attestation soll dies erkannt werden. Da die als IEDs verwendeten Geräte nicht über die Eigenschaften von eingebetteten Systemen verfügen, wird an dieser Stelle der exemplarische Bootvorgang des in Kapitel 5.2.3 entwickelten Measured-Boot-Simulators verwendet. Damit wird es ermöglicht, eine Manipulation am Linuxkernel nachzustellen, welche vom Angreifer genutzt werden kann, um z. B. eine Kernel-Version mit Sicherheitslücken einzuschleusen oder um neue Funktionen im Betriebssystem zu erlangen. Um dies in einem Manipulationsszenario umzusetzen, wurde die main_kernel im Simulator so manipuliert, dass das Wort „manipuliert“ eingefügt wurde. Daraus resultiert beim Messen durch Hashing ein vom Soll abweichender PCR-Wert in Register 7. Der Ablauf und die jeweiligen Testdetails sind im Anhang A.3.3 beschrieben.

Test-ID 7: Manipulation der Sicherheitskonfigurationen

Dass nicht nur die Firmware bzw. der Bootvorgang durch die TPM2-Konzepte abgedeckt werden können, sondern auch die Manipulation der SKI-Datei selbst, wird in diesem Test gezeigt. Da die SKI-Datei ebenfalls kryptografisch gemessen und als Hash in einer PCR erfasst wird, kann diese Abweichung erkannt werden. Als Szenario wurde für diesen Test das Prinzip der Angriffsmethode eines Downgrade-Angriffs gewählt. Bei dieser Attacke versucht der Angreifer, eine unsichere Verbindungsversion oder unsichere Chiffren für die Verbindung aufzuzwingen. Damit

werden bewusst Schwachstellen in den Verbindungsaufbau integriert, die der Angreifer später ausnutzt, um die Kommunikationsverbindung zu kompromittieren. Dazu ist es notwendig, dass unsichere Chiffren akzeptiert werden. Im Rahmen des Testszenarios ist durch eine menschliche Fehlhandlung eine unsichere Konfiguration in die SKI-Dateien auf den IEC-61850-Servern der Substation 1 und 2 eingespielt worden. Die Manipulation betrifft die verfügbaren TLS-Cipher-Suites; Es wurden zwei unsichere hinzugefügt: die TLS_RSA_WITH_NULL_MD5 und die TLS_RSA_WITH_RC4_128_SHA. Die erste deaktiviert gänzlich die Verschlüsselung der TLS-Verbindung, die zweite nutzt RC4, einen veralteten Verschlüsselungsalgorithmus, und gilt daher als sehr unsicher. Der genaue Ablauf sowie die Konfigurationsdetails sind im Anhang A.3.4 beschrieben.

6.3.3 Ergebnisse

Die Ergebnisse aller durchgeführten Funktionstests sind in Tabelle 6.4 dargestellt. Jeder Funktionstest wurde jeweils auf der Substation 1 und auf der Substation 2 ausgeführt.

Tabelle 6.4.: Ergebnisse der Funktionstests als Testmatrix

System	Test-ID	Soll-Ergebnis	Ist-Ergebnis
Substation 1	ID-1	konform	konform
Substation 2	ID-1	konform	konform
Substation 1	ID-2	konform	konform
Substation 2	ID-2	konform	konform
Substation 1	ID-3	konform	konform
Substation 2	ID-3	konform	konform
Substation 1	ID-4	konform	konform
Substation 2	ID-4	konform	konform
Substation 1	ID-5	konform	konform
Substation 2	ID-5	konform	konform
Substation 1	ID-6	konform	konform
Substation 2	ID-6	konform	konform
Substation 1	ID-7	konform	konform
Substation 2	ID-7	konform	konform

6.4 Transformationsfunktion und Trust-Pyramide

Für die weiteren Evaluationsschritte wurde eine sogenannte Trust-Matrix (Vertrauensmatrix) entwickelt, welche im Kontext der Trust-Pyramide als Transformations-

funktion gesehen wird. Die Trust-Matrix erlaubt eine Aussage über die Vertrauenswürdigkeit eines IEDs auf Basis der abgerufenen SKI sowie des Ergebnisses der Remote Attestation. Dazu unterscheidet die Trust-Matrix zwischen vier Vertrauensleveln. Jedes Vertrauenslevel selbst kann für weitere Metriken oder Transformationsfunktionen innerhalb der Trust-Pyramide genutzt werden und gilt für je ein IED. Die Tabelle 6.5 präsentiert diese Trust-Matrix. Die zuvor beschriebenen Funktionstests lassen sich auf die Transformationsfunktionen anwenden und decken damit die Evaluation der Anwendbarkeit des vorliegenden Demonstrators ab. Folgende Auflistung bettet die Anwendungsszenarien ein.

Tabelle 6.5.: Vertrauensbewertungsmatrix (Trust-Matrix) als Transformationsfunktion für die Trust-Pyramide

Vertrauenslevel	Firmware wie erwartet?	Sicherheitskonfiguration wie erwartet?
Kein Vertrauen	Nein	Nein
Geringes Vertrauen	Nein	Ja
Höheres Vertrauen	Ja	Nein
Volles Vertrauen	Ja	Ja

1. **Volles Vertrauen:** Der Client des Controlcenters fragt an beiden Server die PCR-Werte sowie deren SKI ab. Diese geben jeweils die korrekten PCR-Werte und die erwarteten Sicherheitskonfigurationsinformationen zurück. Dieses Szenario stellt den optimalen Fall her, da er sowohl die Integrität der Firmware nachweist als auch die zuvor spezifizierten Sicherheitsanforderungen erfüllt.

2. **Höheres Vertrauen:** Der Client des Controlcenters fragt beide Server ab. Die Server geben jeweils die erwarteten PCR-Werte zurück. Allerdings liegen keine Sicherheitskonfigurationen vor bzw. sie werden vom Server nicht übermittelt.

3. **Geringes Vertrauen:** Der Client des Controlcenters fragt beide Server ab. In diesem Szenario werden keine PCR-Werte zurückgegeben. Die Server senden lediglich SKI zurück. In diesem Szenario wird davon ausgegangen, dass die Geräte über keinen TPM2 verfügen und dies durch die Nichtbereitstellung der entsprechenden IEC-61850-Datenattribute zu erkennen ist.

4. **Kein Vertrauen:** Der Client des Controlcenters fragt beide Server ab. In diesem Szenario stimmen die von den Servern aus den Substationen zurückgegebenen Werte nicht mit den Soll-Werten überein. Dieses Szenario wurde umgesetzt durch die Manipulation der Firmware sowie eine falsche Sicherheitskonfiguration. Abgedeckt wird dieser Fall mit den Funktionstests.

Im nächsten Schritt wurden die Funktionstests auf die einzelnen Vertrauenslevel abgebildet, wie in Tabelle 6.6 dargestellt. Wie aufgezeigt, bilden die einzelnen Funktionstests bereits die Trust-Pyramide ab und weisen somit deren Machbarkeit im Rahmen der vorliegenden Arbeit und des präsentierten Demonstrators nach.

Tabelle 6.6.: Abbildung der Funktionstests auf die Trust-Pyramide

Vertrauenslevel	Abdeckung durch Funktionstest ID
Volles Vertrauen	1, 3
Höheres Vertrauen	3, 4, 5, 6
Geringes Vertrauen	1, 2
Kein Vertrauen	2, 3, 4, 5, 6, 7

Die Tests zeigen erwartungsgemäß die erfolgreichen Funktionsweisen des Demonstrators in der Evaluationsumgebung auf. In der tabellarischen Darstellung der Tests fällt auf, dass ein überwiegender Teil der Tests auf die Nicht-Funktion, daher auf kein Vertrauen, einzahlt, was sich damit begründet, dass eine Vielzahl der Tests eine Abweichung bzw. eine Manipulation erkennen soll. Das heißt, auf diese Kategorien wurde fokussiert getestet. Die Test-ID 7 zeigt mit der Manipulation der SKI gleich die Vor- und Nachteile des Verfahrens auf. Durch eine einzige Veränderung an den SKI werden die Substations auf das Vertrauenslevel „kein Vertrauen“ eingestuft. Dies liegt daran, dass bei diesem Szenario eine Änderung an den SKI auch zu einer Änderung an der Auswertung der Remote Attestation führt. In diesem konkreten Szenario ist die Einstufung in „kein Vertrauen“ gerechtfertigt und sinnvoll. Bei anderen Konfigurationsabweichungen kann dies allerdings nicht treffend sein. Dennoch zeigt dies, dass das Gesamtverfahren stark ist, um manipulierte Geräte zu identifizieren und innerhalb der energienetzspezifischen Kommunikationsprotokolle genutzt zu werden.

6.5 Beurteilung der nichtfunktionalen Anforderungen

Der folgende Abschnitt betrachtet die nichtfunktionalen Anforderungen und bewertet diese im Kontext der entwickelten Artefakte und Resultate.

Berücksichtigung der IT-Sicherheitsstandards der Energiedomäne

IT-Sicherheitsstandards aus der Energiedomäne wurden berücksichtigt. Eine Auswahl wurde bereits in Kapitel 3 getroffen und auch der Sicherheitsstandard IEC 62351 der Referenzarchitektur der TC57 Power System Architecture Model wurde in der

Analyse sowie der Umsetzung berücksichtigt. Im Rahmen der Analyse sowie der weiteren Schritte der vorliegenden Arbeit wurden insbesondere die Teile der Norm betrachtet, die konkrete Anforderungen an die Endgeräte bzw. IEDs stellen. Die identifizierten Anforderungen wurden über das Informationsmodell in Kapitel 4 ebenfalls in der Implementierung des Demonstrators berücksichtigt. Im Rahmen der Evaluation wurden zwei Anforderungen aus der IEC 62351 als Anwendungstestfälle berücksichtigt.

Beobachtungen: Die wesentliche Erkenntnis ist, dass dieser Standard detaillierte technische Vorgaben enthält. Diese Vorgaben können verhältnismäßig gut in technische Konfigurationen übersetzt und als Key-Value-Paare abgefragt werden, da sie bereits technisch formuliert sind.

Berücksichtigung von OT-Sicherheitsstandards

Die Anforderung, Sicherheitsstandards aus bzw. für den Bereich der Operational Technology zu berücksichtigen, wurde erfüllt. Es wurden die Sicherheitsanforderungen der Norm IEC 62443 berücksichtigt. Diese Norm beschreibt die Sicherheit für industrielle Kommunikationsnetze. Aus der Norm wurde der Teil mit einbezogen, der sich an Hersteller von OT-Geräten richtet (IEC 62443-4-2), und es wurden die Sicherheitsanforderungen berücksichtigt, die für den Betreiber der OT-Geräte gelten (IEC 62443-3-3). Diese wurden konsequent berücksichtigt und bereits in der Analyse (siehe Kapitel 3.3.1) sowie dem daraus abgeleiteten Informationsmodell für SKI (siehe Kapitel 4.1) integriert. Eine Implementierung in den Demonstrator wurde mit je zwei Anforderungen umgesetzt und in der Evaluation der Anwendungsfälle aufgegriffen.

Beobachtungen: Die OT-Sicherheitsstandards sind weniger detailliert hinsichtlich technischer Anforderungsbeschreibungen. Stattdessen definieren sie die zu erreichenden Sicherheitsziele, beschreiben allerdings keine konkreten technischen Vorgaben zur Umsetzung. Die vorliegende Arbeit geht über den bisherigen Stand der Technik hinaus und hat einen Vorschlag für ein einheitliches Informationsmodell präsentiert, dessen Integration sowie die Implementierung in die Referenz-Kommunikationsarchitektur der TC57 Power System Architecture Model des Energieversorgungsnetzes umgesetzt, vorgestellt und evaluiert. Dieselbe Beobachtung wurde für den Standard des sogenannten IT-Grundschutzes angestellt, welcher vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird.

Berücksichtigung der Plattformintegrität

Die Berücksichtigung der Plattformintegrität und der damit einhergehende Aspekt der Erhöhung der Sicherheit stellen eine besonders wichtige Anforderung dar. Dies wurde in der Analyse der IT-Sicherheitsstandards bestätigt (siehe Kapitel 3). Die Erfüllung dieser Anforderung erfolgte durch die Integration der Funktionalitäten der Remote Attestation. Diese besagte Anforderung wurde in das Datenmodell der IEC 61850 integriert (siehe Kapitel 4.4) und als solches veröffentlicht [Fra+23]. Die konsequente Berücksichtigung im Gesamtkonzept der vorliegenden Arbeit spiegelt sich ebenfalls in der Trust-Matrix der Evaluation wider und ist gleichzeitig die Voraussetzung zur Erreichung der höchsten Vertrauensstufe. Die Funktionsfähigkeit und Integrierbarkeit konnten im Demonstrator der vorliegenden Arbeit ebenfalls bewiesen werden.

Beobachtung: Die Resultate der IT-Sicherheitsanalyse aus dem Kapitel 3.5 haben die Relevanz der Integrität der Plattform untermauert und dadurch das Thema der Integritätssicherheit bzw. deren Nachweis durch die Remote Attestation in der vorliegenden Arbeit deutlich in den Fokus gerückt. Für die Integration in das IEC 61850 war es von Vorteil, dass seitens der TCG bereits ein Datenmodell für vordefinierte Anwendungsfälle der Remote Attestation zur Verfügung stand.

Berücksichtigte Standards der Energiedomäne

Insgesamt wurden zwei Normen aus der Energiedomäne berücksichtigt: die Norm IEC 61850, die als (zukünftiger) Kernstandard gilt, sowie die zur Referenzarchitektur gehörende Norm IEC 62351, die domänenspezifische Sicherheitsanforderungen beschreibt. Eine Berücksichtigung erfolgte konsequent in jedem Kapitel und insbesondere im Kapitel Analyse der IT-Sicherheitsstandards und -Anforderungen (siehe 3), für die Identifikation und Analyse von IT-Sicherheitsanforderungen. Das Kapitel Informationsmodellelemente für Sicherheitskonfigurationsattribute in Stromnetzen hat die Anforderungen der IEC 62351 in Form von SKI in das Datenmodell der IEC 61850 integriert und damit abgedeckt. Durch diese Integration lässt sich ableiten, dass die SKI ebenfalls innerhalb der Referenzarchitektur des TC57 Power System Architecture Model durch die Nutzung vom Common Information Model (CIM) auch für die Verwendung der Daten oberhalb von Operations (SGAM-Notation), z. B. für Marktakteure, bereitgestellt werden können. Damit können die Sicherheitsinformationen auch außerhalb der typischen IT-Sicherheitssysteme genutzt werden.

