Fraunhofer SIT

Whitepaper

Risiken für Ladeinfrastrukturen im Heimbereich

Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

Risiken für Ladeinfrastrukturen im Heimbereich

Whitepaper

Daniel Zelle, M. Sc.

Dr. Dirk Scheuermann

Jonathan Stancke, M. Sc.

Fraunhofer Institut für Sichere Informationstechnologie SIT

Förderkennzeichen: 01MV21UN12

Darmstadt, 2024

IN ZUSAMMENARBEIT MIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

1
Einführung

Die rasante Entwicklung der Elektromobilität und die damit einhergehende Verbreitung von Ladeinfrastruktur stellen eine bedeutende Herausforderung für die IT-Sicherheit dar. Moderne Ladeinfrastrukturen sind zunehmend vernetzt und bieten neben der reinen Ladefunktionalität auch vielfältige steuerbare Lasten und bidirektionale Kommunikationsmöglichkeiten. Dies ermöglicht nicht nur eine effiziente Nutzung der Energieressourcen, sondern birgt auch erhebliche Sicherheitsrisiken, die sorgfältig adressiert werden müssen.

Dieses Whitepaper hat zum Ziel, die spezifischen Herausforderungen und Risiken im Bereich der IT-Sicherheit von Ladeinfrastrukturen mit steuerbaren Lasten zu beleuchten. Es bietet einen umfassenden Überblick über die aktuellen Bedrohungsszenarien, dabei werden sowohl technische als auch organisatorische Maßnahmen betrachtet.

Zunächst erläutert das Dokument die im Teilprojekt Harmon-E entwickelte Architektur für das gesteuerte Laden von Fahrzeugen. Dabei werden auch die Kommunikationstechnologien beschrieben, die bei der Steuerung eines Ladevorgangs verwendet werden. Zur Bewertung der Sicherheit werden im Anschluss unsere Bewertungskriterien vorgestellt. Anschließend analysieren wir mögliche Angriffe und bewerten die potentiell daraus verursachten Schäden. Abschließend stellen wir eine Übersicht über die finalen Risikobewertungen vor, bei denen ausgewählte Angriffe, ihre Schadenshöhe und das protokollspezifische Sicherheitsniveau berücksichtigt werden.Dabei ist das höchste Risiko durch das Zusammentreffen des geringsten Sicherheitsniveaus mit der höchsten Schadensstufe gegeben.

2
Aufbau der Systemarchitektur

Das Teilvorhaben Harmon-E umfasst zwei wesentliche unterschiedliche Bereiche - die Umgebung eines Eigenheimes und die Umgebung eines Mehrfamilienhauses oder Arbeitsplatzes. In beiden Umgebungen geht es um die Einbindung von angeschlossenen Elektrofahrzeugen sowie um die Interaktionen mit dem Energielieferanten und dem Netzbetreiber.

Hierzu wurde eine Architektur entwickelt, welche in Abb. 2.1 dargestellt ist. Zur genaueren Erläuterung der Komponenten und Schnittstellen sei hier auf die interaktive Darstellung auf der Webseite des unIT-e^2-Projektes verwiesen (`https://sysarc.ffe.de/`). Die hier beschriebenen Untersuchungen konzentrieren sich auf den Bereich des Eigenheimes und der zugehörigen Kommunikation mit dem dort befindlichen Elektrofahrzeug (EV) und den übrigen beteiligten Instanzen. Der Bereich von Mehrfamilienhäusern und Arbeitsplätzen liegt außerhalb der betrachteten Bereiche.

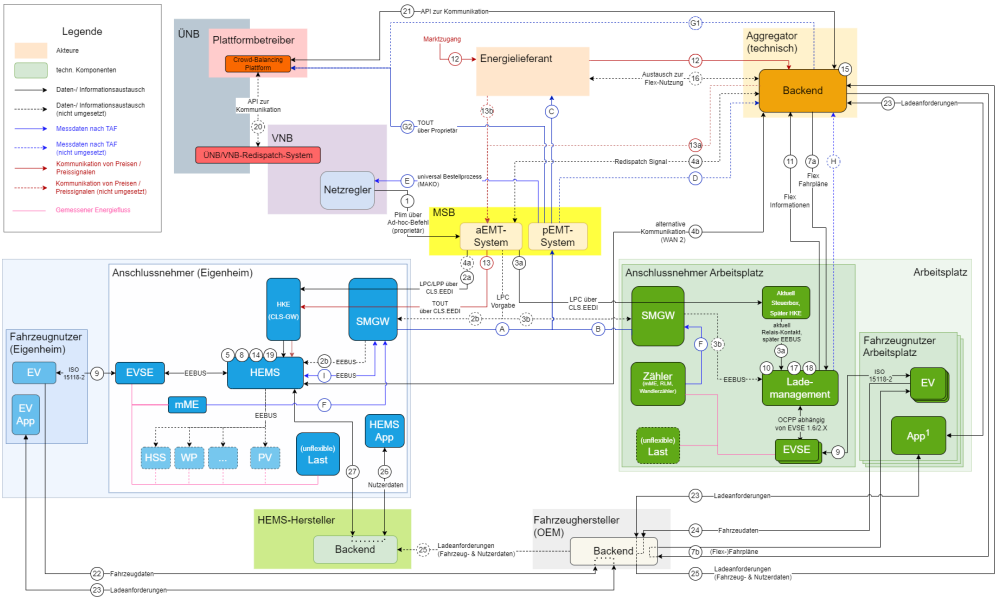

Abb. 2.1
Entwickelte Systemarchitektur für das Teilprojekt Harmon-E

2.1
Komponenten

Im Folgenden werden die verschiedenen Komponenten und Entitäten der Architektur in ihrer Funktion erörtert.

2.1.1
SMGW

Das Smart-Meter-Gateway (SMGW) ist die zentrale Kommunikationseinheit eines intelligenten Messsystems in Deutschland. Es wurde nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gemäß TR 3109-1 entwickelt. Die Hauptaufgabe des SMGW ist die sichere Datenübertragung im intelligenten Messsystem.

Das SMGW befindet sich in der Umgebung des Eigenheims und verfügt über drei definierte Schnittstellen:

Lokales metrologisches Netzwerk (LMN):
Die LMN-Schnittstelle kann nach der Technischen Richtlinie sowohl als Nahbereichs-Funkschnittstelle (wireless Mbus) oder als serielle Schnittstelle ausgeführt sein. Über die LMN-Schnittstelle kommuniziert das SMGW mit den angebundenen Zählern (Strom, Gas, Wasser, Wärme) eines oder mehrerer Netzverbraucher. Die Zähler kommunizieren ihre Messwerte über das LMN an das SMGW.

Weitverkehrsnetz (WAN):
Die WAN-Schnittstelle ist als IP-Schnittstelle ausgeführt. Aus Gründen der Sicherheit gehen sämtliche Kommunikationsverbindungen vom SMGW aus. Diese können bei Bedarf oder zu festgelegten Zeitpunkten durch das Gateway etabliert werden.

Home Area Network (HAN):
Das HAN ist eine Schnittstelle innerhalb des Hauses. Es hat die Aufgabe, die Geräte innerhalb des Hauses mit dem SMGW zu verbinden.

2.1.2 HAN Kommunikationsadaptereinheit (HKE)

Die HKE ist eine weitere zentrale Einheit für die Außenkommunikation des Heimnetzwerkes. Hier werden u.a. Preisinformationen sowie Steuersignale vom aEMT (s.u.) empfangen.

2.1.3 HEMS

Das Home Energy Management System (HEMS) ist ein zentraler Baustein im Haushalt zur Koordination des Zusammenspiels zwischen Stromverbrauchern und -erzeugern. Es steuert u.a. die Informationsflüsse zwischen dem SMGW und den übrigen Architektur-Elementen im Haushalt. Für das SMGW stellt die HAN-Schnittstelle die Verbindung zum HEMS gemäß der BSI-Richtlinie dar.

2.1.4 Ladestation (inkl. EVSE)

Die Ladestation wird mit dem Elektrofahrzeug (EV) verbunden und enthält als Kommunikationscontroller einen sogenannten Supply Equipment Communication Controller (SECC) sowie das Electric Vehicle Supply Equipment (EVSE), über das die physische Verbindung zum Fahrzeug hergestellt wird. Darüber hinaus verfügt die Ladestation über weitere Schnittstellen, um z.B. über EEBUS mit dem HEMS zu kommunizieren.

2.1.5 Fahrzeugnutzer

Der Fahrzeugnutzer besitzt zwei für die Harmon-E-Architektur relevante technische Komponenten. Das EV selbst besitzt die Ladeschnittstelle zum EVSE und eine weitere Schnittstelle zum Fahrzeughersteller zwecks Übermittlung von Fahrzeugdaten; letztere sind jedoch nur für die Arbeitsplatz- bzw. Mehrfamilienhaus-Umgebung relevant. Darüber hinaus besitzt der Fahrzeugnutzer noch eine EV App, um Ladeanforderungen an den Fahrzeughersteller, und dann bei Bedarf weiter an das HEMS-Backend zu übermitteln. Die Verbindung zwischen OEM Backend und HEMS Backend wurde allerdings in Harmon-E nicht umgesetzt.

2.1.6
Weitere Komponenten im Haushalt

Neben der Ladestation gibt es noch eine Reihe weiterer Komponenten im Haushalt, welche über das HEMS angesteuert werden. Hierzu gehören z.B. das Hausspeicher-System (HSS), die Wärmepumpe (WP) sowie Photovoltaik-Anlagen (PVs). Diese wurden jedoch in der Harmon-E-Architektur nicht praktisch umgesetzt.

2.1.7
mME

Die sogenannte moderne Messeinrichtung (mME) dient im Heimbereich als Zähler. Diese Komponente kommuniziert entsprechend den Vorgaben des BSI mit dem SMGW, d.h. die Verbindung zum SMGW stellt die LMN-Schnittstelle dar.