Beobachtung: Die Standards erweisen sich als nur begrenzt geeignet für einen flexiblen Datenaustausch, wie er aktuell bzw. für die vorliegende Arbeit und damit in zukünftigen Entwicklungen benötigt wird. Dies ist vermutlich darauf zurückzuführen, dass sie primär für den Austausch von Informationen über physische Messgrößen und andere typische Stromnetzdaten aus dem Bereich der Primärtechnik konzipiert wurden. Die Standards eignen sich zur Steuerung von SCADA-Systemen, allerdings fehlt ihnen die technische Flexibilität, die beispielsweise von Auszeichnungssprachen (englisch markup language) wie JSON, XML oder YAML abgebildet werden kann. Folglich können die Anforderungen, die das intelligente Stromnetz der Zukunft stellt, nur mit einem beträchtlichen Aufwand umgesetzt werden. Immer häufiger werden Anforderungen, die im IoT-Bereich typisch sind, an die IEDs gestellt, welche jedoch nur schwer in die Kommunikationsprotokolle der Referenzarchitektur der TC57 Power System Architecture Model integrierbar sind.

Komplementär zur TC57-Architektur / Seamless Integration Architecture

Die Lösung ist komplementär zur vorgestellten Kommunikationsarchitektur des TC57 Power System Architecture Model (siehe 2.2). Durch konsequente Berücksichtigung, die bereits mit der Auswahl der IT-Sicherheitsstandards im Kapitel der Analyse der IT-Sicherheitsstandards und -Anforderungen begonnen hat, wurde sie ebenfalls in der Auswahl des IEC-61850-Informationsmodells (siehe Kapitel Informationsmodellelemente für Sicherheitskonfigurationsattribute in Stromnetzen) und in der Implementierung in der IEC-61850-Client-Server-Architektur im Demonstrator (siehe Abschnitt Konzeption) herangezogen. Damit sind sowohl die SKI als auch die Remote Attestation kompatibel zur Referenzarchitektur für Kommunikationsprotokolle des TC57 Power System Architecture Model. Darüber hinaus besteht damit die Möglichkeit zur weiteren Integration der Sicherheitsinformationen oder von deren Auswertungsergebnissen für andere Teilnehmer über das sogenannte CIM.

Beobachtung: Während der Implementierungsarbeiten ist zum einen aufgefallen, dass die IEC 61850 lediglich die Server- bzw. IED-Seite spezifiziert. Ein Client ist hingegen nicht definiert und muss davon abgeleitet werden. Ein weiterer Punkt ist der Umgang mit dynamischen und flexiblen Datenobjekten und -attributen, da diese im Vorfeld über die sogenannte SCL-Datei definiert werden müssen.

7 Schlussbetrachtung

In diesem Kapitel erfolgt als Erstes eine zusammenfassende Betrachtung der vorliegenden Arbeit. Der zweite Teil widmet sich den Limitierungen sowie den daraus resultierenden weiterführenden Forschungs- und Entwicklungsperspektiven. Im dritten Teil erfolgt ein abschließendes Fazit.

7.1 Zusammenfassung der Arbeit

Die vorliegende Arbeit hat die Fragestellung nach der Möglichkeit des automatisierten Assessments von IT-Sicherheitskonfigurationen auf IED-Geräten im Stromnetz erörtert. Im Ergebnis wurden die dafür notwendigen passenden und dem Einsatzzweck angemessenen IT-Sicherheitsanforderungen identifiziert und ausführlich analysiert. Diese wurden größtenteils aus internationalen Normen abgeleitet und berücksichtigen gleichzeitig gesetzliche Gegebenheiten deutscher Stromnetzbetreiber.

Im Anschluss wurden die IT-Sicherheitsanforderungen in ein eigenständiges Datenmodell überführt, welches die in den Anforderungen geforderten Sicherheitsaspekte als technische Konfiguration ausdrücken kann. Der Schritt gewährleistet die Interoperabilität und somit eine konsistente Integration in die Umgebung der Kommunikationsstandards. Dadurch kann eine konsistente und effiziente Handhabung für den Anwendungsbereich im Stromnetz erreicht werden.

Ein Aspekt, der bereits in der Motivation skizziert wurde und eine Grundlage für eine sichere und vertrauensvolle Datenübertragung darstellt, ist die Remote Attestation. Deren Integration in das bestehende Datenmodell des IEC 61850 wurde im Detail vorgestellt. Somit wurde ein weiteres Forschungsziel erreicht und darüber hinaus die Absicherung der Plattformintegrität von IEDs vorgestellt und integriert.

Die konzipierten Lösungen für die Integration von Remote Attestation und den SKI wurden in einem Demonstrator umgesetzt und dieser wurde zur Evaluation verwendet. Für die Umsetzung des Demonstrators wurden C-basierte Implementierungen durchgeführt, um die Integrationskonzepte für die SKI und die Remote Attestation

in einer IEC-61850-basierten Client-Server-Lösung zu implementieren. Als Ergebnis wurde ein Proof of Concept realisiert und im Evaluierungsprozess wurden die vorgesehenen Funktionalitäten erfolgreich nachgewiesen.

Die vorliegende Arbeit hat eine bestehende Lücke geschlossen und relevante SKI für die Bewertung des Sicherheitszustandes von IEDs in die Kommunikationsarchitektur des Stromnetzes integriert. Es wurde deutlich, dass die IEC 61850 und ihr Daten- und Informationsmodell stark auf die Übertragung von Stromnetzdaten ausgerichtet sind. Gleichzeitig hat sich die Übertragung von Informationen, wie sie in der vorliegenden Arbeit benötigt wurden, als kompliziert herausgestellt. Trotzdem wurde die Möglichkeit der Integration von SKI und Remote Attestation erfolgreich gezeigt.

7.2 Limitierungen und zukünftige Arbeiten

Der entwickelte Demonstrator und die darauf aufbauende Evaluation dienen der vorliegenden Arbeit zur Erreichung der Forschungsziele und zur damit verbundenen Beantwortung der Forschungsfrage. Daher kann die vorgestellte Lösung nicht direkt in einen produktiven Betrieb überführt bzw. integriert werden, lässt sich aber für weitere Forschungszwecke nutzen. Um den Demonstrator für einen produktiven Einsatz vorzubereiten, über ein Proof of Concept hinausgehen zu können und damit einen höheren Reifegrad zu erreichen, muss eine grundsätzliche Weiterentwicklung erfolgen. Neben typischen Anforderungen in der Softwareentwicklung wie z. B. der Anbindung einer Datenbank müssen die folgenden spezifischen Limitierungen gelöst werden:

- Die für die Entwicklung eingesetzten Bibliotheken müssen für den Produktivbetrieb intensiv getestet und bewertet werden (z. B. Lizenzrechte).

- Das derzeitige Verfahren zur Bestimmung der Plattformintegrität der IEDs beruht darauf, dass die kryptografischen Messungen im Rahmen des Systemstarts des IEDs durchgeführt werden. Regelmäßige Neustarts eines IEDs sind im produktiven Betrieb (vermutlich) nicht vorgesehen und müssen daher eingeplant werden.

- Für die Umsetzung der Remote Attestation wurde im Rahmen der vorliegenden Arbeit ein von der TCG spezifizierter Anwendungsfall des TAP integriert. Weitere Anwendungsfälle des TAP sollten umgesetzt werden.

- Die korrekte Provisionierung eines TPM2s sowie das dazugehörige Lebenszyklusmanagement müssen für den produktiven Einsatz konzeptuell ausgearbeitet und entsprechend umgesetzt werden.
- Die zu integrierende Datenbank, die die Soll-Werte für den Abgleich enthält und auch die jeweils ermittelten Ist-Werte speichert, muss ein hohes Schutzniveau aufweisen, damit die darin gespeicherten Werte nicht manipuliert werden.
- Die exemplarisch umgesetzten SKI dienen der Demonstration und müssen zunächst von den Soft- und Hardwareherstellern umgesetzt, implementiert und bereitgestellt werden.

Jedes Artefakt hat die in Verbindung mit der Forschungsfrage stehenden Ziele erreicht. Aus dem Prozess der Zielerreichung sind zusätzliche Fragestellungen hervorgegangen, welche für zukünftige Weiterentwicklungen von Bedeutung sind:

- Die gegenwärtige Lösung basiert auf einer relativ statischen Vertrauensbewertung. Im Hinblick auf die Integration in die Trust-Pyramide wäre es jedoch erforderlich, weitere Informationen zu integrieren, um eine umfassendere Bewertung zu ermöglichen.
- In dieser Arbeit liegt der Fokus auf der Bereitstellung der Daten als Eingangsinformationen für eine Sicherheitsbewertung bzw. zur kontinuierlichen Überwachung. Eine kontinuierliche Auswertung solcher Informationen bedarf einer Erweiterung durch entsprechende Monitoring-Systeme wie z. B. ELK, Wazuh oder Ähnliches.
- In diesem Kontext ergibt sich auch die Frage nach einem dafür geeigneten SIEM bzw. Monitoringsystem. Dieses muss ganzheitlich integriert werden, da es aktiv einen Quote anfordern und auch verifizieren können muss. Diese Anforderung muss beachtet werden und könnte durch die Entwicklung neuer Module für Open-Source-SIEM-Systeme umgesetzt werden.
- Ein Thema für zukünftige Arbeiten sind die Interpretation, Auswertung sowie die Schlussfolgerungen, die sich aus abweichenden Informationen ergeben, wenn es beispielsweise darum geht, das Vertrauen einzuschätzen, falls sich Parameter der SKI verändert haben. Denn hier ist die Frage: Warum und wodurch hat diese Veränderung stattgefunden? Für eine automatisierte Abschätzung der Situation sollten mit Blick auf die Trust-Pyramide und die damit verwandten Arbeiten weitere Informationen über das Objekt herangezogen werden, um die Auswirkungen auf das Vertrauen in das Gesamtsystem abzuschätzen.

- Das vorgestellte Daten- und Informationsmodell für die SKI sollte weiterentwickelt werden, sodass eine feste Verankerung dieser in den Normen und Standards der IT-Sicherheit ermöglicht werden kann.

7.3 Fazit

Die eingangs beschriebenen Fragestellungen sowie die daraus abgeleitete Forschungsfrage konnten im Rahmen der vorliegenden Arbeit beantwortet werden. Die vorliegende Arbeit hat aufgezeigt, wie ein Sicherheitskonfigurationsmonitoring im Stromnetz der Zukunft grundsätzlich realisiert werden kann.

Gleichzeitig wurde mit der Integration von Remote Attestation gezeigt, wie den SKI selbst vertraut werden kann, indem die jeweiligen IEDs einen Integritätsnachweis erbringen, um Manipulationen am IED auszuschließen bzw. zu erkennen. Somit wird das Sicherheitslevel zusätzlich erhöht.

Die vorgestellten Integritätsfunktionen wie Measured Boot können somit als Baustein für weitere Vertrauensbewertungen genutzt werden, wie die Integration in die Trust-Pyramide (siehe Abschnitt 6.4) gezeigt hat. Somit adressiert die vorliegende Arbeit auch die eingangs vorgestellte Trust-Pyramide, stellt einen praktisch einsetzbaren Baustein für die Facette der IT-Sicherheit dar und treibt damit den Stand der Technik für sichere Stromnetze voran.

Die durchgeführten Untersuchungen und ausführlichen Analysen bestehender IT-Sicherheitsstandards (siehe Kapitel 3) haben gezeigt, dass eine automatisierte Erfassung von Sicherheitsanforderungen sowie deren Übertragung zu weiteren Auswertungen möglich ist. Des Weiteren wurden die notwendigen Voraussetzungen für die Umsetzung identifiziert und als Ergebnis in einem eigens entwickelten Informationsmodell beschrieben. Dieses Ergebnis stellte die Grundlage für eine erfolgreiche Integration in das Informationsmodell des IEC 61850 dar, wodurch es ermöglicht wurde, die Sicherheitsanforderungen in die energienetzspezifischen Kommunikationsprotokolle zu integrieren und somit die Möglichkeit zu schaffen, SKI direkt in das Controlcenter zu übermitteln.

Die detaillierte Analyse und Auswertung der Normen und Standards haben deutlich gezeigt, dass die Menge der als automatisierbar geltenden Sicherheitsanforderungen hoch ist. Diese Erkenntnis bietet die Chance zur Weiterentwicklung der Normen und Standards für IT-Sicherheitsanforderungen, sodass ein dazugehöriges Daten-

und Informationsmodell Teil der Normen und Standards sein sollte, im optimalen Fall durch internationale Standardisierung. Hier bietet es sich an, ein solches Modell bereits in den Normen und Standards einzubetten. Die Vorteile sind offensichtlich, denn dies ermöglicht unter anderem einen schnelleren Vergleich von Sicherheitseinstellungen zwischen Systemen und zum anderen erleichtert es eine maschinelle Verarbeitung deutlich. Daraus kann eine weitere Integration in bestehenden IT-Sicherheitssystemen umgesetzt werden und so können Fälle von Fehlkonfigurationen und Manipulationen schneller erkannt werden. Dies hat darüber hinaus ebenfalls Vorteile für die Hersteller von Softwarekomponenten, da diese unterschiedliche Sicherheitskonfigurationen in Form von Profilen zur Verfügung stellen können. Außerdem erleichtert dies eine Bewertung hinsichtlich der Fragestellung, ob eine Softwarekomponente oder ein System die Soll-Sicherheitseinstellungen umsetzen kann. Im Rahmen der vorliegenden Arbeit wurde dazu ein erster Ansatz erarbeitet, entwickelt und evaluiert, dessen Weiterentwicklung den Anfang für eine bessere Automation von Sicherheitsinformationen in allen Domänen und Bereichen der Kommunikationstechnik darstellt.