2.1.8
MSB

Der Messstellenbetreiber (MSB) stellt die direkt über das SMGW mit dem Heimnetzwerk kommunizierende Instanz dar. Entsprechend den Vorgaben des BSI dient hierzu die WAN-Schnittstelle des SMGW. Der MSB erfüllt mehrere Funktionalitäten, wobei diese auf eigenständige Instanzen aufgeteilt werden:

Aktiver externer Marktteilnehmer (aEMT):
Als aEMT übermittelt der MSB Preisinformationen sowie P_{lim}-Signale (Informationen über maximale Leistung) über den vom SMGW vermittelten CLS-Proxy an das Heimnetzwerk, genauer gesagt an die HKE (CLS-Gateway).

Passiver externer Marktteilnehmer (pEMT):
Als pEMT empfängt der MSB Messwerte vom Heimnetzwerk.

Gateway-Administrator (GWA):
In der allgemeinen Administratorrolle konfiguriert der MSB den CLS-Proxy-Kanal zwischen dem aEMT und der HKE zur Versendung der Informationen durch den aEMT (s.o.).

2.1.9
VNB

Der Verteilnetzbetreiber ist die unmittelbar mit dem MSB kommunizierende Instanz. Ein zentraler Baustein ist der Netzregler, welcher dem MSB das P_{lim}-Signal übermittelt und vom MSB die Messwerte entgegennimmt.

2.1.10
Aggregator

Der im Wesentlichen aus dem Backend bestehende Aggregator ist eine zentrale Instanz, die mit mehreren anderen Komponenten der Architektur kommuniziert, wobei es in einigen Fällen auch alternative Kommunikationswege gibt. So können Redispatch-Signale entweder direkt an das HEMS oder über den MSB (aEMT) und den SMGW verschickt werden. Der Aggregator kann außerdem Anfragen an den MSB (aEMT) stellen, um einen Kanal zum HKE zur Übermittlung von Preisinformationen aufzubauen. Zu den weiteren festen Aufgaben des Aggregators gehören u.a. der Empfang von Messdaten vom MSB (pEMT) sowie ein Informationsaustausch mit dem Energielieferanten (s.u.). Im Falle einer Notwendigkeit kann der Aggregator auch Ladeanforderungen vom Backend des Fahrzeugherstellers empfangen.

2.1.11
Energielieferant

Der Energielieferant befindet sich in der Architektur als Kommunikationspartner zwischen dem Aggregator und dem MSB. Er versorgt beide Komponenten u.a. mit Informationen über Strompreise. Zu den festen Aufgaben des Energielieferanten gehört außerdem der Austausch von Informationen zu Flexibilitäten mit dem Aggregator. Anstelle des Aggregators kann der Energielieferant auch die Aufgabe übernehmen, beim MSB (aEMT) den Aufbau eines Kanals zur HKE zwecks Übermittlung von Preisinformationen anzufragen.

2.1.12
Weitere Instanz für Redispatch

Zur Abwicklung von Redispatch-Vorgängen wird eine weitere organisatorische Instanz benötigt. Zu den Aufgaben dieser Instanz gehören u.a. der Empfang von Messwerten vom pEMT sowie der Austausch von Signalen zum Redispatch und von Informationen zur Flex-Verfügbarkeit mit dem Aggregator. Diese organisatorische Instanz kann auf unterschiedliche Weise realisiert werden; grundsätzlich ist sie im Bereich des Übertragungsnetzbetreibers (ÜNB) anzusiedeln. Bei der Realisierung der Architektur im Rahmen von uniT-e^2 wird die Equigy Crowd Balancing Platform von Tennet verwendet. Durch eine Anbindung des VNB kann hiermit auch ein gemeinsames Redispatch-System von VNB und ÜNB realisiert werden; dies wurde jedoch in der Harmon-E-Architektur noch nicht umgesetzt.

2.1.13
Fahrzeughersteller und HEMS-Hersteller

Auch der Fahrzeug- und der HEMS-Hersteller bilden mit ihren Backends relevante Komponenten der Harmon-E-Architekur. Der Fahrzeughersteller nimmt vom EV bzw. der EV App Ladeanforderungen entgegen und übermittelt sie bei Bedarf an das Backend des Aggregators oder an das Backend des HEMS-Herstellers. Der HEMS-Hersteller tauscht dann bei Bedarf verschiedene Daten - Messdaten, Anforderungen und Nutzerdaten - mit dem HEMS bzw. der HEMS App aus.

2.2
Protokolle

Um Anwendungsfälle umzusetzen, müssen die einzelnen Komponenten/Entitäten miteinander kommunizieren. Hierzu wird eine Vielzahl an Protokollen verwendet, die im Nachfolgenden kurz beschrieben sind.

2.2.1
ISO 15118

ISO 15118 ist ein mehrteiliger ISO-Standard, welcher die Kommunikation zwischen Fahrzeugen und Energienetzen beschreibt. Die wesentlichen hier beteiligten Instanzen sind das oben beschriebene EVSE sowie der im EV befindliche sogenannte Electric Vehicle Communication Controller (EVCC), welcher die Kommunikation des Fahrzeuges mit der Ladesäule steuert. Darüber hinaus sind noch sogenannte Secondary Actors vorgesehen.

Besonders von Interesse ist der Teil ISO 15118-20, welcher als Neufassung von ISO 15118-2 eine neue Art des Übertragungsprotokolls auf allen Ebenen von der Netzwerkebene (OSI-Schicht 3) bis zur Anwendungsebene (OSI-Schicht 7) beinhaltet. Hier werden auf Anwendungsebene u.a. die Formate der zwischen dem EVCC und dem EVSE

ausgetauschten Nachrichten spezifiziert. An Sicherungsmechanismen ist jetzt u.a. die Verwendung von TLS 1.3 mit einer bilateralen Authentifizierung obligatorisch. In ISO 15118-2 war dies für die meisten Anwendungsbereiche optional. Lediglich für Plug&Charge (PnC) war die ältere TLS-Version 1.2 mit unilateraler Authentifizierung vorgeschrieben.

In der Harmon-E-Architektur wird das ISO 15118-2 Protokoll zwischen dem im Heimbereich abgestellten EV und der im Heimbereich befindlichen Ladesäule angewendet. ISO 15118-20 wurde in der Architektur bisher noch nicht umgesetzt, die Verwendung beschränkt sich derzeit auf das sogenannte Bidi-Labor, in dem bidirektionales Laden erprobt wird.

2.2.2 OCPP

Von der Open Charge Alliance wurde das Open Charge Point Protocol (OCPP) als ein Industriestandard für die Kommunikation zwischen einer Ladesäule (Charging Station - CS) und dem zugehörigen Ladesäulen-Management-System (Charging Station Management System - CSMS) spezifiziert.

In diesem Standard werden u.a. die Formate von ausgetauschten Nachrichten zwischen der CS und dem CSMS spezifiziert. Eine wesentliche Neuheit von OCPP 2.0 und OCPP 2.0.1 gegenüber OCPP 1.6 besteht in der Festlegung von Security Profiles mit TLS, wobei die Nutzung von TLS jedoch optional ist. Eine neue Version 2.1 wurde inzwischen erarbeitet, ist aber noch nicht veröffentlicht.

Ein möglicher Einsatz von OCPP liegt bei der Kommunikation zwischen dem EVSE und dem Aggregator. Außerdem kann man OCPP alternativ zu EEBUS zur Kommunikation der im Heimbereich befindlichen Ladesäule (EVSE) mit dem hauseigenen Energiemanagement-System (HEMS) anwenden. In der Harmon-E-Architektur wurde OCPP jedoch nicht umgesetzt.

2.2.3 EEBUS

Die EEBus Initiative e.V. definiert standardisierte TCP/IP-Protokolle und Use Cases zum Energiemanagement unter der Bezeichnung EEBUS und vereinheitlicht die intelligente herstellerunabhängige Kommunikation zwischen verschiedenen Technologien innerhalb und außerhalb des Hauses. Dabei können beispielsweise Netzbetreiber, HEMS, Wallboxen, PV-Anlagen und weitere Systeme miteinander verbunden werden, wodurch sich eine Steuerung der Verbraucher- und Produktionssysteme realisieren lässt. Das wird vor allem zur Leistungsbegrenzung von Haushalten verwendet, um Netzstabilität sicherzustellen.

In der Harmon-E-Architektur kommt das EEBUS Protokoll zwischen der HKE (in Harmon-E: PPC CLS-Gateway), HEMS, Wallbox (EVSE) sowie den weiteren über das HEMS gesteuerten Komponenten im Haushalt wie HSS, PV-Anlage und WP zum Einsatz. Dabei befindet sich die Software-Komponente von EEBUS in der Steuerungseinrichtung, d.h. der HKE. Das vom aEMT kommende P_{lim}-Signal wird über den sicheren CLS-Proxy von der HKE empfangen und mit dem LPC[1]/LPP[2]-EEBUS Use Case an das HEMS weitergeleitet, das wiederum die angebundenen Komponenten flexibel ansteuern kann, um das Leistungslimit einzuhalten.

1 Limitation of Power Consumption
2 Limitation of Power Production

2.2.4
DIN VDE V 0418-63-8

DIN VDE V 0418-63-8 ist eine Vornorm zur Festlegung von Datenmodellen an der WAN-Schnittstelle des SMGW. Die Vornorm baut u.a. auf der technischen Richtlinie des BSI auf, welche die Spezifikation des SMGW enthält.

Die Datenmodelle werden in der Harmon-E-Architektur vom MSB (aEMT) zur Versendung des P_{lim}-Signals an das SMGW verwendet, wobei hier das Signal per CLS.EEDI über einen vom GWA aufgesetzten verschlüsselten TLS-Kanal an die HKE übermittelt wird.

2.2.5
AS4

AS4 ist ein offener Standard für eine sichere Nachrichtenübertragung im Energiebereich. Zur Absicherung kommen XML-Signaturen und XML-Verschlüsselung zum Einsatz. Eine ausdrückliche Verwendung von AS4 war in der Architektur-Spezifikation ursprünglich nicht vorgesehen; im Bereich der Marktkommunikation ist seine Verwendung jedoch inzwischen obligatorisch (siehe Abschnitt 3.2.1).