Ein weiterer und damit verbundener Aspekt ist, dass die Unschärfe in der Beschreibung der Sicherheitsinformationen in den Standards zwar gewünscht ist, allerdings einer einheitlichen und damit kosteneffizienten, ökonomischen Abbildung von Sicherheitsinformationen im Weg steht. Ein Informations- und Datenmodell kann jedoch dabei unterstützen, diese Unschärfe einzugrenzen oder teilweise sogar zu mildern.

Die vorliegende Arbeit konnte erfolgreich das definierte Umsetzungskonzept in einer praktischen Implementierung demonstrieren und durch die Evaluation dessen Machbarkeit zeigen. Technische Herausforderungen während der Implementierungsphase, die insbesondere das Protokolldesign und Ablaufprozesse des IEC 6180 betrafen, konnten erfolgreich gelöst werden, ohne von der Spezifikation abzuweichen. Hinsichtlich der Integration der SKI und der Remote Attestation in das Datenmodell ist die Norm IEC 61850 zunächst positiv zu bewerten. Die zugrunde liegende Hierarchiestruktur kann grundsätzlich verwendet werden, wenn auch eine Abbildung der Sicherheitskonfigurationen und von Remote Attestation als logisches Gerät (Logical Device) nicht im Sinne des IEC 61850 ist. Dies ist darin begründet, dass diese hierarchische Struktur hauptsächlich den physischen Aufbau der IED-Komponenten abbilden soll. Der Abbildung von anderweitigen Systeminformationen aus dem Feld der Informationssicherheit kann sie damit nicht gerecht werden und dies fällt insbesondere bei der praktischen Umsetzung des Demonstrators ins Gewicht: Die tatsächliche Umsetzung des Datenmodells hat in Bezug auf die Abbildung von

Prozessen den Nachteil, dass kein geeignetes Request-Response-Modell vorhanden ist.

Eine Standardisierung der SKI würde die vorgestellten Konzepte und die damit verbundene Idee der vorliegenden Arbeit stark beschleunigen, da diese nicht auf die Domäne der Stromnetze oder der Energiewirtschaft beschränkt sind.

Anhang

A

A.1 Technische Beschreibungen zum Demonstrator

A.1.1 Client/Server-Aufbau mit Docker

Skript A.1: Beschreibung des Dockercontainers fuer den Demonstrator. Client und Server

```
FROM ubuntu:22.04

WORKDIR /tpm2

RUN apt-get update
RUN apt-get install -y git \
  acl \
  autoconf \
  autoconf-archive \
  automake \
  build-essential \
  cscope \
    cmake \
  curl \
    clang \
  dbus-x11 \
  doxygen \
  g++ \
  gcc \
  gdb \
  lcov \
  libcmocka-dev \
  libcmocka0 \
  libcurl4-gnutls-dev \
  libdbus-1-dev \
  libgcrypt20-dev \
  libglib2.0-dev \
  libjson-c-dev \
  libsqlite3-dev \
  libssl-dev \
  libtool \
  liburiparser-dev \
  libyaml-dev \
```

```
  m4 \
    make \
  net-tools \
    ninja-build \
  openssl \
  pandoc \
  pkg-config \
  python3-pyasn1-modules \
  python3-yaml \
    rsync \
  sqlite3 \
    tar \
  uthash-dev \
  uuid-dev


RUN useradd --system --user-group tss

# Install simulator
ARG ibmtpm_name=ibmtpm1682
ADD "https://downloads.sourceforge.net/project/ibmswtpm2/
    $ibmtpm_name.tar.gz" .
RUN mkdir -p $ibmtpm_name && \
  tar xvf $ibmtpm_name.tar.gz -C $ibmtpm_name && \
  cd $ibmtpm_name/src && \
  make -j$(nproc) && \
  cp tpm_server /usr/local/bin

# install TSS itself
RUN git clone https://github.com/tpm2-software/tpm2-tss.git /tmp/
    tpm2-tss && \
  cd /tmp/tpm2-tss && \
    git checkout tags/3.2.0 && \
  ./bootstrap && \
  ./configure --enable-unit && \
  make -j$(nproc) check && \
  make install && \
  ldconfig

# Install abrmd itself
ENV LD_LIBRARY_PATH /usr/lib
RUN git clone https://github.com/tpm2-software/tpm2-abrmd.git /tmp/
    tpm2-abrmd && \
  cd /tmp/tpm2-abrmd && \
    git checkout tags/2.4.1 && \
  ./bootstrap && \
  ./configure --enable-unit --with-dbuspolicydir=/etc/dbus-1/system
      .d && \
```

```
78    dbus-launch make -j$(nproc) check && \
79    make install && \
80    ldconfig
81
82  # Install tpm2-tools (use 5.1.1 as latest does not work)
83  RUN git clone https://github.com/tpm2-software/tpm2-tools.git
84  /tmp/tpm2-tools && \
85    cd /tmp/tpm2-tools && \
86    git checkout tags/5.1.1 && \
87    ./bootstrap && \
88    ./configure && \
89    make -j$(nproc) check && \
90    make install
91
92  COPY docker-entrypoint.sh /usr/local/bin/docker-entrypoint.sh
93  RUN chmod 755 /usr/local/bin/docker-entrypoint.sh
94
95  # On macOS and Linux, CLion uses the host UID due to file
        permission
96  limitations when writing to volumes from Docker containers.
97  # As a workaround, you can create a parametrized user in the
98  Dockerfile, for example: And then build the image with the
99  new UID:
100 # docker build --build-arg UID=$(id -u) ...
101 #ARG UID=1000
102 #RUN useradd -m -u ${UID} -s /bin/bash builder
103 #USER builder
104
105 # original leonard
106 ENTRYPOINT ["docker-entrypoint.sh"]
```

Definition des Entrypoints

Das in Zeile 92 hinzugefuegte Bash-Script docker-entrypoint.sh ist wie folgt aufgebaut:

Skript A.2: Beschreibung des entry-point scripts fuer den dockercontainer

```
1  #!/bin/bash
2  set -e
3
4  /etc/init.d/dbus start
5  tpm_server &
6  sleep 3
7  tpm2-abrmd --allow-root --tcti=mssim &
8  /bin/bash
```

Measured Boot Emulator

Um innerhalb von Containern in Verbindung mit einem TPM2-Chip oder TPM2-Simulator das Ergebnis des Measured Boot Verfahrens nachstellen zu koennen, wird das folgende Bash-Script eingesetzt. Dieses kann auch auf einem echten Geraet genutzt werden, um Measured Boot nachzustellen. Beim Starten des Scripts werden Hash-werte der im Script hinterlegten Dateien erzeugt und die jeweilige PCR mit dieser erweitert. Damit ist es moeglich, fuer jeden Startvorgang dieselben Hash-Werte in den PCRs zu erhalten und mit diesen das Ergebnis von Measured Boot nachstellen.

Skript A.3: Bash-Script zum messen und erweitern der PCR-Werte

```
1  bios_sha256=$(sha256sum /home/fri/workspace/mqtt-testing/tpm/ boot-
       measure-simulation/biosfile | awk '{print $1}')
2  tpm2_pcrextend 1:sha256=$bios_sha256
3
4  fitfile_sha256=$(sha256sum /home/fri/workspace/mqtt-testing/tpm/
       boot-measure-simulation/fitfile | awk '{print $1}')
5  tpm2_pcrextend 2:sha256=$fitfile_sha256
6
7  uboot_sha256=$(sha256sum /home/fri/workspace/mqtt-testing/tpm/ boot
       -measure-simulation/uboot | awk '{print $1}')
8  tpm2_pcrextend 5:sha256=$uboot_sha256
9
10 main_kernel_sha256=$(sha256sum /home/fri/workspace/mqtt-testing/
       tpm/boot-measure-simulation/main_kernel | awk '{print $1}')
11 tpm2_pcrextend 7:sha256=$main_kernel_sha256
12
13 main_61850_application_sha256=$(sha256sum /home/fri/workspace/ mqtt
       -testing/tpm/boot-measure-simulation/main_61850_application |
       awk '{print $1}')
14 tpm2_pcrextend 9:sha256=$main_61850_application_sha256
15
16 config_61850_application_sha256=$(sha256sum /home/fri/workspace/
       mqtt-testing/tpm/boot-measure-simulation/
       config_61850_application | awk '{print $1}')
17 tpm2_pcrextend 10:sha256=$config_61850_application_sha256
18
19 echo "Changed PCRs are now: "
20 tpm2_pcrread sha256:0
21 tpm2_pcrread sha256:1
22 tpm2_pcrread sha256:2
23 tpm2_pcrread sha256:3
24 tpm2_pcrread sha256:5
25 tpm2_pcrread sha256:7
26 tpm2_pcrread sha256:9
```

```
tpm2_pcrread sha256:10
tpm2_pcrread > /home/fri/workspace/mqtt-testing/tpm/boot-measure-
    simulation/pcrlog.txt
```

Client: Geraetekonfigurationen und deren Sollwerte

Skript A.4: JavaScript Object Notation der Geraetekonfigurationen

```
{
  "device_test_pi": {
    "name": "Pi at Home",
    "type": "Raspberry Pi",
    "ip": "192.168.188.89",
    "port": 102,
    "public_signing_key": "/path/to/keyfile",
    "plattform_configurations_expected": [
      "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4F
         BABB8291E8F0872E062",
      "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECEE
         77E42365E1D5FA9ED6",
      "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B2278
         5D29DB324B23C53C9B4",
      "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C5106
         E8E9B7153EEB36598BB",
      "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5D
         E4E884F7A0E3DF506A3",
      "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D2
         ED8951D16E175E92763"
    ],
    "security_configurations_expected": []
  },
  "device_1": {
    "name": "IED 1",
    "type": "Rpi4_TPM2",
    "ip": "172.17.0.2",
    "port": 102,
    "public_signing_key": "/path/to/keyfile",
    "plattform_configurations_expected": [
```

```
        "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4F
           BABB8291E8F0872E062",
        "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECEE
           77E42365E1D5FA9ED6",
        "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B2278
           5D29DB324B23C53C9B4",
        "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C5106
           E8E9B7153EEB36598BB",
        "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5D
           E4E884F7A0E3DF506A3",
        "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D2
           ED8951D16E175E92763"
    ],
    "security_configurations_expected": [
      {
        "BSI.IND.1:2023": [
          {
            "id": "A9-02",
            "functional requirement": 5,
            "description": "Auf den OT-Komponenten
               SOLLTEN alle nicht benoetigten
               Schnittstellen deaktiviert werden. An
               den aktiven Schnittstellen SOLLTE die
               Nutzung auf bestimmte Geraete oder
               Medien eingeschraenkt werden.",
            "name": "interface status",
            "status": [
              {
                "interface id": "id",
                "type": "usb",
                "interface name": "usb_1",
                "status": "disabled"
              }
            ]
          },
          {
            "id": "A21",
            "functional requirement": 2,
```

```
            "description": "Es SOLLTE dokumentiert
               werden, mit welchen Systemen eine ICS-
               Komponente welche Daten austauscht.
               Ausserdem SOLLTEN die
               Kommunikationsverbindungen neu
               integrierter ICS-Komponenten
               dokumentiert werden.",
            "name": "communication whitelist",
            "allowed connections": [
              {
                "id": "id",
                "connection name": "update-service",
                "address": "ftp://XYZ.de",
                "port": 53,
                "protocol": "TLS"
              }
            ]
          }
        ],
        "IEC.62351.3:": [
          {
            "id": "6.3.4.3",
            "edition": "",
            "functional requirement": 3,
            "description": "Liste unterstuetzer
               chiffren",
            "name": "supported cipher suites",
            "configuration": {
              "operation_mode": "native",
              "available cipher suites": [
                "TLS_RSA_WITH_AES_128_CBC_SHA256",
                "TLS_DH_RSA_WITH_AES_128_GCM_SHA256",
                "TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
                "
                   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
                   "
              ]
            }
          },
```

```
            {
              "id": "7.2",
              "functional requirement": 3,
              "description": "LDAP
                 Konfigurationsanforderungen",
              "name": "LDAP Konfigurationsinformationen",
              "configuration": {
                "LDAP version": 3,
                "ldap unavailability logging":true
                "jwt unavailability logging":true
              }
            }
          ],
          "IEC.62443.4.2": [
            {
              "id": "CR.1.1.RE.2",
              "functional requirement": 1,
              "description": "Die Komponenten muessen die
                  Faehigkeit haben, eine Multi-Faktor-
                 Authentifikation fuer den Zugriff aller
                 menschlichen Nutzer auf die Komponente
                 zu verwenden.",
              "name": "MFA for human user",
              "configuration": {
                "has mfa":true
              }
            },
            {
              "id": "CR.1.9.RE.1",
              "functional requirement": 1,
              "description": "Die Komponenten muessen die
                  Faehigkeit haben, die kritischen,
                 dauerhaften privaten Schluessel mittels
                 Hardware zu schuetzen.",
              "name": "",
              "configuration": {
                "hardware key protection":true
              }
            }
```

```
        ]
      }
    ]
  },
  "device_2": {
    "name": "IED 2",
    "type": "Kunbus RevPi Connect 4",
    "ip": "192.168.188.20",
    "port": 102,
    "public_signing_key": "/path/to/keyfile",
    "plattform_configurations_expected": [
      "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4FBABB8291E8F0872E062",
      "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECEE77E42365E1D5FA9ED6",
      "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B22785D29DB324B23C53C9B4",
      "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C5106E8E9B7153EEB36598BB",
      "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5DE4E884F7A0E3DF506A3",
      "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D2ED8951D16E175E92763"
    ],
    "security_configurations_expected": []
  },
  "device_3": {
    "name": "IED 3",
    "type": "Docker IED",
    "ip": "192.168.188.30",
    "port": 102,
    "public_signing_key": "/path/to/keyfile",
    "plattform_configurations_expected": [
      "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4FBABB8291E8F0872E062",
      "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECEE77E42365E1D5FA9ED6",
      "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B22785D29DB324B23C53C9B4",
```

```
144         "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C5106E
                8E9B7153EEB36598BB",
145         "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5DE
                4E884F7A0E3DF506A3",
146         "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D2E
                D8951D16E175E92763"
147       ],
148       "security_configurations_expected": []
149     },
150     "device_4": {
151       "name": "IED 4",
152       "type": "Docker IED",
153       "ip": "192.168.188.40",
154       "port": 102,
155       "public_signing_key": "/path/to/keyfile",
156       "plattform_configurations_expected": [
157         "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4F
                BABB8291E8F0872E062",
158         "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECE
                E77E42365E1D5FA9ED6",
159         "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B227
                85D29DB324B23C53C9B4",
160         "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C510 6
                E8E9B7153EEB36598BB",
161         "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5
                DE4E884F7A0E3DF506A3",
162         "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D 2
                ED8951D16E175E92763"
163       ],
164       "security_configurations_expected": []
165     },
166     "device_5": {
167       "name": "IED 5",
168       "type": "Docker IED",
169       "ip": "192.168.188.50",
170       "port": 102,
171       "public_signing_key": "/path/to/keyfile",
172       "plattform_configurations_expected": [
```

```
        "0x72AA59B7798C6A6203930673FAC56DEF8E4FCC2628E4F
           BABB8291E8F0872E062",
        "0x8932B65D01BCDB9F82088C9E5171FC4B7141B99D6ECE
           E77E42365E1D5FA9ED6",
        "0x99129AA7857ECC3CFCA15221B30ADA83FE445B51B227
           85D29DB324B23C53C9B4",
        "0x992AEC5EBB61E1AFE7ED0313E63DEF75D994D5E3C510 6
           E8E9B7153EEB36598BB",
        "0xAA9A8F7EE75D1DA343FE7D68762284CF19EB18E327E5
           DE4E884F7A0E3DF506A3",
        "0x8C28A85B9F66EC8C696A06503E5F5DCB54AA7CE9983D 2
           ED8951D16E175E92763"
      ],
      "security_configurations_expected": []
    }
}
```