2.2.6
IEC 63110

Die Standard-Reihe IEC 63110 befasst sich mit der Spezifikation eines neuen Protokolls für das Management von Ladeinfrastrukturen. Es soll in Zukunft als Alternative zu OCPP (siehe Abschnitt 2.2) dienen. Bislang wurde nur der Teil 1 mit grundlegenden Definitionen, Anwendungsfällen und Architekturen veröffentlicht. Die eigentliche Protokollspezifikation wird erst in Teil 2 erfolgen, welcher sich noch in einem frühen Entwicklungsstadium befindet. Somit kommt eine mögliche Anwendung auf die Harmon-E-Architektur erst bei späteren Weiterentwicklungen in Betracht.

2.2.7
COSEM

Die Companion Specification for Energy Metering (COSEM) bezeichnet eine Serie von Standards mit Kommunikationsprotokollen für den Datenaustausch mit Messgeräten. Hierzu gehört auch die Device Language Message Specification (DLMS). Die Standards gehören zur Serie IEC 62056. In der Harmon-E-Architektur kommt DLMS/COSEM (IEC 62056-4-7, IEC 62056-5-3) bei der Übertragung der Messerte vom SMGW zum peMT zum Einsatz, wobei die Daten im XML-Format vorliegen.

3
Bewertungskriterien IT-Sicherheitseigenschaften

Im Folgenden werden die Bewertungskriterien für IT-Sicherheitseigenschaften dargelegt. Zu diesem Zweck werden zunächst mögliche Sicherheitseigenschaften und -verfahren definiert, anhand derer das Risiko von Angriffen bewertet werden kann. Andererseits wird bei der Bewertung berücksichtigt, ob Sicherheitseigenschaften durch Normen oder Gesetze definiert sind.

3.1
IT-Sicherheitseigenschaften

In diesem Abschnitt werden die verschiedenen Sicherheitseigenschaften, die bei den verschiedenen Komponenten zum Einsatz kommen könnten, um Angriffe zu erschweren, einzudämmen oder zu verhindern, kurz beschrieben. Im Rahmen der Bewertung werden die folgenden Sicherheitseigenschaften berücksichtigt: Transportsicherheit, Einsatz von Hardwaresicherheitsmodulen, sichere Speicherung von sensiblen Daten, Unterteilung von Berechtigungen, Vorhandensein eines Authentifizierungssystems (z. B. PKI) sowie Protokollierung von Sicherheitsvorfällen.

3.1.1
Abgesicherter Datentransport

Innerhalb der vorliegenden Architektur (Kapitel 2) sind alle Anwendungsfälle in hohem Maße vom Datenaustausch abhängig. In diesem Kontext ist es von entscheidender Bedeutung, die Daten während des Transports angemessen zu sichern. Grundsätzlich ist das „CIA-Prinzip" mit den drei wichtigen Sicherheitszielen Vertraulichkeit, Integrität und Verfügbarkeit zu berücksichtigen. Dabei ist zu beachten, dass die Vertraulichkeit nicht für alle Daten und Anwendungsfälle relevant ist.

Grundsätzlich existieren mehrere kryptografische Konzepte, die eine Absicherung von Verbindungen ermöglichen. Dabei stellt die Verschlüsselung von Daten mittels TLS die verbreitetste Variante dar. Des Weiteren findet im Unternehmenskontext die Verwendung von IPsec und vergleichbaren VPN-Technologien statt. Beide Technologien sind auf die Existenz einer aktiven Verbindung zwischen zwei Kommunikationspartnern angewiesen. Als alternative Möglichkeit können asymmetrische Signatur- und Verschlüsselungsverfahren eingesetzt werden, um Kommunikationsszenarien zu realisieren, bei denen keine direkte Verbindung besteht. Als Beispiele können hier das PGP-Verfahren sowie das Signieren von Messwerten im Stromzähler genannt werden.

Die genannten Verfahren ermöglichen die Realisierung von Kommunikationsszenarien, bei denen keine direkte Verbindung zwischen den Kommunikationspartnern besteht.

3.1.2
PKI/Zertifikatsprüfung

Innerhalb der Harmon-E-Infrastruktur erfolgt eine Absicherung der Daten, insbesondere im Kontext des Schlüsselaustauschs von TLS-Verbindungen sowie bei Signaturen, mittels asymmetrischer Kryptografie, auch als Public-Key-Kryptografie bezeichnet. Es ist von essenzieller Bedeutung, den Schlüsseln der Gegenstelle zu vertrauen. Das erforderliche Vertrauen wird entweder durch Kenntnis der Gegenstelle hergestellt oder mittels einer geeigneten Public-Key-Infrastruktur (PKI) gewährleistet. Im Rahmen dessen werden von autorisierten Instanzen Zertifikate signiert, welche anschließend zur Überprüfung der Schlüssel genutzt werden können. In der Vergangenheit wurde bei unseren Wallboxtests

immer wieder festgestellt, dass diese essentielle Prüfung in der Praxis nicht erfolgt und beliebige selbst signierte Zertifikate verwendet werden können. Werden Zertifikate explizit durch gegenseitiges Vertrauen erlaubt (Certificate Pinning) und beim Verbindungsaufbau entsprechend darauf geprüft, so kann auch ohne PKI eine sichere Kommunikation stattfinden.

3.1.3 Sichere Datenspeicher

In diesem Kontext ist zudem die Sicherung der Daten zu berücksichtigen. Auch hier ist das CIA-Prinzip zu wahren. Andernfalls bestünde die Möglichkeit, dass Angreifer in kompromittierten Systemen oder durch physischen Zugriff Daten verändern oder lesen. Zu den geeigneten Maßnahmen zählen Zugriffskontrollsysteme, kryptografische Verschlüsselung und Integritätsschutz.

3.1.4 Hardwaresicherheitsmodul

Reine Software-Lösungen für die Absicherung der Daten sind in komplexen, sicherheitskritischen Systemstrukturen häufig unzureichend. Dies betrifft insbesondere die gesicherte Aufbewahrung geheimer oder privater Schlüssel, was mit einer reinen Software-Lösung nicht gewährleistet ist. Sicherheitslösungen müssen auch in Hardware realisiert werden, um dem System eine hinreichende Stabilität zu bieten. Neben der reinen Absicherung von Daten und der gesicherten Aufbewahrung von Schlüsseln sind auch weitere Funktionalitäten wie die Überprüfung von Systemzuständen und die Unversehrtheit von implementierter Software notwendig.

Zu diesem Zweck sind bestimmte Systemkomponenten mit einem Hardwaresicherheitsmodul (HSM) auszustatten, welches wichtige grundlegende Sicherheitsfunktionen beinhaltet. Die wesentlichen Funktionalitäten eines HSMs sind die folgenden:

- Private und geheime Schlüssel sind sicher gespeichert, sodass kein Zugriff von außen möglich ist.
- Kryptografische Operationen können direkt auf dem HSM sicher ausgeführt werden.
- Die Integrität der Software wird durch Abgleich mit der vom HSM signierten Version geprüft.
- Die Überprüfung des Systemzustandes mittels HSM ermöglicht sichere Softwareupdates.
- Bestimmte Operationen, z.B. Ausführung der kryptografischen Operationen, werden durch Autorisierung von Systembenutzern (mit entsprechenden Rollen) freigeschaltet.
- Der Lesezugriff auf private bzw. geheime Schlüssel ist grundsätzlich gesperrt; eine Schlüsseldatei kann nur gelöscht oder überschrieben werden.

In der Harmon-E-Architektur spielt z.B. der MSB mit dem Aufbau von TLS-Verbindungen in verschiedenen Heimumgebungen eine zentrale Rolle. Hier ist die gesicherte Speicherung der verwendeten privaten Schlüssel in einem HSM angebracht.

Ein HSM kann z.B. durch ein Trusted Platform Module (TPM), eine spezielle von der Trusted Comuting Group spezifizierte HSM-Lösung, realisiert werden. Als Alternativlösung bieten sich z.B. die im Automobilbereich anerkannten und weitverbreiteten EVITA HSMs an. Grundsätzlich ist der Begriff HSM, in Übereinstimmung mit ISO 15118-20, als Oberbegriff zu sehen.

3.1.5
Rollen- und Rechtemanagement

In der Harmon-E-Architektur kommuniziert eine Vielzahl von Instanzen miteinander, und jede Instanz hat dabei bestimmte Rollen und die Berechtigung zur Ausführung von Aktionen. Sowohl natürliche Personen als auch Geräte können Rollen und Rechte beinhalten, wobei die Rollen von Geräten ggf. durch autorisierte Benutzer freigeschaltet werden müssen.

Neben den zahlreichen Geräten in der Systemarchitektur gibt es die folgenden wesentlichen Personenrollen:

- Benutzer der Eigenheimumgebung (Annahme: EV-Besitzer ist Eigenheimbesitzer)
- Monteure und Wartungstechniker von Eigenheimumgebung
- Operateure bei Energielieferant, MSB und VNB

Mit diesen Rollen sind die folgenden Benutzungsrechte verbunden:

- Benutzer der Eigenheimumgebung können die Ladeinfrastruktur nutzen und das EV und die Ladesäule konfigurieren.
- Für die Eigenheimumgebung zuständige Monteure und Wartungstechniker können alle dort befindlichen Komponenten konfigurieren.
- Operateure von Komponenten außerhalb der Eigenheimumgebung (Energielieferant, MSB, VNB) können dort Konfigurationen durchführen, haben jedoch keinen Zugriff auf Komponenten in der Eigenheimumgebung.
- Sowohl Operateure als auch Monteure und Wartungstechniker können Nachrichten an die Eigenheimumgebung senden oder von dort abrufen.

3.1.6
Protokollierung von Sicherheitsvorfällen

Ist im System ein IT-Sicherheitsvorfall aufgetreten (d.h. ein unbefugter Eingriff in die IT-Infrastruktur des Systems), so muss er geeignet protokolliert werden. Hierzu benötigt man geeignete Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS).

Die grundlegenden Aufgaben eines IDS sind die folgenden:

- Erkennung und Klassifizierung von Sicherheitsvorfällen
- Protokollierung und sichere Verwahrung
- Reaktion auf Sicherheitsvorfälle

Ein IPS dient dann zur automatischen Behebung von Sicherheitslücken nach aufgetretenen Sicherheitsvorfällen.

3.2
Vorgegebene Richtlinien

Für die Bewertung betrachten wir vorrangig, ob es etablierte Standards oder Gesetze gibt, die ein Sicherheitsniveau erzwingen. Proprietäre oder herstellerspezifische Lösungen können dasselbe Sicherheitsniveau erreichen, allerdings muss dies nicht für jeden Hersteller gelten.

3.2.1
Normen und Standards

Zusätzlich zu den bereits in Abschnitt 2.2 beschriebenen Protokollen sind nachfolgend aufgelistete Normen und Standards ebenfalls relevant für die Harmon-E-Architektur.

BSI-Richtlinien
Für die Harmon-E-Archtitektur sind mehrere technische Richtlinien des BSI relevant.

Für alle Arten von kryptografischer Absicherung von Daten, für den Transport ebenso wie für die Speicherung, sind die BSI-Richtlinien TR-02102 für kryptografische Verfahren zu beachten. Dies betrifft u.a. die grundlegende Auswahl von Verfahren und Schlüssellängen (Teil 1) sowie den Einsatz von TLS (Teil 2).

Speziell relevant für einige technische Komponenten der Architektur, insbesondere bei der Erhebung und Verarbeitung von Messwerten, sind die Richtlinien TR-03109 für intelligente Messsysteme (Smart Metering). Dies beinhaltet insbesondere die technische Spezifikation des SMGWs (Teil 1) sowie die Richtlinien für die zugehörigen PKIs (Teil 4).

ISO 20078
Die mehrteilige Standard-Reihe 20078 (Extended Vehicles) beschreibt eine Webdienst-Plattform zum Abruf von Fahrzeugdaten. Sie ist in der Harmon-E-Architektur für die Verbindung vom EV zu den Backends der OEMs und des Aggregators relevant.

CENELEC EN 50631
Die Normenreihe EN 50631 befasst sich mit dem Informationsaustausch zwischen Haushaltsgeräten und Energiemanagementsystemen in verschiedenen Arten von Gebäuden. In den verschiedenen Teilen werden sowohl allgemeine als auch produktspezifische Datenmodelle für die Datenübertragung festgelegt. Konkret zum Einsatz in der Harmon-E-Architektur kommt EN 50631 an den EEBUS-Schnittstellen des HEMS mit den verschiedenen Komponenten.

BDEW Web-API
Der Bundesverband der Energie- und Wasserwirtschaft hat kürzlich Regelungen zur Erstellung und Nutzung von API-Webdiensten in der Energiewirtschaft formuliert und in einer API-Guideline dargelegt. In der Harmon-E-Architektur wird die BDEW Web-API für die Übertragung des P_{lim}-Signals vom VNB an den MSB verwendet. Zukünftig sollen diese Webdienste auch bei der Kommunikation zwischen Aggregator und MSB oder alternativ zwischen Energielieferant und MSB zum Einsatz kommen, wenn es um die Anfragen zum Aufbau eines CLS-Proxy-Kanals geht. Ebenso ist ein Einsatz bei der Übertragung des Redispatch-Signals vom Aggregator zum MSB vorgesehen. Letztgenannte zwei Punkte wurden jedoch in der Harmon-E-Architektur bisher nicht umgesetzt.

3.2.2
Juristische Vorschriften und Gesetze

Energiewirtschaftsgesetz (EnWG)
Das EnWG enthält relevante Regelungen für Energiesysteme, insbesondere zur Vermeidung der Überlastung von Stromsystemen. Eine besondere Rolle spielt dabei der in den §§ 13 und 14 vorgegebene Redispatch.

Cyber Resilience Act (CRA)
Der CRA ist eine neue EU-Verordnung mit Vorgaben für die Gewährleistung von Cybersicherheit für jede Art von Produkten, welche miteinander oder mit dem Internet kommunizieren. Auch sie muss beim Design der Harmon-E-Architektur berücksichtigt werden. Dies bedeutet insbesondere die dynamische Gestaltung von

Sicherheitskonzepten, sodass im Falle von erkannten Schwachstellen entsprechende Updates möglich sind.

Neuregelungen der Bundesnetzagentur zu MAKO
Aufgrund eines Beschlusses der Bundesnetzagentur sind Marktpartner für den Bereich Strom für ihre Kommunikation (MAKO) seit dem 01.04.2024 zur Verwendung des AS4-Protokolls (siehe Abschnitt 2.2) verpflichtet. Dies beinhaltet die verpflichtende Einführung einer signierten und verschlüsselten Datenübertragung unter Einbindung einer BSI Smart Metering PKI.

3.2.3 Identifizierte Sicherheitseigenschaften

Im Folgenden sollen die durch die Spezifikation der Architektur vorgegebenen Sicherheitseigenschaften bewertet werden. Dabei beziehen sich die Bewertungen nicht auf eine konkret implementierte Lösung, sondern auf alle denkbaren praktischen Umsetzungen, welche nach den Vorgaben für die Architektur möglich sind. Dies bedeutet, dass hohe Sicherheitsniveaus nur dann gewährleistet sind, wenn ein in der Architektur anzuwendender Standard oder sonstige technische Festlegungen entsprechende Sicherheitseigenschaften beinhalten.

Kryptografische Absicherung mit vorgegebener PKI
Bei der Kommunikation des MSB mit dem SMGW, bei der CLS-Verbindung mit dem aEMT als auch bei der DLMS/COSEM-Verbindung mit dem pEMT, wird eine TLS-Verschlüsselung in Zusammenhang mit einer Smart Metering PKI des BSI verwendet (siehe auch Abschnitt 3.2.1). Gleiches gilt für das Durchreichen des P_{lim}-Signals vom MSB an die HKE über den CLS-Proxy. Auch bei der ISO 15118-2 Kommunikation zwischen dem EV und dem EVSE kommt eine TLS-Absicherung in Zusammenhang mit einer vorgegebenen PKI zum Einsatz. ISO 15118-2 beinhaltet, ebenso wie die bisher nicht in der Architektur eingesetzte ISO 15118-20, selbst lediglich die Spezifikation von Zertifikatsstrukturen und -hierarchien, aber keine PKI. Die Verwendung der Plug&Charge PKI[1] ist jedoch in der Architektur fest vorgesehen.

Für die Übertragung von Messwerten zwischen dem VNB und dem MSB sowie zwischen dem MSB und dem Aggregator (letztes wurde noch nicht praktisch umgesetzt) war in der Architektur lediglich die Verwendung von MAKO-Prozessen vorgesehen; besondere Sicherheitsmechanismen wurden hier nicht spezifiziert. Aufgrund der neuesten Anordnung der Bundesnetzagentur (siehe Abschnitt 3.2.1) besitzt diese Schnittstelle jedoch jetzt zwingend eine kryptografische Absicherung - hier auf Anwendungsebene mit XML-Signaturen und XML-Verschlüsselung - zusammen mit einer BSI Smart Metering PKI.

Ebenfalls durch TLS in Verbindung mit einer PKI abgesichert ist die Übertragung des P_{lim}-Signals vom VNB an den MSB, da eine entsprechende Absicherung in Verbindung mit der BSI Smart Metering PKI durch die zu verwendende BDEW Web-API vorgegeben ist.

Solche Sicherheitsmechanismen mit kryptografischer Absicherung in Kombination mit einer vorgegebenen PKI sind als **Hoch** einzustufen.

Man beachte, dass die Verwendung von TLS bei ISO 15118-2 (im Gegensatz zu ISO 15118-20) noch für zahlreiche Anwendungen optional ist. Man kann die Verwendung von ISO 15118-2 jedoch als sicher betrachten, wenn die gleichzeitige Verwendung von TLS in Verbindung mit einer vorgegebenen PKI als fester Bestandteil der Architektur spezifiziert und nicht als Option dem Implementierer überlassen wird. Dies ist wie oben beschrieben bei der Systemarchitektur von Harmon-E der Fall.

1 https://www.hubject.com/download-pki

EEBUS-Kommunikation mit TLS
Bei einigen Verbindungen kommt das EEBUS-Protokoll zum Einsatz. Dieses beinhaltet die obligatorische Anwendung von TLS 1.2 mit bilateraler Authentifizierung durch selbstsignierte oder PKI-Zertifikate. Allerdings gibt es hier keine Vorgaben zur Gestaltung einer PKI. Auch für die Verwendung von Zertifikaten gibt es nur die Vorgabe, dass jede SHIP Node ein Zertifikat besitzen muss, jedoch keine weiteren Vorgaben für Zertifikatsstrukturen und -hierarchien. Auch die BSI-Richtlinien für die Smart Metering PKI machen an dieser Stelle keine Vorgaben, da die dort spezifizierten Smart Metering Zertifikate lediglich an der WAN-Schnittstelle des SMGW zum Einsatz kommen, während die Nutzung von Zertifikaten an der HAN- und der LMN-Schnittstelle optional ist. Selbstsignierte Zertifikate bieten dennoch ein hohes Sicherheitslevel, da das Zertifikat beim Pairing-Prozess durch den Nutzer als vertrauenswürdig eingestuft wird. Ausgenommen davon ist der nicht empfohlene Auto-Accept-Modus, bei dem in einem Zeitfenster von maximal zwei Minuten jeder Public Key akzeptiert wird. Dieser Modus birgt das Risiko eines Man-in-the-Middle-Angriffs und sollte nicht bei kritischen Systemen wie einem HEMS verwendet werden.