A.2 Funktionstests zur Evaluation

Die folgend aufgeführten Funktionstests dienen der Evaluation. Die Tests soweit beschrieben, dass Ablauf sowie die Testein- und ausgaben nachvollziehbar sind. Weitere Informationen zu Konfigurationsdateien sowie detaillierteren Testein- und Ausgaben sind im Repository im Ordner ‘docs‘ und den eigenständigen Ordnern mit Konfigurationsdateien speziell für die Evaluationstests hinterlegt.

A.2.1 Server Substation 1 und Substation 2

Skript A.5: Sicherheitskonfigurationsinformationen der IEC 61850-Server in Substation 1 und Substation 2 als json-Objekt

```
{
  "security_configuration_information": [
    {
      "logical-node-name": "BSI_IND_1_2023",
      "logical-node": "GGIO3",
      "data-objects": [
        {
```

```
            "id": "A9_02",
            "functional requirement": 5,
            "description": "Auf den OT-Komponenten
               SOLLTEN alle nicht benoetigten
               Schnittstellen deaktiviert werden. An den
               aktiven Schnittstellen SOLLTE die Nutzung
               auf bestimmte Geraete oder Medien
               eingeschraenkt werden.",
            "name": "interface status",
            "configuration": [
              {
                "interface_id": "id",
                "type": "usb",
                "interface_name": "usb_1",
                "status": "disabled"
              }
            ]
          },
          {
            "id": "A21",
            "functional requirement": 2,
            "description": "Es SOLLTE dokumentiert werden
               , mit welchen Systemen eine ICS-Komponente
                welche Daten austauscht. Ausserdem
               SOLLTEN die Kommunikationsverbindungen neu
                integrierter ICS-Komponenten dokumentiert
                werden.",
            "name": "communication whitelist",
            "configuration": [
              {
                "allowedConnections": [
                  {
                    "id": "id",
                    "name": "update-service",
                    "ipAddress": "ftp://XYZ.de",
                    "ipPort": 53,
                    "protocol": "TLS"
                  }
                ]
```

```
            }
          ]
        }
      ]
    },
    {
      "logical-node-name": "IEC_62351_3",
      "logical-node": "GGIO2",
      "data-objects": [
        {
          "id": "6_3_4_3",
          "edition": "",
          "functional requirement": 3,
          "description": "Liste unterstuetzer chiffren"
            ,
          "name": "supported cipher suites",
          "configuration": {
            "operationMode": "native",
            "available_cipher_suites": [
              "TLS_RSA_WITH_AES_128_CBC_SHA256",
              "TLS_DH_RSA_WITH_AES_128_GCM_SHA256",
              "TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
              "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
            ]
          }
        },
        {
          "id": "7_2",
          "functional requirement": 3,
          "description": "LDAP
             Konfigurationsanforderungen",
          "name": "LDAP Konfigurationsinformationen",
          "configuration": [
            {
              "ldapVersion": "3",
              "ldapUnavailLog":true
              "jwtUnavailLog":true
            }
          ]
```

```
        }
      ]
    },
    {
      "logical-node-name": "IEC_62443_4_2",
      "logical-node": "GGIO4",
      "data-objects": [
        {
          "id": "CR_1_1_RE_2",
          "functional requirement": 1,
          "description": "Die Komponenten muessen die
             Faehigkeit haben, eine Multifaktor-
             Authentifikation fuer den Zugriff aller
             menschlichen Nutzer auf die Komponente zu
             verwenden.",
          "name": "MFA for human user",
          "configuration": [
            {
              "available":true
              "activated":true
            }
          ]
        },
        {
          "id": "CR_1_9_RE_1",
          "functional requirement": 1,
          "description": "Die Komponenten muessen die
             Faehigkeit haben, die kritischen,
             dauerhaften privaten Schluessel mittels
             Hardware zu schuetzen.",
          "name": "",
          "configuration": [
            {
              "available":true
              "activated":true
            }
          ]
        }
      ]
```

```
106         }
107     ]
108 }
```

A.3 Evaluationstests der Remote Attestation

Im Folgenden werden die Konfigurationen für die Positiv- und Negativtests dokumentiert. Außerdem wird die Vorgehensweise der Positiv- und Negativtests der RA kurz dargestellt. Die Tests sind hauptsächlich mit Veränderungen in den Konfigurationen durchgeführt worden.

A.3.1 Konfiguration und Ablauf des Positivtest

Der Positivtest soll ein erwartet korrektes Testergebnis erzielen. Für die Remote Attestation bedeutet dies, dass keine Abweichung in den PCRs vorliegt, den Public-Keys sowie dem nonce vorliegt und die Auswertung auf Seiten des Clients korrekt abläuft. Daraus resultiert ein korrekter Quote mit den Sollwerten des Clients. Für den Positivtest wurden sowohl client- als auch serverseitig korrekte Konfigurationen verwendet. Dies sind: Die Public-Keys der Substation 1 und 2, sowie die Soll-Werte für den Client, die im Quellcode an folgenden Stellen zu finden sind:

- Public-Key: *client_fapi_impl/data/devices/public-keys/substation-1/exportKey*
- Public-Key: *client_fapi_impl/data/devices/public-keys/substation-2/exportKey*
- Client-Config: *client_fapi_impl/data/devices/device_configs-hardware-evaluation.json*

Der Client und die Substations wurden mit den beschriebenen Konfigurationen gestartet. Die Abfrage der SKI wurde zuvor deaktiviert. Der Client fragt gemäß der Reihenfolge in der Client-Config zuerst die Substation 1 ab und wertet diese aus. Anschließend wird automatisch Substation 2 abgefragt und ebenfalls ausgewertet. Das Ergebnis ist wie erwartet korrekt und im Folgenden Skript A.6 als Konsolenausgabe gezeigt.

Skript A.6: Logausgabe des Positivtests

```
1
```

```
/root/workspace/mz_libiec61850/cmake-build-ssh-docker-client/client_fapi_impl/iec61850_tpm_quote_client_fapi /root/workspace/mz_libiec61850/client_fapi_impl/data/devices/security-configurations.json
debug1: permanently_set_uid: 0/0

Initialise TPM2 Feature API
WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
   ifapi_io_check_create_dir() Directory /tmp/fapi_tmpdir.MzDtaP/user/dir does not exist, creating
WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
   ifapi_io_check_create_dir() Directory /tmp/fapi_tmpdir.MzDtaP/system_dir/policy does not exist,
    creating
Init feature API done
Connecting to: device substation-1.
Device type: "Raspberry Pi"
IP: 192.168.188.40:102
Connection to Server 192.168.188.40:102 established

Asking for security information:

Fetching data object from simpleIOGenericIO/GGIO2.6_3_4_3.operationMode
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.operationMode:
Expected value: native, Is value: native, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.6_3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.available_cipher_suites:

  Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
  Is value:        TLS_RSA_WITH_AES_128_CBC_SHA256
  Compliant: true

  Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
```

```
28    Is value:        TLS_DH_RSA_WITH_AES_128_GCM_SHA256
29    Compliant: true
30
31    Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
32    Is value:        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
33    Compliant: true
34
35    Expected value:
         TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
36    Is value:
         TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
37    Compliant: true
38
39  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       ldapVersion
40  Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
41  Expected value: 3, Is value: 3, Compliant:true
42
43  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       ldapUnavailLog
44  Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
45  Expected value:true Is value:true Compliant:true
46
47  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       jwtUnavailLog
48  Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
49  Expected value:true Is value:true Compliant:true
50
51  Set pcrSelect values on server
52  19, 39, 176, 121, 117, 134, 74, 48, 144, 0, 188, 154,
       248, 92, 98, 106, 189, 238, 17, 106,
53  Loaded SRK for substation-1
54
55  Quote Verification was successfull
56
57  !! Quote data has error in PCR values / digest not
       identical!!
58  ERROR:fapi_server:/root/workspace/mz_libiec61850/
       client_fapi_impl/61850_tpm_client.c:251:verifyQuote
```

```
   () BF: Thats the error at the end of function
   verifyQuote..
n


 - - - - - - - - NEXT IED  - - - - - - -


Connecting to: device substation-2.
Device type: "Kunbus RevPi Conect 4"
IP: 192.168.188.25:102
Connection to Server 192.168.188.25:102 established

Asking for security information:

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.operationMode
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   operationMode:
Expected value: native, Is value: native, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   available_cipher_suites:

  Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
  Is value:        TLS_RSA_WITH_AES_128_CBC_SHA256
  Compliant: true

  Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Is value:        TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Is value:        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

```

```
  Expected value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Is value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Compliant: true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapVersion
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
Expected value: 3, Is value: 3, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
Expected value:true Is value:true Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   jwtUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
Expected value:true Is value:true Compliant:true

Set pcrSelect values on server
79, 48, 95, 96, 106, 3, 28, 230, 219, 15, 209, 128, 216
   , 112, 173, 193, 33, 73, 55, 178,
Loaded SRK for substation-2

Quote Verification was successfull

 Quoted Information are correct!
ERROR:fapi_server:/root/workspace/mz_libiec61850/
   client_fapi_impl/61850_tpm_client.c:251:verifyQuote
   () BF: Thats the error at the end of function
   verifyQuote..
```

A.3.2 Konfiguration und Ablauf Negativtests

Mittels Negativtest wird überprüft, ob die RA ein negatives Ergebnis zurückgibt, wenn die Quote-Informationen nicht verifiziert werden können. Dies soll sicherstel-

len, dass Abweichungen vom Soll korrekt erkannt und ein fehlgeschlagener Quote vom Client gemeldet wird. In den folgenden Testszenarien wird darauf geachtet, wie das System reagiert, wenn die von der Substation übermittelten Werte und die vom Client erwarteten Werte nicht übereinstimmen. Dazu zwei Funktionstests, um entsprechende Szenarien zu bedienen.

1. Szenario 1: Abweichende Sollwerte bei den PCR

2. Szenario 2: Das Zertifikat der Substation stimmt nicht mit dem Sollwerten überein

Szenario 1: Abweichende Sollwerte bei den PCR

Die Abweichung der im Quote gesendeten PCRs ist nicht Teil der von der TSS-Bibliothek bereitgestellten Quote-Verifikation und wurde im Rahmen dieser Arbeit eigens in den Client implementiert. Dessen korrekte Funktionalität wurde im Rahmen der Evaluation getestet. Dazu wurde der PCR-Digest in den Sollwerten verändert, sodass eine Abweichung zustande kommen muss. Dazu wurden die Soll-PCRs verändert und ebenfalls der dazugehörige Digest für die geänderten PCRs neu kalkuliert, um das Szenario realistisch zu halten. Dies ist in der Konfiguration ‘client_fapi_impl/data/devices/device_**configs-wrong_pcr.json**‘ hinterlegt. Für den Ablauf wurden beide Server in den Substations 1 und 2 mit der normalen Konfiguration gestartet. Der Client im Controlcenter lädt die beschriebene Konfiguration.

Daraus resultiert folgendes Ergebnis in Script A.7 für Substation 1 und Substation 2:

Skript A.7: Logausgabe der korrekt fehlgeschlagenen PCR verifikation

```
1 Quote Verification was successfull
2
3  !! Quote data has error in PCR values / digest not
      identical!!
```

Das Script zeigt, dass zum einen die Quote-Verifikation korrekt ist, in einer weiteren Zeile wird aber darauf hingewiesen, dass Soll- und Istwerte der PCR abweichen. Der Test zeigt, dass abweichende PCR vom Client erkannt werden.

Szenario 2: Zertifikat der Substation stimmt nicht mit dem Sollwert überein

Um zu überprüfen, ob der Client korrekt auf abweichende Zertifikate reagiert, wurde das Zertifikat der Substations geändert, sodass es nicht mehr mit dem erwarteten Sollwert übereinstimmt. Dies führt dazu, dass der Client bei der Verifizierung des Quotes ein ungültiges Zertifikat erhält, was wiederum zu einem Fehler bei der Validierung führt. Der Test wurde durchgeführt, indem die Zertifikatsinformationen der Substation in den Sollwerten des Clients modifiziert wurden. Die modifizierte Zertifikatskonfiguration ist in der Datei 'client_fapi_impl/data/devices/device_configs-**wrong_cert**.json hinterlegt. Die „wrong-cert" zeigen auf Zertifikate, die speziell für diesen Test verändert wurden, indem ein ABCDEF anstelle der korrekten Zeichen eingesetzt wurde. Diese Zertifikate sind ebenfalls im Git-Repository hinterlegt, um die Nachvollziehbarkeit und Reproduzierbarkeit des Tests zu gewährleisten.