Bzgl. zu verwendender Cipher Suites empfiehlt die EEBUS-SHIP-Spezifikation TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 bei der Verwendung von TLS und sieht zusätzlich TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 und TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 als optionale Erweiterungen vor. Es gab in der Vergangenheit Angriffe, die auf die Schwäche des Cipher Block Chaining (CBC) Modes zurückzuführen sind. Das BSI stuft die Cipher Suite dennoch als sicher ein, allerdings nur unter der Voraussetzung, dass der Text zuerst verschlüsselt und danach über einen Message Authentication Code (MAC) geschützt wird. Dieser Modus nennt sich Encrypt-then-MAC und bietet eine höhere Sicherheit als der zuvor genutzte MAC-then-Encrypt Ansatz. Mit der neuesten Version der gesonderten EEBUS-Spezifikation für Anforderungen an den Installationsprozess für SHIP-Nodes[2] wurden diese BSI-Vorgaben berücksichtigt, wobei TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 für kritische Infrastrukturen aufgrund der zu geringen Länge des Authentifizierungstags (authentication tag) von 64 Bit nicht mehr empfohlen wird.

Ergänzend ist zu erwähnen, dass die EEBUS-Kommunikation neben der TLS-Funktionalität auch eine Art „Heartbeat"-Funktionalität besitzt: Über die aktiven Verbindungen werden laufend Signale als „Lebenszeichen" verschickt, und nach Erhalt dieser Nachricht antwortet die Gegenseite mit einem Acknowledgement-Signal (ACK). Damit lassen sich ungewollte, möglicherweise von einem Angreifer verursachte Unterbrechungen der Übertragung schnell erkennen. Kommt es zu einem Aussetzer der Verbindung, so schalten sich CLS-Komponenten in einen Fail-Safe Modus, in dem eine vordefinierte Leistungsvorgabe aktiviert wird, bis die Verbindung zur Gegenstelle wiederhergestellt ist.

Die Vorgaben zu Cipher Suites in der neuesten SHIP-Spezifikation zum Installationsprozess haben die vorhandenen Sicherheitsvorgaben gegenüber dem Stand zum Projektstart entscheidend vorangebracht. Insgesamt ist den durch EEBUS vorgegebenen Sicherheitsmechanismen deshalb jetzt die Sicherheitsstufe **Hoch** zuzuweisen. Langfristig sollte trotzdem auf Cipher Suites ohne CBC gesetzt werden.

OCPP-Kommunikation mit TLS
Die OCPP-Schnittstelle zwischen dem EVSE und dem Backend wurde wie erwähnt bei Harmon-E nicht realisiert. Da jedoch eine Umsetzung in anderen unIT-e[2]-Clustern erfolgte, soll hier kurz auf das Sicherheitsniveau dieses Protokolls eingegangen werden.

Die Verwendung von TLS ist bei OCPP optional, sodass eine alleinige Festlegung auf OCPP nur eine niedrige Sicherheit bietet. Legt man sich jedoch auf die Verwendung von TLS

2 https://www.eebus.org/wp-content/uploads/2024/07/EEBUS_TS_ShipRequirementsForInstallationProcess_V1.0.0.pdf

fest, so hat man über die OCPP-Spezifikation auch gleich Vorgaben für die Verwendung von Zertifikaten und den Zertifikatsvalidierungspfad. Somit ist einer Festlegung auf OCPP mit TLS, wie sie bei der praktischen Umsetzung in anderen unIT-e²-Clustern getroffen wurde, die Sicherheitsstufe **Hoch** zuzuordnen.

ISO 20078-Kommunikation mit TLS
Die Kommunikation zwischen dem EV und dem OEM-Backend basiert auf ISO 20078-1 und beinhalten damit die Anwendung von TLS 1.2. Vorgaben für die Verwendung einer PKI oder zum Zertifikatsmanagement gibt es keine. Somit bieten diese Verbindungen ein Sicherheitsniveau der Stufe **Mittel**.

Kommunikationen mit optionaler Sicherheit
Bei der Übertragung der Ladeanforderungen vom OEM-Backend an das HEMS-Backend oder den Aggregator wird das Kafka-Protokoll über TCP verwendet. Hier kann TLS eingesetzt werden, die Verwendung ist jedoch, so wie das gesamte Security-Konzept von Kafka, optional.

Alle derartigen optionalen Sicherheitsmechanismen, die man jederzeit deaktivieren kann, sind vom Sicherheitsniveau her grundsätzlich als **Niedrig** einzustufen.

Gewählte Implementierungen, bei denen die Sicherheitsmechanismen aktiviert sind, stellen ggf. ein höheres Sicherheitsniveau dar. Wir gehen bei unseren Bewertungen, wie eingangs erwähnt, jedoch von den niedrigsten Sicherheitsniveaus aus, die bei Einhaltung der Vorgaben für die Umsetzung der Architektur möglich sind.

Unbekannte oder proprietäre Protokolle
Für einige Übertragungswege in der Harmon-E-Architektur wurde bisher kein Protokoll und damit auch keinerlei Sicherheitsmechanismen spezifiziert. Manche Übertragungswege sehen auch proprietäre Protokolle vor. Dies betrifft z.B. die Schnittstellen vom HEMS-Backend zum HEMS und zur HEMS-App sowie die LMN-Schnittstelle zur mME. Dies bedeutet konkret, dass der Hersteller oder Anbieter hier viele Freiheiten hat, an keinerlei Standards gebunden ist und folglich auch keine Sicherheitsmechanismen verwenden muss. Da man hier keinerlei Sicherheitsniveau garantieren kann, sind solche Schnittstellen mit dem Sicherheitsniveau **Niedrig** zu bewerten.

Abb. 3.1 zeigt eine Übersichtsgrafik über die Schnittstellen mit den Sicherheitsstufen der verwendeten Protokolle. OCPP wird, wie schon in den Abschnitten 2.2 und 3.2.3 angemerkt, im Cluster Hamon-E nicht verwendet, kommt allerdings im Gesamtprojekt unIT-e² in anderen Clustern vor. Ausgegraute Pfeile wurden nicht genauer betrachtet.

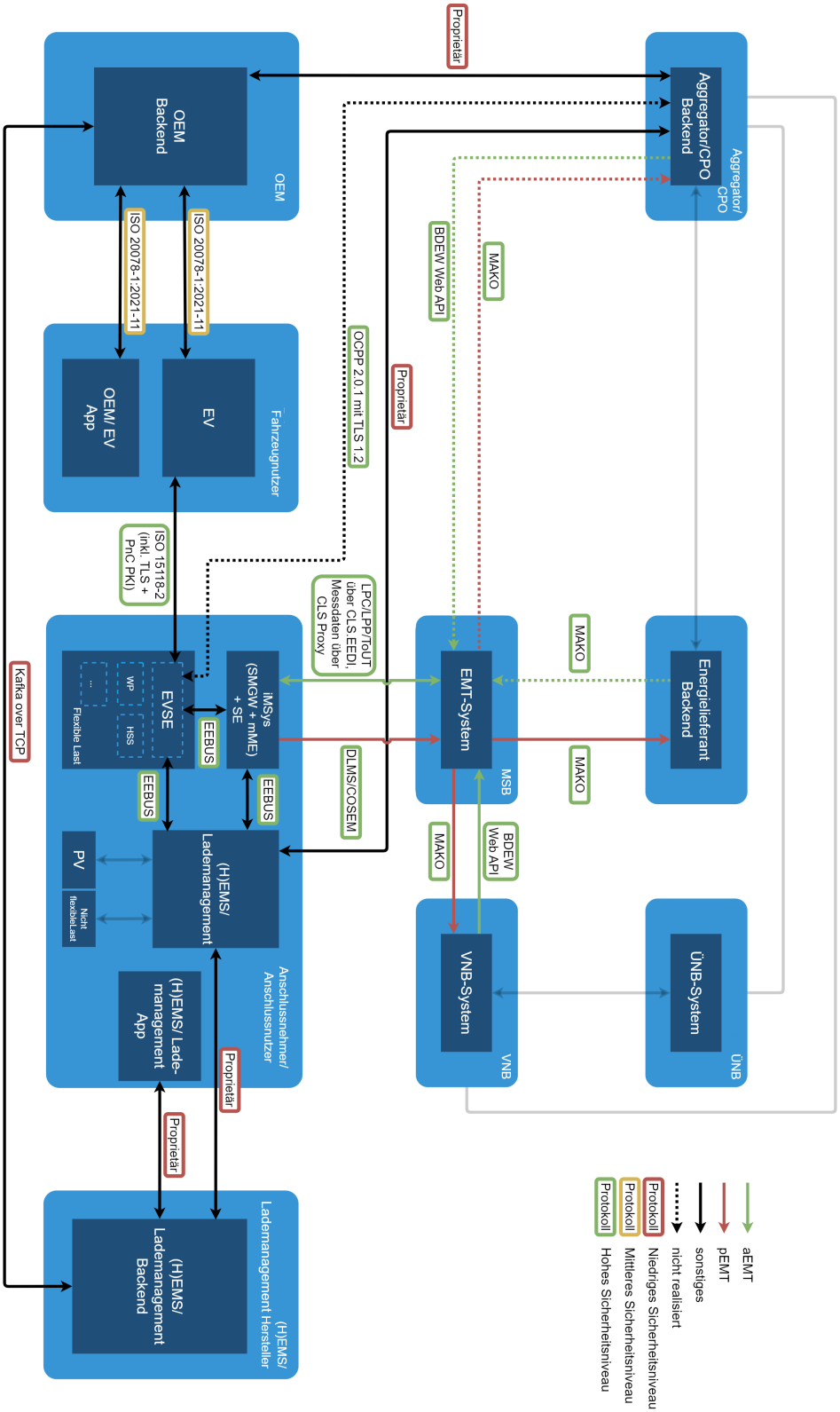

Abb. 3.1
Übersicht über Protokolle mit Sicherheitsniveaus

4
Risiken durch Angreifer

Nachdem im vorherigen Kapitel die Sicherheitsmerkmale identifiziert wurden, werden in diesem Kapitel mögliche Angriffe und die daraus resultierenden Risiken behandelt. Zunächst werden dazu die möglichen Schäden betrachtet, die ein Angreifer in der gegebenen Architektur erzielen kann. Anschließend erfolgt die Identifizierung von Angriffsszenarien.

Üblicherweise erfolgt eine Risikobewertung durch die Gegenüberstellung von Angriffswahrscheinlichkeiten bzw. Schwierigkeitsgraden zur Durchführung von Angriffen und den resultierenden Schäden. Da wir jedoch bereits vorhandene Sicherheitsmaßnahmen identifiziert haben, mit denen man die Durchführung von Angriffen erschweren kann, wählen wir einen anderen Ansatz und stellen die bei einem Angriff identifizierten Schadensauswirkungen dem Niveau der identifizierten Sicherheitsmaßnahmen gegenüber.

4.1
Verursachte Schäden

Die potenziellen Schäden sind vielfältig. Möglich sind Abrechnungsbetrug, die Störung von einzelnen Fahrzeugen und Geräten, aber auch globale Auswirkungen bis hin zur Instabilität ganzer Stromnetze. Bei einigen Schadensszenarien hängt die Höhe des Schadens vom Umfang des betroffenen Personenkreises ab.

Grundsätzlich gibt es verschiedene Kategorien von Schäden. Eine Schadenskategorie ist die Gefährdung der Sicherheit für den Benutzer, den Betreiber und die Umgebung (Safety). Darüber hinaus gibt es finanzielle Schäden sowie Schäden operationaler Art, welche die grundlegende Funktionsfähigkeit von Systemkomponenten beeinträchtigen. Ebenfalls zu berücksichtigen sind Schäden in Form von Verletzungen von Vertraulichkeit und Privatsphäre; letztere sind nicht bei allen Anwendungsfällen relevant, müssen jedoch bei einer Risikoanalyse stets mit betrachtet werden. In der Regel fallen die Schadensstufen für die unterschiedlichen Kategorien, und damit auch die resultierenden Risiken, auch beim selben Schadensszenario unterschiedlich aus. In der Gesamt-Bewertung eines Schadensszenarios gehen wir stets von der höchsten Schadensstufe aus, die bei einer Kategorie auftritt.

4.1.1
Störung der Stabilität des Stromnetzes

Die Herbeiführung von Instabilitäten im Stromnetz birgt für die betroffene Bevölkerung und den Netzbetreiber sowie die involvierten Instanzen ein signifikantes Risiko. Für alle Bewohner des betroffenen Gebietes sind elektronische Geräte nicht mehr regulär nutzbar. Dies umfasst Fahrzeuge, Küchengeräte, Heizungen, aber auch IT-Systeme. Kritische Infrastrukturen wie Krankenhäuser wären auf die Verwendung von Notstromgeneratoren angewiesen.

Die verursachten Schäden sind zunächst operationaler Natur und lassen sich für den Bewohner je nach Länge des Ausfalls in die Kategorien **niedrig** bis **mittel** einordnen. Für den Netzbetreiber betrifft der Ausfall das Kerngeschäft und ist daher im Bereich **mittel** bis **hoch** zu verorten. Für den Energieanbieter können sich finanzielle Schäden ergeben, sollte es aufgrund nicht erbrachter Leistungen zu Einnahmeausfällen kommen. Bei einem **hohen** Schaden sind auch Auswirkungen auf Industriebetriebe und kritische Infrastruktur nicht ausgeschlossen, bei denen Menschenleben durch den Ausfall betroffen sind. Des

Weiteren drohen Schäden an der Infrastruktur, beispielsweise durch ungewöhnlich hohe Spannungen, welche Schäden an Stromverteilern verursachen.

Das genaue Ausmaß der Schäden infolge einer gestörten Stabilität des Stromnetzes hängt davon ab, in welchem Umfang ein Angriff das Stromnetz durchdringen kann. Eine *lokale Manipulation am Stromnetz*, bei der nur von einzelnen Stromanschlüssen störende Aktionen ausgeführt werden, ist ausschließlich als **niedrig** zu bewerten.

Insgesamt umfasst das mögliche Schadensausmaß die volle Breite von **Niedrig** bis **Hoch**, sodass man für die Gesamtbewertung von einem möglichen **hohen** Schaden ausgehen muss.

4.1.2 Unterbrechen des Ladevorgangs

Ein erfolgreicher Angriff auf den Ladevorgang kann dazu führen, dass das Fahrzeug nicht mehr funktionsfähig ist. Dies kann verschiedene Ursachen haben. Zunächst kann es passieren, dass die Batterie nicht ausreichend aufgeladen wird, um das Fahrzeug in Betrieb zu setzen. Ein unsachgemäßer Abbruch eines Ladevorgangs kann zudem zur Konsequenz haben, dass das Fahrzeug nicht mehr ordnungsgemäß von der Ladesäule getrennt und folglich nicht mehr von dort wegbewegt werden kann.

Diese Schäden und Risiken betreffen zunächst den Fahrzeugbesitzer und sind operationeller Natur. Die Schadenshöhe ist als **Niedrig** einzustufen, da das Fahrzeug in diesem Fall komplett unbenutzbar ist, allerdings nur eine geringe Personenanzahl betroffen ist. Nur in speziellen Anwendungsfällen (Feuerwehr, Polizei, Notarzt oder ÖPNV) können die Auswirkungen größer sein, mit mehr betroffenen Personen oder mit schlimmeren Folgen, was die Schadenskategorie **Mittel** rechtfertigt.

Für den Energieanbieter können sich finanzielle Schäden im **hohen** Bereich ergeben, wenn durch einen Angriff viele Ladevorgänge gleichzeitig abgebrochen werden. Dies ist insbesondere der Fall, wenn die Energie beim Ladevorgang direkt vermarktet wird oder wenn ein derartiger Vorfall Reputationsschäden zur Folge hat, welche dann zu Börsenverlusten führen.

Somit kann die Schadenshöhe, je nach Art und Umfang der Betroffenen, auch hier die volle Breite von **Niedrig** bis **Hoch** umfassen, d.h. man muss bei der Gesamtbewertung von der Schadensstufe **Hoch** ausgehen.

4.1.3 Manipulation der Fahrzeugsoftware

Eine Manipulation der Fahrzeugsoftware birgt für den Fahrzeugbesitzer zunächst ähnliche Risiken wie das Unterbrechen des Ladevorgangs. Grundsätzlich ist die Funktionsfähigkeit des Fahrzeugs gefährdet, d.h. es handelt sich um operationale Risiken. Die Schadenshöhe hängt davon ab, welche konkreten Funktionalitäten durch manipulierte Software beeinträchtigt werden. Im schlimmsten Fall kann auch hier das gesamte Fahrzeug funktionsuntüchtig sein. Grundsätzlich sind die Schäden jedoch für einen einzelnen Fahrzeugbesitzer, ähnlich wie bei der Unterbrechung des Ladevorgangs, nur als **niedrig** anzusetzen, während bei der Betroffenheit einer größeren Fahrzeugflotte auch Schäden der Kategorie **Mittel** auftreten können.

Allerdings können hier, neben den operationalen Schäden, **hohe** Schäden für die Sicherheit des Fahrzeugbesitzers, auch für Leib und Leben, auftreten, wenn das Fahrzeug während des laufenden Betriebes ein unerwartetes Fehlverhalten zeigt.

4.1.4
Störung der Geräte im Haus-/Firmennetz

Eine Störung der Geräte im Hausnetz kann für den Hausbesitzer, der die Geräte nutzt, mit Schäden und Risiken verbunden sein. Das Ausmaß der Schäden ist abhängig vom jeweiligen Gerät.

Grundsätzlich handelt es sich um operationale Risiken. Es besteht jedoch auch die Möglichkeit von Schäden für Leib und Leben, wenn das Gerät durch Fehlverhalten entsprechende Gefahren verursachen kann. Der Schweregrad der Schäden ist in diesem Kontext von der Art des Geräts und der verursachten Fehlfunktionen abhängig und bewegt sich demnach im **mittleren Bereich**.

4.1.5
Manipulation von Zählerständen und Abrechnungsdaten

Eine Manipulation von Zählerständen und Abrechnungsdaten durch einen Angreifer kann sowohl für den Hausbesitzer als auch für den Netzbetreiber bzw. Energielieferanten potenzielle Schäden nach sich ziehen. Dabei umfasst diese Schadenkategorie alle Informationsflüsse, die schlussendlich zu einer Änderung der Rechnung führen können.

Die hieraus resultierenden Schäden und Risiken sind überwiegend finanzieller Natur. Dabei können Manipulationen sowohl zugunsten des Stromkunden als auch des Energieanbieters erfolgen. Je nach Szenario kann dies unterschiedliche Auswirkungen haben. So können Steuersignale manipuliert werden, um für eine Flexibilität beim Ladevorgang bezahlt zu werden, ohne diese tatsächlich anzubieten. Manipulierte Zählerstände oder übertragene Zählerwerte wirken sich direkt auf die Zahlung nach verbrauchtem Strom aus. Weiterhin können beim Stromanbieter Manipulationen im Abrechnungssystem die Rechnung beeinflussen.

Die Schadenshöhe für den Hausbesitzer kann als **mittel**, für Netzbetreiber und Energieanbieter dagegen je nach Anzahl der betroffenen Haushalte auch als **hoch** betrachtet werden.

4.1.6
Unbefugter Abgriff persönlicher Daten

Die Zählerstände und Abrechnungsdaten unterliegen dem besonderen Schutz personenbezogener Daten. Bereits das unbefugte Abhören der Daten kann ein Sicherheitsrisiko darstellen. Dies stellt einen Eingriff in die Privatsphäre des Hausbesitzers dar. Die Schadenshöhe ist jedoch als **niedrig** einzustufen, solange es sich um einen begrenzten Datensatz handelt (einzelne Betroffene über einen begrenzten Zeitraum).

4.2
Mögliche Angriffsszenarien

4.2.1
Kriterien zur Klassifizierung von Angriffen

Die Angriffsszenarien zur Herbeiführung der in Abschnitt 4.1 beschriebenen Schäden sind nach verschiedenen Kriterien zu unterscheiden.