Zur Testausführung wurde der Client des Controlcenters mit der veränderten Konfiguration gestartet. Der Client im Controlcenter lädt die beschriebene, fehlerhafte Konfiguration und versucht, die Quote-Verifizierung mit dem ungültigen Zertifikat durchzuführen. Das erwartete Ergebnis dieses Tests ist, dass die Verifizierung aufgrund des abweichenden Zertifikats fehlschlägt.

Daraus resultiert folgendes Ergebnis in Script A.8 für Substation 1 und 2:

Skript A.8: Logausgabe der korrekt fehlgeschlagenen Signaturverifikation

```
1
2 # Error Message im Controlcenter fuer Substation 1:
3 ERROR:fapi:src/tss2-fapi/fapi_crypto.c:1370:
     ifapi_verify_signature_quote() PEM format could not
     be decoded.
4 ERROR:fapi:src/tss2-fapi/api/Fapi_VerifyQuote.c:293:
     Fapi_VerifyQuote_Finish() Verify signature.
     ErrorCode (0x0006000b)
5 ERROR:fapi:src/tss2-fapi/api/Fapi_VerifyQuote.c:103:
     Fapi_VerifyQuote() ErrorCode (0x0006000b)
     Key_VerifyQuote
6 ERROR:fapi_server:/root/workspace/mz_libiec61850/
     client_fapi_impl/61850_tpm_client.c:208:verifyQuote
     ()
7 Error Fapi_VerifyQuote
8 ErrorCode (0x0006000b)
9
```

```
10 # Error Message im Controlcenter fuer Substation 2:
11 ERROR:fapi:src/tss2-fapi/fapi_crypto.c:1370:
      ifapi_verify_signature_quote() PEM format could not
      be decoded.
12 ERROR:fapi:src/tss2-fapi/api/Fapi_VerifyQuote.c:293:
      Fapi_VerifyQuote_Finish() Verify signature.
      ErrorCode (0x0006000b)
13 ERROR:fapi:src/tss2-fapi/api/Fapi_VerifyQuote.c:103:
      Fapi_VerifyQuote() ErrorCode (0x0006000b)
      Key_VerifyQuote
14 ERROR:fapi_server:/root/workspace/mz_libiec61850/
      client_fapi_impl/61850_tpm_client.c:208:verifyQuote
      ()
15 Error Fapi_VerifyQuote
16 ErrorCode (0x0006000b)
```

A.3.3 Manipulation der Firmware

Um zu zeigen, dass auch Firmwaremanipulationen auf Seiten der Leitstelle erkannt werden können, wurde mit diesem Test gezeigt. Es wurde das Wort manipuliertin die Firmwaredatei des Boot-Simulators eingefügt. Das Vorgehen für diesen Test war wie folgt:

1. Per SSH auf die Server verbinden
2. Mit dem Konsoleneditor vi das Wort manipuliertin die Datei ‘main_kernel‘eingefügt.
3. Neustarten der Server
4. Starten der Serveranwendungen
5. Ausführen des Leitstellen-Clients
6. Ergebnis im Controlcenter Client auswerten

Das Ergebnis wurde vom Client im Controlcenter entdeckt und ist als Logausgabe in Skript **??** gezeigt.

Skript A.9: Logausgabe der Tests Manipulierte Firmware

```
/root/workspace/mz_libiec61850/cmake-build-ssh-docker-
   client/client_fapi_impl/
   iec61850_tpm_quote_client_fapi /root/workspace/
   mz_libiec61850/client_fapi_impl/data/devices/
   security-configurations.json
debug1: permanently_set_uid: 0/0

Initialise TPM2 Feature API
WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
   ifapi_io_check_create_dir() Directory /tmp/
   fapi_tmpdir.m3gZOT/user/dir does not exist, creating
WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
   ifapi_io_check_create_dir() Directory /tmp/
   fapi_tmpdir.m3gZOT/system_dir/policy does not exist,
    creating
Init feature API done
Connecting to: device substation-1.
Device type: "Raspberry Pi"
IP: 192.168.188.40:102
Connection to Server 192.168.188.40:102 established

Asking for security information:

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.operationMode
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   operationMode:
Expected value: native, Is value: native, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   available_cipher_suites:

  Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
  Is value:       TLS_RSA_WITH_AES_128_CBC_SHA256
  Compliant: true

  Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
```

```
  Is value:        TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Is value:        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Is value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Compliant: true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapVersion
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
Expected value: 3, Is value: 3, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
Expected value:true Is value:true Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   jwtUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
Expected value:true Is value:true Compliant:true

Set pcrSelect values on server
187, 22, 215, 132, 10, 123, 162, 169, 38, 131, 30, 194,
    149, 221, 166, 77, 192, 47, 65, 60,
Loaded SRK for substation-1

Quote Verification was successfull

**!! Quote data has error in PCR values / digest not
   identical!!**
ERROR:fapi_server:/root/workspace/mz_libiec61850/
   client_fapi_impl/61850_tpm_client.c:251:verifyQuote
```

```
   () BF: Thats the error at the end of function
   verifyQuote..
n


- - - - - - - - NEXT IED  - - - - - - -


Connecting to: device substation-2.
Device type: "Kunbus RevPi Conect 4"
IP: 192.168.188.25:102
Connection to Server 192.168.188.25:102 established

Asking for security information:

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.operationMode
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   operationMode:
Expected value: native, Is value: native, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   available_cipher_suites:

  Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
  Is value:       TLS_RSA_WITH_AES_128_CBC_SHA256
  Compliant: true

  Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Is value:       TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Is value:       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

```

```
  Expected value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Is value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Compliant: true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapVersion
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
Expected value: 3, Is value: 3, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   ldapUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
Expected value:true Is value:true Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.
   jwtUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
Expected value:true Is value:true Compliant:true

Set pcrSelect values on server
247, 3, 52, 116, 65, 5, 186, 68, 184, 167, 104, 255, 50
   , 241, 27, 174, 92, 162, 4, 4,
Loaded SRK for substation-2

Quote Verification was successfull

**!! Quote data has error in PCR values / digest not
   identical!!**
ERROR:fapi_server:/root/workspace/mz_libiec61850/
   client_fapi_impl/61850_tpm_client.c:251:verifyQuote
   () BF: Thats the error at the end of function
   verifyQuote..
```

A.3.4 Manipulation der Sicherheitskonfigurationen

Um diesen Test durchzuführen, wurden die Sicherheitskonfigurationsdateien bei den Servern in Substation 1 und in Substation 2 manipuliert. Es wurden zwei schwächere Cipher-Suites in die erlaubten Konfigurationen hinzugefügt (siehe Skript A.10). Ablauf wie folgt:

1. Inhalt der Datei 'security-configs-tls-manipulated.json' in die Datei '../server_fapi_impl/security-configs.json'.
2. Hochladen der manipulierten Datei auf die Substation-Server
3. Neustarten der Server
4. Starten der Serveranwendungen
5. Ausführen des Leitstellen-Clients
6. Ergebnis im Controlcenter Client auswerten

Skript A.10: Manipulierte TLS-Konfiguration

```
{
"logical-node-name": "IEC_62351_3",
"logical-node": "GGIO2",
"data-objects": [
{
  "id": "6_3_4_3",
  "edition": "",
  "functional requirement": 3,
  "description": "Liste unterstuetzer chiffren",
  "name": "supported cipher suites",
  "configuration": {
    "operationMode": "native",
    "available_cipher_suites": [
      "TLS_RSA_WITH_AES_128_CBC_SHA128",
      "TLS_ECDHE_RSA_WITH_RC4_128_SHA",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA128",
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_RSA_WITH_NULL_MD5 ",
      "TLS_RSA_WITH_RC4_128_SHA"
    ]}}]
}
```

Die Logausgabe dieses Tests ist in A.11 zu sehen. Darin ist erkennbar, dass der Client im Controlcenter zwei Konfigurationseinträge nicht in den hinterlegten Sollwerten finden kann und diese als non-compliant markiert. Die Auswertung der PCR-Informationen stellt ebenfalls eine Abweichung fest und meldet einen Fehler (error). Korrekt ist, dass die Quote-Verfication erfolgreich ist. Damit wird nachgewiesen, dass die ausgewerteten Informationen von dem jeweiligen Gerät stammen.

Skript A.11: Manipulierte TLS-Konfiguration

```
1
2  /root/workspace/mz_libiec61850/cmake-build-ssh-docker-
       client/client_fapi_impl/
       iec61850_tpm_quote_client_fapi /root/workspace/
       mz_libiec61850/client_fapi_impl/data/devices/
       security-configurations.json
3  debug1: permanently_set_uid: 0/0
4
5  Initialise TPM2 Feature API
6  WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
       ifapi_io_check_create_dir() Directory /tmp/
       fapi_tmpdir.y6cz3a/user/dir does not exist, creating
7  WARNING:fapi:src/tss2-fapi/ifapi_io.c:339:
       ifapi_io_check_create_dir() Directory /tmp/
       fapi_tmpdir.y6cz3a/system_dir/policy does not exist,
        creating
8  Init feature API done
9  Connecting to: device substation-1.
10 Device type: "Raspberry Pi"
11 IP: 192.168.188.40:102
12 Connection to Server 192.168.188.40:102 established
13
14 Asking for security information:
15
16 Fetching data object from simpleIOGenericIO/GGIO2.6
       _3_4_3.operationMode
17 Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
       operationMode:
18 Expected value: native, Is value: native, Compliant:true
19
```

```
Fetching data object from simpleIOGenericIO/GGIO2.6_3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.available_cipher_suites:

  Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
  Is value:       TLS_RSA_WITH_AES_128_CBC_SHA256
  Compliant: true

  Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Is value:       TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Is value:       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  Compliant: true

  Expected value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Is value:
     TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  Compliant: true
Cipher suite is: TLS_RSA_WITH_NULL_MD5 , but could not be found in expected values. Compliant:false
Cipher suite is: TLS_RSA_WITH_RC4_128_SHA, but could not be found in expected values. Compliant:false

Fetching data object from simpleIOGenericIO/GGIO2.7_2.ldapVersion
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
Expected value: 3, Is value: 3, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog
Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
Expected value:true, Is value:true, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog
```

```
Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
Expected value:true Is value:true Compliant:true

Set pcrSelect values on server
190, 91, 17, 160, 74, 61, 95, 123, 213, 138, 213, 170,
   119, 73, 138, 209, 240, 76, 232, 136,
Loaded SRK for substation-1

Quote Verification was successfull

!! Quote data has error in PCR values / digest not
   identical!!
ERROR:fapi_server:/root/workspace/mz_libiec61850/
   client_fapi_impl/61850_tpm_client.c:251:verifyQuote
   () BF: Thats the error at the end of function
   verifyQuote..



- - - - - - - - NEXT IED  - - - - - - - -


Connecting to: device substation-2.
Device type: "Kunbus RevPi Conect 4"
IP: 192.168.188.25:102
Connection to Server 192.168.188.25:102 established

Asking for security information:

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.operationMode
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   operationMode:
Expected value: native, Is value: native, Compliant:true

Fetching data object from simpleIOGenericIO/GGIO2.6
   _3_4_3.available_cipher_suites
Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
   available_cipher_suites:
```

```
80
81    Expected value:    TLS_RSA_WITH_AES_128_CBC_SHA256
82    Is value:        TLS_RSA_WITH_AES_128_CBC_SHA256
83    Compliant: true
84
85    Expected value:    TLS_DH_RSA_WITH_AES_128_GCM_SHA256
86    Is value:        TLS_DH_RSA_WITH_AES_128_GCM_SHA256
87    Compliant: true
88
89    Expected value:    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
90    Is value:        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
91    Compliant: true
92
93    Expected value:
         TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
94    Is value:
         TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
95    Compliant: true
96  Cipher suite is: TLS_RSA_WITH_NULL_MD5 , but could not
       be found in expected values. Compliant:false
97  Cipher suite is: TLS_RSA_WITH_RC4_128_SHA, but could
       not be found in expected values. Compliant:false
98
99  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       ldapVersion
100 Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
101 Expected value: 3, Is value: 3, Compliant:true
102
103 Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       ldapUnavailLog
104 Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
105 Expected value:true Is value:true Compliant:true
106
107 Fetching data object from simpleIOGenericIO/GGIO2.7_2.
       jwtUnavailLog
108 Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
109 Expected value:true Is value:true Compliant:true
110
111 Set pcrSelect values on server
```

```
112 191, 107, 221, 224, 37, 113, 31, 220, 248, 100, 139, 47
    , 24, 211, 53, 99, 149, 86, 72, 176,
113 Loaded SRK for substation-2
114
115 Quote Verification was successfull
116
117 !! Quote data has error in PCR values / digest not
    identical!!
118 ERROR:fapi_server:/root/workspace/mz_libiec61850/
    client_fapi_impl/61850_tpm_client.c:251:verifyQuote
    () BF: Thats the error at the end of function
    verifyQuote..
```

A.4 Testprotokoll: Abfrage der SKI in den Substations über die IEC 61850-Server

Die Testfälle wurden durch entsprechende Konfigurationen der Substation abgebildet. Für jeden Testfall wurde in der jeweiligen Substation eine Konfiguration beim Start als Parameter übergeben. Dabei enthält die Datei security-configs-test-true.json die konformen Konfigurationsparameter und die security-configs-test-false.json die nicht konformen Parameter. Die Konfigurationsdateien sind im Code-Repository hinterlegt.