Grundlegende Art des Angriffs
Folgende grundsätzliche Arten von Angriffen sind möglich:

- Systemkomponenten können direkt manipuliert werden, sodass sie nicht mehr richtig funktionieren und ggf. falsche Daten aussenden.
- Die Kommunikation zwischen Systemkomponenten an entsprechenden Schnittstellen kann unterbrochen werden. Damit wird der Datenaustausch zwischen den Komponenten unterbunden.
- Entlang der Übertragungsschnittstellen können übertragene Daten manipuliert oder neue, gefälschte Daten eingespielt werden. Die empfangende Systemkomponente wird dadurch getäuscht und geht davon aus, dass es sich um echte, gewollte Daten der sendenden Komponente handelt.
- Übertragungsschnittstellen können missbraucht werden, um den Systemkomponenten nicht vorgesehene Daten zuzufügen und damit ihre Funktionalitäten zu stören.
- Übertragene Daten können ausgespäht und abgegriffen und anschließend missbräuchlich verwendet werden.

Durchführbarkeit
Um verschiedene Angriffe durchzuführen, braucht man unterschiedliche Voraussetzungen. Systemkomponenten und Schnittstellen im Netz können nur remote angegriffen werden. Hierzu zählen etwa das OEM-Backend, die PKI, der VNB, der MSB sowie das HEMS-Backend. Für Komponenten in der Heimumgebung mit externen Schnittstellen sind sowohl Remote- als auch lokale Angriffe mit physischem Zugang möglich; dies betrifft die HKE und das SMGW. Systemkomponenten und Schnittstellen in der Heimumgebung, z.B. das HEMS, die Ladesäule sowie die ISO 15118- und die EEBUS-Schnittstellen können lokal angegriffen werden, d.h. der Angreifer kann über physischen Zugriff mit dem System interagieren. Ein rein physischer Angriff skaliert jedoch schlechter als ein Remote-Angriff. Zu möglichen Unterbrechungen der EEBUS-Kommunikation ist anzumerken, dass derartige Angriffe prinzipiell durchführbar sind, jedoch mit Hilfe der eingebauten Heartbeat-Funktionalitäten schnell erkannt werden können. Durch den Failsafe-Modus, der bei fehlenden Heartbeats aktiviert wird, kann weiterhin zur Netzstabilität beigetragen werden.

4.2.2 Konkrete Szenarien

Nachfolgend werden verschiedene Szenarien beschrieben, um die in Abschnitt 4.2.1 beschriebenen grundlegenden Angriffsarten umzusetzen.

Angriff auf Datenübertragung zwischen Heimumgebung und MSB
Ein Remote-Angriff auf die Netzwerkverbindung der Heimumgebung mit dem MSB verursacht Störungen der Datenübertragung von und zum HEMS und zur HKE. Hiervon betroffene Daten sind das P_{lim}-Signal, Preistabellen, Redispatch-Signal sowie Messdaten. Die Folgen sind Störungen von Hausgeräten und der Ladesäule. Die Messdaten können persönliche, vertrauliche Daten darstellen, sodass ein Angriff auf die Datenübertragung mit dem MSB auch eine Verletzung der Privatsphäre des Hauseigentümers bedeuten kann.

Angriff auf weitere Kommunikationen mit dem MSB
Auch die Netzwerkverbindungen des MSB mit dem VNB und dem Energielieferanten können Ziele von Angreifern sein. Eine Manipulation oder Unterbrechung dieser Datenübertragung kann zunächst zur Folge haben, dass VNB und Energielieferant entweder falsche Messdaten bekommen oder dass keine Messdaten mehr bei ihnen ankommen. Auch Manipulationen der Heimumgebung können an dieser Verbindung ansetzen, indem die ordnungsgemäße Übermittlung des P_{lim}-Signals oder eine Anfrage zum Aufbau einer transparenten CLS-Verbindung zur HKE gestört wird.

Angriff auf Ladekommunikation
Ein lokaler Angriff auf die ISO 15118-Schnittstelle zwischen EV und EVSE kann eine Manipulation oder einen Abbruch des Ladevorgangs verursachen. Relevante Daten

bestehen aus Ladeplänen und sonstigen Steuerbefehlen für den Ladevorgang.

Angriff auf EEBUS-Schnittstellen im Heimnetzwerk
Ein lokaler Angriff auf die EEBUS-Schnittstellen zwischen den Systemkomponenten des Heimnetzwerkes hat in der Heimumgebung zunächst ähnliche Auswirkungen wie eine Störung der Kommunikation mit dem MSB. Betroffene Daten sind die vom HEMS benötigten und übermittelten Daten - P_{lim}-Signal, Preistabellen und Messwerte sowie Steuerbefehle an das EVSE. Betroffen von diesen Angriffen sind zusätzlich die vom HEMS gesteuerten Flexibilitäten mit den übermittelten Fahrplandaten.

Direkter Angriff auf das HEMS
Eine weitere mögliche Angriffsstrategie besteht in einer direkten Manipulation des HEMS, welches dann seine Funktionen nicht mehr ordnungsgemäß ausführen kann. Diese Art von Angriff verursacht ähnliche Folgen wie eine Störung der EEBUS-Kommunikation, kann aber auch zur Überlastung des Netzes führen, wenn koordiniert mehrere HEMS angegriffen und beispielsweise P_{lim}-Steuersignale ignoriert werden. Grundsätzlich kann ein Angriff auf das HEMS entweder durch direkten physischen Zugriff oder über die externen Verbindungen zum HEMS-Backend oder zum Aggregator erfolgen.

Physischer Angriff auf die Ladesäule
Hat es ein Angreifer auf die Störung oder Unterbrechung von Ladevorgängen abgesehen, so kann er zu diesem Zweck auch einen direkten physischen Angriff auf die Ladesäule ausführen.

Remote-Angriff auf den MSB
Ein Remote-Angriff auf den MSB kann verschiedenartige Störungen mit Fehlfunktionen verschiedenartiger Komponenten sowohl in der Heimumgebung als auch im übrigen Netzwerk verursachen. Ein DoS-Angriff führt im schlimmsten Fall bis zu einer Lahmlegung der gesamten Infrastruktur inkl. der Komponenten in der Heimumgebung. Weitere Manipulationen des MSB haben ähnliche Auswirkungen wie die vorher beschriebenen Manipulationen der Datenübertragungswege vom und zum MSB.

Remote-Angriff auf den VNB
Direkte Angriffe auf den VNB haben unmittelbaren Einfluss auf den MSB als nachgeschaltete Instanz. Durch einen DoS-Angriff kann die Übermittlung von P_{lim}-Signalen an den MSB komplett unterbunden werden. Sonstige Manipulationen, u.a. auch die Störung der Verarbeitung empfangener Messwerte, führen zur möglichen Übermittlung falscher P_{lim}-Signale.

Remote-Angriff auf das HEMS-Backend
Durch einen Angriff auf das HEMS-Backend oder den Kommunikationskanal zwischen Backend und HEMS erlangt der Angreifer die Fähigkeiten, sämtliche Steuersignale zu übertragen, die regulär auch vom Hersteller gesendet werden können. Dies umfasst die mögliche Kontrolle über einen Ladevorgang oder den Batteriespeicher. Weiterhin können Informationen über das Verhalten von Hausbesitzern über das Backend abgefragt werden, die sich aus dem Steuerverhalten und Sensorinformationen des Hauses ergeben. Ein koordinierter Angriff auf mehrere HEMS zur gleichen Zeit kann zudem Einfluss auf die Stabilität des Netzes nehmen.

Remote-Angriff auf den Energielieferanten oder den Aggregator
Direkte Angriffe auf den Energielieferanten oder den Aggregator, welche sich bei bestimmten Funktionen gegenseitig ergänzen bzw. alternativ in Aktion treten können, haben die Störung der Übermittlung verschiedenartiger Informationen und Signale zur Folge. Hierzu gehört z.B. der Empfang von Messdaten sowie die Versendung von Redispatch-Signalen und Preisinformationen.

Kompromittierung kryptografischer Schlüssel
Ein fundamentales Angriffsszenario ist das Kompromittieren kryptografischer Schlüssel. Geheime oder private Schlüssel können beispielsweise aus einem HSM ausgelesen oder aus der Firmware extrahiert werden, wenn diese Komponenten unzureichend gesichert sind. Nach einer erfolgreichen Kompromittierung ist ein Angreifer im Besitz des Schlüssels und kann ihn zur unbefugten Entschlüsselung oder zum unbefugten Signieren von Daten verwenden. Somit können entsprechende Angriffe zur Manipulation oder Verfälschung sowie zum unbefugten Abhören von Daten durchgeführt werden, bei denen der jetzt kompromittierte Schlüssel zur Absicherung dient.

4.3 Abschließende Bewertung

Zur abschließenden Bewertung der Risiken werden die an einer Stelle in der Architektur erkannten möglichen Schäden mit ihrer Schadenshöhe gemäß Abschnitt 4.1 den in Abschnitt 3.2.3 an derselben Stelle identifizierten Sicherheitseigenschaften gegenübergestellt. Sofern Schadensszenarien je nach ihrem Ausmaß unterschiedlich zu bewerten sind, ist immer von der höchstmöglichen Schadenshöhe auszugehen. Sind ausreichend hohe Sicherheitseigenschaften vorhanden, so kann das resultierende Risiko auch für hohe Schäden gering gehalten werden. Ernst zu nehmende Risiken bestehen nur dann, wenn keine geeigneten Sicherheitsmaßnahmen existieren, um ein zum entsprechenden Schaden führendes Angriffsszenario abzuwehren. Tabelle 4.1 zeigt eine Übersicht über das Bewertungsschema. Dabei ist zu beachten, dass die Bewertung auf den Annahmen der Architektur und Sicherheitsvorgaben von Standards basiert. Jeder Betreiber kann durch die Implementierung von zusätzlichen Maßnahmen sein Sicherheitsniveau bereits erhöht und damit das Risiko reduziert haben.

	Niedrig	Mittel	Hoch	**Schadens-bewertung**
Niedrig	Niedrig	Mittel	Hoch	
Mittel	Niedrig	Mittel	Mittel	
Hoch	Niedrig	Niedrig	Niedrig	
Sicherheits-niveau				**Finales Risiko**

Tabelle 4.1
Bewertungsschema für finales Risiko

Tabelle 4.2 zeigt die finalen Risikobewertungen der Schadens- und Angriffsszenarien, die in Abbildung 4.1 in die Referenzarchitektur eingebettet werden.

Tabelle 4.2
Finale Risikobewertungen

Schadens-szenario	Angriffs-szenario	Schadens-höhe	Sicherheits-niveau	Finales Risiko
Instabilität im Stromnetz	Manipulation der Datenüber-tragung von Heimumgebung zum MSB	Hoch	Hoch	Niedrig
Instabilität im Stromnetz	Manipulation der Datenübertra-gung zwischen MSB und Aggre-gator	Hoch	Hoch	Niedrig
Instabilität im Stromnetz	Manipulation der Datenübertra-gung zwischen MSB und VNB	Hoch	Hoch	Niedrig
Instabilität im Stromnetz	Manipulation der Datenübertra-gung zwischen HEMS und Ba-ckend	Hoch	Niedrig	Hoch
Instabilität im Stromnetz	Manipulation der Datenübertra-gung zwischen HEMS und Aggre-gator	Hoch	Niedrig	Hoch
Störung der Geräte im Haushalt	Manipulation der Datenübertra-gung im Heim-netzwerk (EEBUS-Schnittstellen)	Mittel	Hoch	Niedrig
Lokale Mani-pulation am Stromnetz	Manipulation der Datenübertra-gung im Heim-netzwerk (EEBUS-Schnittstellen)	Mittel	Hoch	Niedrig
Verfälschung von Mess- und Abrech-nungsdaten	Manipulation der Datenüber-tragung von Heimumgebung zum MSB	Hoch	Hoch	Niedrig
Verfälschung von Mess- und Abrech-nungsdaten	Manipulation der Datenübertra-gung zwischen MSB und VNB	Hoch	Hoch	Niedrig

Verfälschung von Abrechnungsdaten (lokal)	Manipulation der Datenübertragung im Heimnetzwerk (LMN-Schnittstelle zur mME)	Mittel	Niedrig	Mittel
Verfälschung von Messdaten (lokal)	Manipulation der Datenübertragung im Heimnetzwerk (EEBUS-Schnittstellen)	Mittel	Hoch	Niedrig
Unterbrechung des Ladevorgangs	Manipulation oder Unterbrechung der Ladekommunikation an der ISO 15118-2 oder ISO 15118-20-Schnittstelle zwischen EV und EVSE	Hoch	Hoch	Niedrig
Manipulation der Fahrzeugsoftware	Missbräuchliche Nutzung der Schnittstelle zwischen EV und OEM Backend	Hoch	Mittel	Mittel
Abgreifen persönlicher Daten	Abhören von Kommunikation	Niedrig	<abhängig von abgehörter Kommunikationsverbindung>	Niedrig

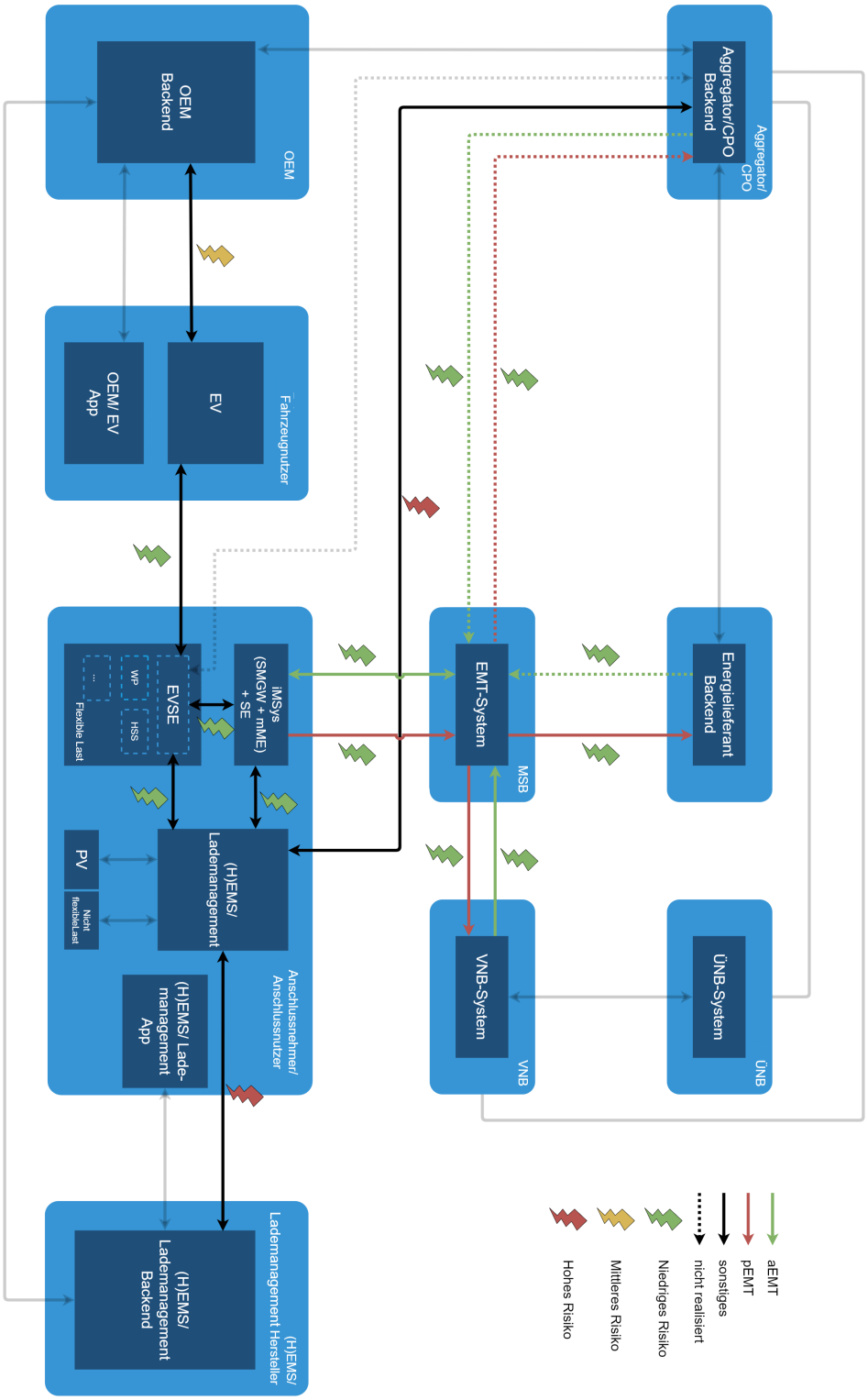

Abb. 4.1
Übersicht der finalen Risiken als Ergebnis der Gegenüberstellung von Schadenshöhe und Sicherheitsniveau

5
Zusammenfassung

Wie gezeigt, ist das Gesamtsystem des gesteuerten und bidirektionalen Ladens eine komplexe Infrastruktur mit zahlreichen Entitäten und Kommunikationswegen. Jede einzelne dieser Komponenten ist potenziell Angriffen ausgesetzt. Im Whitepaper haben wir dargelegt, dass je nach geforderten Sicherheitseigenschaften und deren Position in der Architektur unterschiedliche Risiken bestehen.

Insbesondere sind Kommunikationskanäle kritisch zu betrachten, die die Laststeuerung beeinflussen und bei denen keine Sicherheitsmaßnahmen vorgeschrieben sind, obwohl sie gleichzeitig eine Vielzahl von Lasten oder Generatoren steuern können. Dazu zählen die Steuerung des HEMS über das Herstellerbackend sowie die Verbindung zwischen MSB und VNB, ebenso wie die Verbindung zum und vom Aggregator.

Unsere Untersuchung bezieht sich ausschließlich auf die bestehenden Standards und gesetzlichen Vorgaben sowie auf technische Vorgaben durch die Spezifikation der Architektur, und nicht auf die tatsächlichen Implementierungen, die möglicherweise ein abweichendes Sicherheitsniveau bieten können.

Es zeigt sich, dass ein Großteil der Schnittstellen in der Harmon-E-Architektur durch technische und gesetzliche Vorgaben und verwendete Standards bereits hinreichend abgesichert ist, um die Angriffsrisiken gering zu halten. Dennoch besteht ein offensichtlicher Handlungsbedarf zur Modifikation der bestehenden Architekturspezifikation mit weiteren technischen Vorgaben, da die bestehenden Sicherheitsanforderungen durch aktuelle gesetzliche Vorgaben und verwendete technische Standards noch nicht vollständig abgedeckt sind. Die Verwendung geeigneter Sicherheitsmechanismen, insbesondere an den hier identifizierten kritischen Stellen mit erhöhtem Sicherheitsrisiko, muss durch die Architekturspezifikation vorgegeben sein. Insbesondere an Stellen, an denen die Bereitstellung von Sicherheitsmechanismen in einem technischen Standard optional ist,muss ihre Bereitstellung für die Architektur vorgegeben werden. Sofern die Verwendung proprietärer Protokolle vorgesehen ist, müssen nachvollziehbare Sicherheitsmechanismen der Spezifikation hinzugefügt werden. Bei Verwendung von Protokollen mit optionalen Sicherheitsmechanismen muss eine Aktivierung dieser Mechanismen durch die Architekturspezifikation vorgegeben werden.

Ungeachtet des bereits gewährleisteten Sicherheitsniveaus durch Verwendung von ISO 15118-2 in Verbindung mit der Plug&Charge PKI ist die Implementierung von ISO 15118-20 an der Schnittstelle zwischen dem EV und dem EVSE baldmöglichst anzustreben.

Die hier aufgezeigten Analyseergebnisse sollten auch in die Standardisierung einfließen. Sofern hier bei technischen Standards Defizite in Bezug auf die Vorgabe von Sicherheitsmaßnahmen festgestellt wurden, sollten diese bei der nächsten Überarbeitung der Standards berücksichtigt werden.