Tabelle A.1.: Ablaufprotokoll der SKI Abfrage der Substations

System	Konfiguration	Auswertung Korrekt
Substation 1	security-configs-test-**true**.json	Ja
Substation 2	security-configs-test-**true**.json	Ja
Substation 1	security-configs-test-**false**.json	Ja
Substation 2	security-configs-test-**false**.json	Ja

Die Abfrage der SKI im Rahmen des Funktionstests wurde ohne die Remote Attestation Funktionalität durchgeführt (deaktiviert). Der IEC 61850 Client wird von der IDE (via Remote Deployment) im lokalen Docker Container gestartet und erhält als Argument den Pfad zu den hinterlegten Geräten und deren Sollkonfigurationen (siehe Skript A.5). Der Client arbeitet die in den Sollkonfigurationen hinterlegten Unterstationen (1 und 2) nacheinander ab und wertet diese jeweils aus. Das Ergebnis der Auswertung wird durch Log- und Printinformationen in der Konsole protokolliert und im Skript A.12 festgehalten.

Skript A.12: Logausgabe der SKI abfrage durch IEC 61850-Client im Dockercontainer (aus der IDE gestartet)

```
1
2  /root/workspace/mz_libiec61850/cmake-build-ssh-docker-
       client/client_fapi_impl/
       iec61850_tpm_quote_client_fapi /root/workspace/
       mz_libiec61850/client_fapi_impl/devices/security-
       configs-testtruejson
3  debug1: permanently_set_uid: 0/0
4  Connecting to: device Substation_1.
5  Device type: "Raspberry Pi"
6  IP: 192.168.188.40:102
7  Connection to Server 192.168.188.40:102 established
8
9  \textbf{Asking for security informations}
10
11 Fetching data object from simpleIOGenericIO/GGIO2.6
       _3_4_3.operationMode
12 Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
       operationMode: Expected value: native, Is value:
       native, Compliant:true
13
14 Fetching data object from simpleIOGenericIO/GGIO2.6
       _3_4_3.available_cipher_suites
15 Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
       available_cipher_suites:
16   Expected value:   TLS_RSA_WITH_AES_128_CBC_SHA256
17   Is value:       TLS_RSA_WITH_AES_128_CBC_SHA256
18   Compliant: true
19
20   Expected value:   TLS_DH_RSA_WITH_AES_128_GCM_SHA256
21   Is value:       TLS_DH_RSA_WITH_AES_128_GCM_SHA256
22   Compliant: true
23
24   Expected value:   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
25   Is value:       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
26   Compliant: true
27
```

```
28    Expected value:
          TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
29    Is value:
          TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
30    Compliant: true
31  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      ldapVersion
32  Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
      Expected value: 3, Is value: 3, Compliant:true
33
34  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      ldapUnavailLog
35  Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
      Expected value:true Is value:true Compliant:true
36
37  Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      jwtUnavailLog
38  Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
      Expected value:true Is value:true Compliant:true
39
40  Remote Attestation is disabled
41  BF: Thats the error at the end of the main function.
      Something went wrong ;)
42
43  Connecting to: device Substation_2.
44  Device type: "Kunbus RevPi Conect 4"
45  IP: 192.168.188.25:102
46  Connection to Server 192.168.188.25:102 established
47
48  \textbf{Asking for security informations}
49
50  Fetching data object from simpleIOGenericIO/GGIO2.6
      _3_4_3.operationMode
51  Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
      operationMode: Expected value: native, Is value:
      native, Compliant:true
52
53  Fetching data object from simpleIOGenericIO/GGIO2.6
      _3_4_3.available_cipher_suites
```

```
54 Candidate: simpleIOGenericIO/GGIO2.6_3_4_3.
      available_cipher_suites:
55   Expected value:    TLS_RSA_WITH_AES_128_CBC_SHA256
56   Is value:         TLS_RSA_WITH_AES_128_CBC_SHA256
57   \textbf{Compliant: true
58
59   Expected value:    TLS_DH_RSA_WITH_AES_128_GCM_SHA256
60   Is value:         TLS_DH_RSA_WITH_AES_128_GCM_SHA256
61   \textbf{Compliant: true
62
63   Expected value:    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
64   Is value:         TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
65   \textbf{Compliant: true
66
67   Expected value:
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
68   Is value:
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
69   \textbf{Compliant: true
70
71 Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      ldapVersion
72 Candidate: simpleIOGenericIO/GGIO2.7_2.ldapVersion:
      Expected value: 3, Is value: 3, Compliant:true
73
74 Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      ldapUnavailLog
75 Candidate: simpleIOGenericIO/GGIO2.7_2.ldapUnavailLog:
      Expected value:true Is value:true Compliant:true
76
77 Fetching data object from simpleIOGenericIO/GGIO2.7_2.
      jwtUnavailLog
78 Candidate: simpleIOGenericIO/GGIO2.7_2.jwtUnavailLog:
      Expected value:true Is value:true Compliant:true
79
80 Remote Attestation is disabled
81 BF: Thats the error at the end of the main function.
      Something went wrong ;)
```

A.4.1 Server RA-Integration

SCL-DataSet konfiguration fuer die Remote Attestation Attribute

Skript A.13: Serverseitige Datensatzkonfiguration fuer die Remote Attestation Informationen

```
<DataSet name="QuoteDS" desc="TPM Quote Data Set">
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="sigScheme"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="sigSchemeHashAlg"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
        doName="TpmQuote2" daName="magic"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
        doName="TpmQuote2" daName="type"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="qualifiedSigner"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="extraData"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="clock"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="restartCount"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="resetCount"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="safe"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="firmwareVersion"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="firmwareVersionArrSize"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="pcrSelectAlgHash"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
        doName="TpmQuote2" daName="pcrSelect"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="pcrDigest"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="pcrUpdateCounter"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="OR" lnInst="1"
        doName="TpmQuote2" daName="signature"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
        doName="TpmQuote2" daName="pcrSelectArr"/>
    <FCDA ldInst="GenericIO" lnClass="GGIO" fc="DC" lnInst="1"
        doName="TpmQuote2" daName="pcrSelectSize"/>
</DataSet>
```

Skript A.14: Deklaration des Dataobjekts und den Dataattributes in der SCL-Datei.

```
<DOType id="TPM_2_Quote_2" cdc="TQC">
  <DA name="sigScheme" bType="VisString255" fc="OR"/>
  <DA name="sigSchemeHashAlg" bType="VisString255" fc="OR" />
  <DA name="magic" bType="VisString255" fc="DC" />
  <DA name="type" bType="VisString255" fc="OR" />
  <DA name="size" bType="INT16U" fc="OR" />
  <DA name="qualifiedSigner" bType="VisString255" fc="OR" />
  <DA name="extraData" bType="VisString255" fc="OR" />
  <DA name="clock" bType="INT64" fc="OR" />
  <DA name="restartCount" bType="INT64" fc="OR" />
  <DA name="resetCount" bType="INT64" fc="OR" />
  <DA name="safe" bType="BOOLEAN" fc="OR" />
  <SDO name="firmwareVersion" type="firmwareVersionArr" count="32"
     />
  <DA name="firmwareVersionArrSize" bType="INT8U" fc="OR" />
  <DA name="pcrSelectAlgHash" bType="VisString255" fc="OR" />
  <DA name="pcrSelect" bType="VisString255" fc="DC" />
  <DA name="pcrSelectSize" bType="INT8U" fc="DC" />
  <DA name="pcrDigest" bType="VisString255" fc="OR" />
  <DA name="pcrUpdateCounter" bType="VisString255" fc="OR" />
  <DA name="signature" bType="INT8U" fc="OR" />
  <DA name="signatureSize" bType="INT8U" fc="OR" />
  <DA name="log1" bType="VisString255" fc="OR" />
  <DA name="log2" bType="VisString255" fc="OR" />
  <DA name="log3" bType="VisString255" fc="OR" />
  <DA name="log4" bType="VisString255" fc="OR" />
  <SDO name="pcrSelectArr" type="pcrSelectionArr" count="32"/>
</DOType>
```

Skript A.15: Darstellung der wichtigsten Startkonfigurationen des IEC 61850-Servers

```
    /* Init FAPI */
    ret = init_fapi(FAPI_PROFILE, &global_fapi_context);

    /* Set the base path for the MMS file services */
    IedServerConfig_setFileServiceBasePath(config, "/home/fri/
        workspace/mz_libiec61850/cmake-build-pi-tpm-ssh/
        server_fapi_impl/");

    /* Configure WriteAccess for data model's attribute
        pcrSelectSize */
    IedServer_handleWriteAccess(iedServer,
        IEDMODEL_GenericIO_GGIO1_TpmQuote2_pcrSelectSize,
        writeAccessHandlerPcrSelectSize, NULL);

    /* Configure WriteAccess for data model's attribute values
        pcrSelect */
```

```
11      IedServer_handleWriteAccess(iedServer,
            IEDMODEL_GenericIO_GGIO1_TpmQuote2_pcrSelect,
            writeAccessHandlerPcrSelect, NULL);
12
13      /* Configure WriteAccess for data model's attribute nonce/magic
             */
14      IedServer_handleWriteAccess(iedServer,
            IEDMODEL_GenericIO_GGIO1_TpmQuote2_magic,
            writeAccessHandlerNonce, NULL);
```

Glossar

A

ACSI Abstract Communication Service Interface. 21, 75

API Application Programming Interface (dt. Anwendungsschnittstelle). 80, 98

B

BDA Basic Data Attribute. 75, 93, 94, 96

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.. 44

BSI Bundesamt für Sicherheit in der Informationstechnik. 3, 6, 48, 118

C

CENELEC Europäisches Komitee für elektrotechnische Normung, französisch: Comité Européen de Normalisation Électrotechnique. 61

CIM Common Information Model. 32, 64, 65, 68, 119, 120

CPS cyberphysisches System. 31

D

DER Distributed Energy Resource. 21, 62, 66

DHCP Dynamic Host Configuration Protocol. 45

DOS Denial of Service. 57

DSRP Design Science Research Process. 12, 13, 107, 169

E

ENISA Agentur der Europäischen Union für Cybersicherheit. 34–36, 169

EnWG Energiewirtschaftsgesetz. 43

F

FAPI Feature API. 94, 96

FDIA False Data Injection Attack. 3–5

G

GOOSE Generic Object Oriented Substation Events. 40, 53, 65, 86

GPLv3 GNU General Public License version 3. 82

H

HSM Hardware-Sicherheitsmodul. 87

I

IACS Industrial Automation and Control Systems. 37, 39, 46

ICS Industrial Control System. 3

IEC International Electrotechnical Commission. 18, 20, 40, 59, 168

IED Intelligent Electronic Device. 2, 5, 7–10, 12, 14, 21, 27, 40, 45–49, 54, 55, 64, 65, 67–70, 75, 78, 79, 83, 87, 88, 99, 100, 102–104, 107, 109, 110, 114, 116, 118, 120–122, 124, 125, 170

IEEE Institute of Electrical and Electronics Engineers. 15

IETF Internet Engineering Task Force. 29

IKT Informations- und Kommunikationstechnik. 2, 3, 5, 6, 9, 30, 66, 78, 79

IoT Internet of Things. 7, 109

ISMS Managementsystem für Informationssicherheit. 5–7, 35, 41–43, 53

ISO International Standards Organisation. 5, 8, 35, 44, 67

J

JSON JavaScript Object Notation. 58, 61, 93, 94, 96, 97, 99, 100, 102, 111, 175

K

KMU kleine und mittelständische Unternehmen. 41

L

LAN Local Area Network, dt. lokales Netzwerk. 79

M

MIB Management Information Base. 57

MITM Man-in-the-Middle. 4

MMS Manufacturing Messaging Specification. 41, 65, 82, 84, 86, 94

N

NERC North American Electric Reliability Corporation. 36

NIST National Institute of Standards and Technology. 29, 33

nonce Number Used Once. 92, 93, 97, 113

O

OASIS Organization for the Advancement of Structured Information Standards. 30

OSI Open Systems Interconnection. 65, 82

OSS Open Source Software. 80

OT Operational Technology. 6, 29, 30, 42, 65–68, 118

P

PCR Platform Configuration Register. 25–28, 71, 74, 90, 92, 93, 97, 99, 113, 114, 130, 141, 146, 169, 175

PES Power and Energy Society. 15

PV Photovoltaik. 8

R

RA Remote Attestation. 55, 88, 91–93, 96, 103, 104, 141, 145

RoT Root of Trust. 31, 87

RTU Remote Terminal Unit. 19–21, 31, 78, 170

S

SCADA Supervisory, Control, and Data Acquisition. 2, 4, 6, 9, 12, 19, 31, 36, 65–68, 78, 84, 120

SCAP Security Content Automation Protocol. 29

SCL Substation Configuration Description Language. 83, 93, 96, 100, 102, 120

SGAM Smart Grid Architecture Model. 55, 61–65, 76, 77, 119, 170

SIEM Security Information and Event Management. 31

SKI Sicherheitskonfigurationsinformationen. viii, 12–14, 55, 56, 60, 68–70, 76, 77, 85, 88, 98–105, 107, 110–112, 114–126, 141, 158, 159, 161, 163, 170, 173, 175, 176

SNMP Simple Network Management Protocol. 64, 66–68, 99

SPS Speicherprogrammierbare Steuerung. 46

STIX Structured Threat Information Expression. 30

SV Sampled Values. 40

T

TAP Trusted Attestation Protocol. 70–75, 122, 173

TAXII Trusted Automated Exchange of Intelligence Information. 30

TC Technical Committee. 18, 168

TC57 Power System Architecture Model IEC WG 15 TC 57 Power System Architecture Model. 18, 20, 56, 57, 61, 63, 64, 66–68, 76, 77, 79, 109, 117–120

TCG Trusted Computing Group. 23, 24, 27, 28, 31, 68, 70, 80, 81, 83, 119, 122, 168, 173

TISAX Trusted Information Security Assessment Exchange. 8

TLS Transport Layer Security (dt. Transportschichtverschlüsselung). 58, 83, 115

TPM1 Trusted Platform Module v1. 30, 31

TPM2 Trusted Platform Module v.2. 24–28, 70–72, 75, 76, 80, 82, 85, 87, 89–92, 94, 99, 105, 109, 110, 113, 114, 116, 123

TSS TCG Software Stack 2.0. 80, 82, 83, 94, 96, 146

U

UML Unified Modelling Language, dt. einheitliche Modellierungssprache. 61

V

VNB Verteilnetzbetreiber. 36

VPN Virtual Private Network (dt. virtuelles privates Netzwerk). 99

VPP virtuelles Kraftwerk, (engl. virtual power plant). 2

W

WG Working Group. 18, 168

X

XML Extensible Markup Language, dt. erweiterte Auszeichnungssprache. 93

Abbildungsverzeichnis

Tabellenverzeichnis

Skriptverzeichnis

Literaturverzeichnis

[Art15] Will Arthur. *A practical guide to TPM 2.0: Using the new Trusted Platform Module in the new age of security*. The expert's voice in secure computing. New York NY: Apress Open, 1. Jan. 2015. 357 S. ISBN: 978-1-4302-6583-2 (siehe S. 24, 25).

[Bic+18] Ani Bicaku, Christoph Schmittner, Markus Tauber und Jerker Delsing. "Monitoring Industry 4.0 applications for security and safety standard compliance". In: *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, Mai 2018, S. 749–754. ISBN: 978-1-5386-6531-2 (siehe S. 29, 30).

[Bir+17] Pascal Birnstill, Christian Haas, Daniel Hassler und Jurgen Beyerer. "Introducing Remote Attestation and Hardware-based Cryptography to OPC UA". In: *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, Sep. 2017, S. 1–8. ISBN: 978-1-5090-6505-9. DOI: 10.1109/ETFA.2017.8247591 (siehe S. 31, 32).

[Bra+20] Michael Brand, Davood Babazadeh, Carsten Krüger, Björn Siemers und Sebastian Lehnhoff. "Trust assessment of power system states". In: *Energy Informatics* 3 (S1 Okt. 2020), S. 18. ISSN: 2520-8942. DOI: 10.1186/s42162-020-00121-9 (siehe S. 10).

[BEL23] Michael Brand, Dominik Engel und Sebastian Lehnhoff. "Assess: anomaly sensitive state estimation with streaming systems". In: *Energy Informatics* 6 (S1 19. Okt. 2023), S. 19. ISSN: 2520-8942. DOI: 10.1186/s42162-023-00276-1 (siehe S. 11).

[BNL24] Michael Brand, Anand Narayan und Sebastian Lehnhoff. "Applying Trust for Operational States of ICT-Enabled Power Grid Services". In: *ACM Transactions on Autonomous and Adaptive Systems* (3. Apr. 2024), S. 3654672. ISSN: 1556-4665, 1556-4703. DOI: 10.1145/3654672 (siehe S. 10).

[BRT21] Bret Jordan, Rich Piazza und Tret Darley. *Struktured Threat Information Exchange (STIX)*. Version 2.1. 10. Juni 2021 (siehe S. 30).

[Bro+24] Christoph Brosinsky, Matija Naglič, Sebastian Lehnhoff, Rainer Krebs und Dirk Westermann. "A Fortunate Decision That You Can Trust: Digital Twins as Enablers for the Next Generation of Energy Management Systems and Sophisticated Operator Assistance Systems". In: *IEEE Power and Energy Magazine* 22.1 (Jan. 2024), S. 24–34. ISSN: 1540-7977, 1558-4216. DOI: 10.1109/MPE.2023.3330120 (siehe S. 11).

[BS20] Bernd M. Buchholz und Zbigniew A. Styczynski. “Advanced Information and Communication Technology: The Backbone of Smart Grids”. In: *Smart Grids*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, S. 297–366. ISBN: 978-3-662-60930-9 (siehe S. 1, 2, 21).

[Bun23] Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2023*. Lagebericht. Nov. 2023 (siehe S. 3).

[Cle14] Frances Cleveland. *IEC TC57 WG15: Security Standards for the Power System Information Infrastructure*. Version 16. März 2014 (siehe S. 18, 19, 78).

[Cok+11] George Coker, Joshua Guttman, Peter Loscocco u. a. “Principles of remote attestation”. In: *International Journal of Information Security* 10.2 (2011), S. 63–81. ISSN: 16155262 (siehe S. 27).

[Dem+21] Konstantinos Demertzis, Konstantinos Tsiknas, Dimitrios Taketzis u. a. “Communication Network Standards for Smart Grid Infrastructures”. In: *Network* 1.2 (3. Aug. 2021), S. 132–145. ISSN: 2673-8732. DOI: 10.3390/network1020009 (siehe S. 18).

[Deu] Deutschland, Hrsg. *IT-Grundschutz-Kompendium*. ger. Bd. EDition 2023. Unternehmen und Wirtschaft. Köln: Bundesanzeiger-Verl. ISBN: 978-3-8462-0906-6 (siehe S. 41, 42).

[DH08] Jochen Dinger und Hannes Hartenstein. *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung*. Universitätsverlag Karlsruhe, 2008, S. 344. ISBN: 9783866442092 (siehe S. 67).

[Dra17] Incorporated Dragos. *CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations*. Whitepaper version 2.20170613. Dragos.com, 6. Dez. 2017 (siehe S. 4).

[Eck18] Claudia Eckert. *IT-Sicherheit: Konzepte, Verfahren, Protokolle*. 10. Auflage. De Gruyter studium. München: De Gruyter Oldenburg, 2018. 1004 S. ISBN: 978-3-11-055158-7 (siehe S. 5, 23).

[Fab21] Fabian Niehaus. “Entwurf eines SNMP-basierten Sicherheitskonfigurationsmonitorings für Endgeräte der Betriebstechnik”. Masterarbeit. Bremen: Hochschule Bremen, 14. Sep. 2021. 106 S. (siehe S. 46, 67).

[Fal19a] Herbert Falk. *IEC 61850 demystified*. power engineering series. Artech House, 1. Jan. 2019. ISBN: 978-1-63081-661-2 (siehe S. 20, 21).

[Fal19b] Herbert Falk. *IEC 61850 demystified*. Power Engineering Series. Artech House, 2019. ISBN: 9781630816612 (siehe S. 22).

[Fra+19] Andre Luis Franceschett, Paulo R. A. De Souza, Fabio L. Pereira De Barros und Vivian R. De Carvalho. “A Holistic Approach - How to Achieve the State-of-art in Cybersecurity for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard”. In: *2019 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America)*. Gramado, Brazil: IEEE, Sep. 2019, S. 1–5. ISBN: 978-1-5386-9567-8. DOI: 10.1109/ISGT-LA.2019.8895368 (siehe S. 36).

[Fra22] Bastian Fraune. *Automated Monitoring of Operational Technology Security and Compliance for Power Grids*. GI SICHERHEIT 2022. 2022. DOI: 10.18420/sicherheit2022_19 (siehe S. 1, 15).

[Fra+23] Bastian Fraune, Torben Woltjen, Björn Siemers und Richard Sethmann. "Integration of Remote Attestation into IEC 61850". In: *2023 IEEE Belgrade PowerTech*. 2023, S. 1–7. DOI: 10.1109/PowerTech55446.2023.10202741 (siehe S. 1, 15, 55, 71, 72, 119).

[GHS17] Carl-Heinz Genzel, Olav Hoffmann und Richard Sethmann. *Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilungsnetzbetreiber*. Techn. Ber. Hochschule Bremen - FRI, 2017 (siehe S. 35).

[GG14] CEN-CENELEC-ETSI Smart Grid Coordination Group Grid und Group. *SG-CG/M490/K _ SGAM usage and examples SGAM User Manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM) Version 3.0*. 2014 (siehe S. 62).

[Gro16] Trusted Computing Group. *Trusted Platform Module Library: Part 2: Structures*. 2016 (siehe S. 71).

[GD20] Muhammed Zekeriya Gunduz und Resul Das. "Cyber-security on smart grid: Threats and potential solutions". In: *Computer Networks* 169 (März 2020), S. 107094. ISSN: 13891286. DOI: 10.1016/j.comnet.2019.107094 (siehe S. 3).

[Int23] International Electrotechnical Comission (IEC). *IEC 62351: Cybersecurity for IEC 61850 – IEC 61850*. en-US. Dez. 2023 (siehe S. 41).

[Int10] International Engineering Comission. *Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)*. 2010 (siehe S. 21, 22, 92).

[ISO17] ISO Central Secretary. *Information technology - Security techniques - Information security management systems - Requirements*. en. Standard ISO/IEC 27001:2017. Geneva, CH: International Organization for Standardization, 2017 (siehe S. 5).

[ISO15] ISO/IEC. *11889:2015: Information technology - Trusted Platform Module Library: Part 1: Architecture*. Techn. Ber. Edition: 2015 Issue: 11889:2015. Genf, Schweiz: ISO/IEC, 15. Dez. 2015 (siehe S. 24).

[20] *IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC65/756/CDV:2019)*. Version 2019. Okt. 2020 (siehe S. 38).

[Jha+19] Kumarsinh Jhala, Balasubramaniam Natarajan, Anil Pahwa und Hongyu Wu. "Stability of Transactive Energy Market-Based Power Distribution System Under Data Integrity Attack". In: *IEEE Transactions on Industrial Informatics* 15.10 (1. Okt. 2019). Publisher: IEEE Computer Society, S. 5541–5550. ISSN: 1551-3203. DOI: 10.1109/TII.2019.2901768 (siehe S. 4).

[Ker+16] Heinrich Kersten, Gerhard Klett, Jürgen Reuter und Klaus-Werner Schröder. *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Wiesbaden: Springer Fachmedien Wiesbaden, 2016, S. 268. ISBN: 978-3-658-14693-1 (siehe S. 5, 6).

[KL15] Eric D. Knapp und Joel Thomas Langill. "Security Monitoring of Industrial Control Systems". In: *Industrial Network Security*. Elsevier, 2015, S. 351–386. ISBN: 9780124201149. DOI: 10.1016/B978-0-12-420114-9.00012-5 (siehe S. 5).

[Kob16] Pierre Kobes. *Leitfaden Industrial Security: IEC 62443 einfach erklärt*. Berlin: VDE Verlag GmbH, 2016. ISBN: 3800741652 (siehe S. 37, 40).

[KKL23] C. Krüger, J. Kamsamrong und S. Lehnhoff. "Virtualisation and management technologies of smart substations". In: *27th International Conference on Electricity Distribution (CIRED 2023)*. Bd. 2023. 2023, S. 3171–3175. DOI: 10.1049/icp.2023.0888 (siehe S. 89, 99).

[Kun] Kunbus GmbH. *Revolution Pi RevPi Connect 4 - Datenblatt - Technische Daten* (siehe S. 109).

[Kun+10] N. Kuntze, C. Rudolph, M. Cupelli, J. Liu und A. Monti. "Trust infrastructures for future energy networks". In: *IEEE PES General Meeting*. IEEE, Juli 2010, S. 1–7. ISBN: 978-1-4244-6549-1. DOI: 10.1109/PES.2010.5589609 (siehe S. 30).

[Lef+15] Thierry Lefebvre, Eric Lambert, Heiko Englert und Edf. "Advanced standardization in distribution system management and associated information exchange". In: *CIRED 2015*. 23rd International Conference on Electricity Distribution. Lyon, 15. Juni 2015 (siehe S. 20).

[Leh22] Sebastian Lehnhoff. "Vorlesung Smart Grid Management, Carl Ossietzky Universität Oldenburg". Vorlesung. Vorlesung. Universität Oldenburg, 2022 (siehe S. 62).

[Leh+11] Sebastian Lehnhoff, Sebastian Rohjans, Wolfgang Mahnke und Mathias Uslar. "IEC 61850 based OPC UA communication - The future of smart grid automation". In: 2011, S. 759–766 (siehe S. 32).

[Lep18] Olof Leps. "Hybride Testumgebungen in der Informationssicherheit: Effiziente Sicherheitsanalysen für Industrieanlagen". de. In: *Hybride Testumgebungen für Kritische Infrastrukturen*. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, S. 41–68. ISBN: 978-3-658-22613-8. DOI: 10.1007/978-3-658-22614-5_4 (siehe S. 42).

[Lin24] Marcel Linnemann. *Energiewirtschaft für (Quer-)Einsteiger: Einmaleins der Stromwirtschaft*. 2. Auflage. Wiesbaden [Heidelberg]: Springer Vieweg, 2024. 416 S. ISBN: 978-3-658-43555-4 (siehe S. 7).

[MF11] Raydel Montesino und Stefan Fenz. "Information Security Automation: How Far Can We Go?" In: *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, Aug. 2011, S. 280–285. ISBN: 978-1-4577-0979-1. DOI: 10.1109/ARES.2011.48 (siehe S. 33).

[Mon00] A. Monticelli. “Electric power system state estimation”. In: *Proceedings of the IEEE* 88.2 (2000), S. 262–282. DOI: 10.1109/5.824004 (siehe S. 4).

[Nat] National Institute of Standardization and Technology (NIST). *Security Content Automation Protocol - Project Overview* (siehe S. 29).

[Nev+13] N. Neves, N. Kuntze, C. Di Sarno und V. Vianello. *Resilient SIEM framework architecture, services and protocols. Deliverable D5.1.4, FP7-257475 MASSIF European project*. Techn. Ber. 2013, S. 1–153 (siehe S. 31).

[Nor23] Deutsches Institut für Normung. *DIN EN 62351-3 (VDE 0112-351-3) Energiemangementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 3 Sicherheit von Kommunikationsnetzen und Systemen - Profile einschließlich TCP/IP (IEC 62351-3:2014 + A1:2018 + A2:2020)*. Version VDE 0112-351-3. März 2023 (siehe S. 41).

[Nor19a] Deutsches Institut für Normung. *DIN EN 62351-6 Energiemanagementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 6: Sicherheit für IEC 61850 (IEC 57/2033/CDV:2018); Deutsche und Englische Fassung prEN IEC 62351-6:2018, Entwurf*. Version VDE 0112-351-6:2019-05. Mai 2019 (siehe S. 41).

[Nor19b] Deutsches Institut für Normung. *DIN EN 62351-7 (VDE 0112-351-7) Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen - Daten- und Kommunikationssicherheit - Teil 7: Datenobjektmodelle für Netzwerk- und Systemmanagement (NSM) (IEC 62351-7:2017); Deutsche Fassung EN 62351-7:2017*. Version VDE 0112-351-7:2019-09. Sep. 2019 (siehe S. 41, 57).

[Nor21a] Deutsches Institut für Normung. *DIN EN IEC 62351-4 VDE 0112-351-4:2021-11 Energiemangementsysteme und zugehöriger Datenaustausch - IT-Sicherheit für Daten und Kommunikation - Teil 4: Profile einschließlich MMS und Ableitungen (IEC 62351-4:2018 + A1:2020)*. Version VDE 0112-351-4. Nov. 2021 (siehe S. 41).

[Nor21b] Deutsches Institut für Normung. *DIN EN IEC 62351-8 (VDE 0112-351-8:2021-07) Energiemanagementsysteme und zugehöriger Datenaustausch – IT-Sicherheit für Daten und Kommunikation Teil 8: Rollenbasierte Zugriffskontrolle für Energiemanagementsysteme (IEC 62351-8:2020); Deutsche Fassung EN IEC 62351-8:2020*. Version VDE 0112-351-8:2021-07. Juli 2021 (siehe S. 41).

[Nor] DIN Deutsches Institut für Normung. *DIN EN 50160:2020-11, Merkmale Der Spannung in Öffentlichen Elektrizitätsversorgungsnetzen; Deutsche Fassung EN_50160:2010_+ Cor.:2010_+ A1:2015_+ A2:2019_+ A3:2019*. DOI: 10.31030/3187943 (siehe S. 1).

[OAS21] OASIS OPEN. *Trusted Automated Exchange of Intelligence Information (TAXII)*. 10. Juni 2021 (siehe S. 30).

[Oes18] Oestereichs E-Wirtschaft und BDEW - Bundesverband der Energie- und Wasserwirtschaft, Hrsg. *Whitepaper: Anforderungen an sichere Steuerungs - und Telekommunikationssysteme, Version 2.0*. Deutsch. Mai 2018 (siehe S. 44).

[Pef+20] Ken Peffers, Tuure Tuunanen, Charles E Gengler u. a. “Design Science Research Process: A Model for Producing and Presenting Information Systems Research”. In: (Juni 2020). arXiv: 2006.02763 (siehe S. 13).

[Poh22] Norbert Pohlmann. *Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. 2. Auflage. Wiesbaden [Heidelberg]: Springer Vieweg, 2022. 746 S. ISBN: 978-3-658-36242-3. DOI: 10.1007/978-3-658-36243-0 (siehe S. 5).

[18] *Power system management and associated information exchange*. Business plan. Num Pages: 4. 11. Sep. 2018 (siehe S. 20).

[Rei+16] Andre Rein, Roland Rieke, Michael Jäger, Nicolai Kuntze und Luigi Coppolino. “Trust Establishment in Cooperating Cyber-Physical Systems”. In: *Security of Industrial Control Systems and Cyber Physical Systems*. Hrsg. von Adrien Bécue, Nora Cuppens-Boulahia, Frédéric Cuppens, Sokratis Katsikas und Costas Lambrinoudakis. ISSN: 16113349. Cham: Springer International Publishing, 2016, S. 31–47. ISBN: 978-3-319-40385-4. DOI: 10.1007/978-3-319-40385-4_3 (siehe S. 31).

[Rin+23] J. Rintala, M. Loukkalahti, S. Musunuri, J. Haapaniemi und C. Hampel. “Is the cybersecurity standard IEC 62443 applicable to distribution substations?” en. In: *27th International Conference on Electricity Distribution (CIRED 2023)*. Rome, Italy: Institution of Engineering und Technology, 2023, S. 1554–1558. ISBN: 978-1-83953-855-1. DOI: 10.1049/icp.2023.0931 (siehe S. 36).

[Roh+10] Sebastian Rohjans, Mathias Uslar, Robert Bleiker u. a. “Survey of Smart Grid Standardization Studies and Recommendations”. In: *2010 First IEEE International Conference on Smart Grid Communications*. Num Pages: 6. IEEE, 2010, S. 583–588. ISBN: 978-1-4244-6510-1. DOI: 10.1109/SMARTGRID.2010.5621999 (siehe S. 20, 21).

[RU13] Christine Rosinger und Mathias Uslar. “Smart Grid Security: IEC 62351 and Other Relevant Standards”. In: *Power Systems*. Bd. 71. Series Title: Power Systems ISSN: 16121287. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, S. 129–146. ISBN: 978-3-642-34915-7. DOI: 10.1007/978-3-642-34916-4_8 (siehe S. 35, 36).

[RUS14] Christine Rosinger, Mathias Uslar und Jürgen Sauer. “Using Information Security as a Facet of Trustworthiness for Self-Organizing Agents in Energy Coalition Formation Processes”. In: *Proceedings of the 28th Conference on Environmental Informatics - Informatics for Environmental Protection, Sustainable Development and Risk Management* (2014) (siehe S. 2, 7).

[Sai+18] Qais Saif Qassim, Norziana Jamil, Maslina Daud u. a. “Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system”. In: *International Journal of Engineering & Technology* 7.2 (2018), S. 153. DOI: 10.14419/ijet.v7i2.14.12816 (siehe S. 3).

[SRA13] Ustun Taha Selim, Ozansoy Cagil R. und Zayegh Aladin. “Implementing Vehicle-to-Grid (V2G) Technology With IEC 61850-7-420”. In: *IEEE Transactions on Smart Grid* 4.2 (1. Jan. 2013), S. 1180–1187. ISSN: 1949-3053. DOI: 10.1109/TSG.2012.2227515 (siehe S. 21).

[She+21] Tohid Shekari, Celine Irvene, Alvaro A. Cardenas und Raheem Beyah. “MaMIoT: Manipulation of Energy Market Leveraging High Wattage IoT Botnets”. In: *Proceedings of the ACM Conference on Computer and Communications Security* (2021). ISBN: 9781450384544, S. 1338–1356. ISSN: 15437221. DOI: 10.1145/3460120.3484581 (siehe S. 3).

[Sic18] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz-Kompendium*. Unter Mitarb. von Bundesanzeiger Verlag GmbH und Deutschland. Unternehmen und Wirtschaft. Köln: Reguvis Bundesanzeiger Verlag; Bundesanzeiger Verlag, 1. Jan. 2018. ISBN: 978-3-8462-0906-6 (siehe S. 3, 6).

[Ste+10] Jan-Philipp Steghöfer, Rolf Kiefhaber, Karin Leichtenstern u. a. “Trustworthy Organic Computing Systems: Challenges and Perspectives”. In: *Autonomic and Trusted Computing*. Hrsg. von Bing Xie, Juergen Branke, S. Masoud Sadjadi, Daqing Zhang und Xingshe Zhou. Bd. 6407. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 62–76. ISBN: 978-3-642-16575-7. DOI: 10.1007/978-3-642-16576-4_5 (siehe S. 10).

[Tan+19] Heng Chuan Tan, Carmen Cheh, Binbin Chen und Daisuke Mashima. “Tabulating Cybersecurity Solutions for Substations: Towards Pragmatic Design and Planning”. In: *2019 IEEE Innovative Smart Grid Technologies – Asia (ISGT Asia)*. IEEE, 2019, S. 1018–1023. ISBN: 978-1-7281-3520-5. DOI: 10.1109/ISGT-Asia.2019.8881706 (siehe S. 31).

[Tec23] Technischer Überwachungsverein e.V. (TÜV). *TISAX® Assessment für die Automobilindustrie | TÜV NORD*. Nov. 2023 (siehe S. 8).

[Tru20a] Trusted Computing Group. *TCG Feature API (FAPI) Specification*. Version 0.94. 11. Juni 2020 (siehe S. 81).

[Tru19a] Trusted Computing Group. *TCG TSS 2.0 Overview and Common Structures Specification*. Version 0.9. 2. Okt. 2019 (siehe S. 80, 81).

[Tru24a] Trusted Computing Group. *Trusted Platform Module Library Part 1: Architecture*. Version Revision 1.83. 25. Jan. 2024 (siehe S. 25).

[Tru17] Trusted Computing Group (TCG). *TCG Glossary*. Version 1.1. 11. Mai 2017 (siehe S. 24).

[Tru19b] Trusted Computing Group (TCG). *TCG Trusted Attestation Protocol (TAP) Use Cases for TPM Families 1.2 and 2.0 and DICE*. 2019 (siehe S. 27).

[Tru20b] Trusted Computing Group (TCG). *TCG TSS 2.0 Enhanced System API (ESAPI) Specification*. Version 1.00. 28. Mai 2020 (siehe S. 81).

[Tru20c] Trusted Computing Group (TCG). *TCG TSS 2.0 JSON Data Types and Policy Language Specification*. Version 0.7. 2020 (siehe S. 81).

[Trub] Trusted Computing Group (TCG). *TCG TSS 2.0 Marshaling/Unmarshaling API Specification* (siehe S. 81).

[Tru19c] Trusted Computing Group (TCG). *TCG TSS 2.0 System Level API (SAPI) Specification*. Version 1.1. 6. Aug. 2019 (siehe S. 81).

[Tru24b] Trusted Computing Group (TCG). *TCG TSS 2.0 TPM Command Transmission Interface (TCTI) API Specification*. Version 1.0. 24. Jan. 2024 (siehe S. 81).

[Tru19d] Trusted Computing Group TCG. *TCG Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0*. 2019 (siehe S. 27, 71, 73, 75).

[US19] Ustun Taha Selim und Suhail Hussain S. M. "Extending IEC 61850 Communication Standard to Achieve Internet-of-Things in Smartgrids". In: *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*. 2019, S. 1–6. DOI: 10.1109/ICPECA47973.2019.8975510 (siehe S. 66).

[WF18] David Waltermire und Jessica Fitzgerald-McKay. *Transitioning to the Security Content Automation Protocol (SCAP) Version 2*. Techn. Ber. Gaithersburg, MD: National Institute of Standards und Technology, Sep. 2018. DOI: 10.6028/NIST.CSWP.09102018 (siehe S. 29).

[Wan+14] Yong Wang, Zhaoyan Xu, Jialong Zhang u. a. "SRID: State Relation Based Intrusion Detection for False Data Injection Attacks in SCADA". In: *Computer Security - ESORICS 2014*. Hrsg. von Mirosław Kutyłowski und Jaideep Vaidya. Lecture Notes in Computer Science. Num Pages: 18. Cham: Springer International Publishing, 1. Jan. 2014, S. 401–418. ISBN: 978-3-319-11211-4. DOI: 10.1007/978-3-319-11212-1_23 (siehe S. 4).

[Wan+18] Zhisheng Wang, Ying Chen, Feng Liu, Yue Xia und Xuemin Zhang. "Power System Security Under False Data Injection Attacks With Exploitation and Exploration Based on Reinforcement Learning". In: *IEEE Access* 6 (1. Jan. 2018). Num Pages: 12, S. 48785–48796. DOI: 10.1109/ACCESS.2018.2856520 (siehe S. 4).

[WFN22] Thomas Wolgast, Stephan Ferenz und Astrid Niebe. "Reactive Power Markets: A Review". In: *IEEE Access* 10 (2022), S. 28397–28410. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3141235 (siehe S. 7).

[XMS11] Le Xie, Yilin Mo und Bruno Sinopoli. "Integrity Data Attacks in Power Market Operations". In: *IEEE Transactions on Smart Grid* 2.4 (Dez. 2011). Publisher: IEEE, S. 659–666. ISSN: 1949-3053. DOI: 10.1109/TSG.2011.2161892 (siehe S. 4).

Webseiten

[@Bun13] Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV). *Europäische Energie- und Klimaziele*. Umweltbundesamt. Publisher: Umweltbundesamt. 16. Juli 2013. URL: https://www.umweltbundesamt.de/daten/klima/europaeische-energie-klimaziele (besucht am 16. Aug. 2024) (siehe S. 1).

[@Fou] OPC Foundation. *IEC 61850 - Electrical Substation Automation*. OPC Foundation. URL: https://opcfoundation.org/developer-tools/documents/view/295 (besucht am 2. Juli 2024) (siehe S. 32).

[@Lin] Linux TPM2 & TSS2 Software Developer Community. *GitHub - tpm2-software/tpm2-tss: OSS implementation of the TCG TPM2 Software Stack (TSS2)*. URL: https://github.com/tpm2-software/tpm2-tss (besucht am 24. Apr. 2024) (siehe S. 80).

[@Mic] Microsoft. *Windows 11-Spezifikationen und -Systemanforderungen | Microsoft*. Windows. URL: https://www.microsoft.com/de-de/windows/windows-11-specifications (besucht am 21. Aug. 2024) (siehe S. 24).

[@MZ] MZ Automation GmbH. *Documentation | libIEC61850 / Server-Client API*. Documentation / API Overview. URL: https://libiec61850.com/documentation/ (besucht am 26. Apr. 2024) (siehe S. 86, 87).

[@MZ 23] MZ Automation GmbH. *IEC61850 Protocol Library - MZ Automation*. 3. Nov. 2023. URL: https://www.mz-automation.de/iec61850-protocol-library/ (besucht am 24. Apr. 2024) (siehe S. 82).

[@Sic24] Bundesamt für Sicherheit in der Informationstechnik (BSI). *IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit*. Bundesamt für Sicherheit in der Informationstechnik. 2024. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/itgrundschutzKompendium.html?nn=128568 (besucht am 14. Jan. 2024) (siehe S. 42).

[@Ste] Stefan Feuerhahn. *IEC61850bean/OpenIEC61850: The IEC 61850 Java Stack | beanit*. URL: https://www.beanit.com/iec-61850/ (besucht am 24. Apr. 2024) (siehe S. 82).

[@Trua] Trusted Computing Group. *Welcome To Trusted Computing Group*. Trusted Computing Group. URL: http://trustedcomputinggroup.org/ (besucht am 20. Aug. 2024) (siehe S. 23).

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Außerdem versichere ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis an der Carl von Ossietzky Universität Oldenburg und den DFG-Richtlinien festgelegt sind, befolgt habe.

Datum der Disputation: 16. März 2026

Bastian Fraune