Fraunhofer AISEC

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT AISEC

Betrachtung von Security-Risiken der DigitalTWIN Use Cases

ERSTELLT IM AUFTRAG VON

se commerce

DIGITAL TWIN

Fraunhofer AISEC

Betrachtung von Security-Risiken der DigitalTWIN Use Cases

Peter Schneider, Hannah Wester, Michael Heinl

Oktober 2020

Erstellt im Auftrag von

se commerce

DIGITAL TWIN

Version 1.0

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit
www.aisec.fraunhofer.de

Fraunhofer AISEC
Lichtenbergstraße 11
85748 Garching (bei München)

Kontakt Autoren
hannah.wester@aisec.fraunhofer.de
michael.heinl@aisec.fraunhofer.de

Kontakt Abteilungsleitung Product Protection & Industrial Security
bartol.filipovic@aisec.fraunhofer.de
daniel.angermeier@aisec.fraunhofer.de

Inhaltsverzeichnis

1. Einleitung

Die drei im Vorhaben DigitalTWIN beschriebenen Use Cases erfordern die Umsetzung gezielter IT-Sicherheitsmaßnahmen, um die neuen Technologien auch in Zukunft robust gegen Ausfälle, vertraulich, integer und authentisch betreiben zu können. In Szenario 1 geht es um das Monitoring im Betrieb und die Wartungsunterstützung basierend auf in Fassadenelementen verbauter Sensorik. Die hier verbauten Sensoren liefern Daten, die als Grundlage für Betriebsdaten sowie zur Optimierung der Wartung genutzt werden. Szenario 2 beschreibt hingegen die datengestützte Fertigung auf der Baustelle anhand einer Remote-Schweißprüfung. Darauf aufbauend wird in Szenario 3 durch eine virtuelle Montageunterstützung am Beispiel eines Stahlknotenpuzzles eine noch engere Integration von Baustelle und Digitalisierung vorgenommen.

Um einen Überblick über allgemeine Risiken und fehlende Schutzmaßnahmen für die angedachten Use Cases des Forschungsprojekts zu gewinnen, wurde die in Kapitel 2 beschriebene Methode *Modular Risk Assessment* (MoRA) zur Erstellung von Risikoanalysen angewandt. Ein wohldefiniertes Bewertungsmodell und eine detaillierte Modellierung ermöglichen eine aussagekräftige Risikoanalyse und die Erstellung eines dedizierten Schutzkonzeptes. Aufgrund der generischen Natur der DigitalTWIN Use Cases befinden sich die vorliegenden Betrachtungen auf einem höheren Abstraktionslevel, weshalb sie einerseits zwar weniger konkret, andererseits jedoch auch für eine breitere Zielgruppe relevant und nachvollziehbar sind. Der Einstieg („Basis“) wurde bewusst mit geringeren Anforderungen modelliert, damit durch die Anwendung der erweiterten Maßnahmen („ALL“) die jeweiligen Unterschiede bei der Risikobewertung deutlich werden. Einige Risiken wurden unter Umständen zu hoch eingeschätzt, da z. B. keine Aussage über Zutrittskontrollen zum Gebäude gemacht werden konnten. Bei entsprechend spezifizierten Use Cases lässt sich der Detaillierungsgrad wesentlich erhöhen, technisch vertiefen und damit eine höhere Aussagekraft erzielen.

Die Betrachtung der Security-Risiken hat gezeigt, dass sich für die in DigitalTWIN angedachten Use Cases drei wesentliche Herausforderungen ergeben. Zuerst muss die Integrität der Komponente selbst gewährleistet werden. Dies stellt sowohl bei verbauter Sensorik als auch bei Komponenten, die auf Baustellen verwendet werden, eine besondere Schwierigkeit dar. Zusätzlich muss die Kommunikation in der Regel vor Manipulation geschützt sein, da im schlimmsten Fall die Integrität des Gebäudes gefährdet ist. Hierzu sind vor allem sichere Speicherelemente notwendig, um das verwendete Schlüsselmaterial seinerseits vor unberechtigten Zugriffen zu schützen.

2. Methode

Mit Hilfe der am Fraunhofer AISEC entwickelten Methode MoRA [1, 2] wurden die Use Cases analysiert und angedachte Security-Maßnahmen evaluiert. MoRA wurde ursprünglich konzipiert, um die Erstellung von Risikoanalysen als Teil des sicheren Entwicklungsprozesses in der Automobilbranche einzuführen. Mittlerweile hat sich die Methode insbesondere in dieser Domäne bei namhaften OEMs etabliert, wird aber auch in anderen Industrien erfolgreich angewandt.

MoRA gliedert sich in vier Blöcke:

- Modellieren des Untersuchungsgegenstandes,
- Bewerten des Schutzbedarfs,
- Erstellen und Bewerten von Bedrohungen und Schutzmaßnahmen sowie
- Analysieren der Risiken und Reduzieren der Restrisiken durch den Vorschlag neuer Schutzmaßnahmen.

Um den Schutzbedarf bewerten und Angriffe modellieren zu können, muss zuerst ein geeignetes Modell des Untersuchungsgegenstandes erstellt werden. Hierfür werden *Funktionen*, *Komponenten* und *Daten* modelliert. Aus den Funktionen geht der wesentliche Schutzbedarf des Untersuchungsgegenstandes hervor. Die Komponenten können hierarchisch gegliedert werden und je nach Granularität der Untersuchung sowohl strukturgebende Komponenten wie Gebäude als auch technische Komponenten wie PCs und Sensoren oder darauf laufende Softwarekomponenten beschreiben. Daten beschreiben die Informationen, die im Rahmen der Funktionen ausgetauscht werden, oder kryptografisches Material, von dem Schutzmaßnahmen abhängen. Die Daten können sowohl nur auf einer Komponente gespeichert sein als auch in einem *Datenfluss* zwischen Komponenten über eine *Technologie* übertragen werden. Durch die Zuordnung von Datenflüssen zu Funktionen können auch die daran beteiligten Komponenten und Daten auf die Funktionen abgebildet werden. Die modellierten Assets wie Funktionen und Komponenten werden als Knoten in einem Graphen modelliert. Die Abhängigkeiten wie Datenflüsse und Funktionszugehörigkeit stellen die Kanten zwischen den Knoten dar.

Für Funktionen, Komponenten und Daten wird im Anschluss der Schutzbedarf durch Erstellung von *Schutzzielen* festgehalten, indem für die *Schutzzielklassen* Integrität/Authentizität, Verfügbarkeit und Vertraulichkeit der Assets bewertet wird, welche Schäden entstehen können, wenn diese Schutzziele jeweils verletzt

werden. Die möglichen Schäden werden bereits im Bewertungsmodell in Kategorien wie Safety, finanzielle Schäden und rechtliche Verstöße gegliedert und innerhalb der Kategorien in Schadenslevel abgestuft. Dadurch kann die Bewertung der einzelnen Assets einheitlich erfolgen. Die Bewertung der Schäden ist zunächst unabhängig von bereits angedachten Schutzmaßnahmen, um die Wirksamkeit eben dieser Schutzmaßnahmen ebenfalls bewerten zu können. Die Methode richtet sich bei der Schutzbedarfsbewertung nach dem IT-Grundschutz [3].

Im Folgenden werden die *Bedrohungen* schematisch nach Microsoft STRIDE [6] auf die modellierte Architektur, d. h. auf alle Datenflüsse und Komponenten sowie die entsprechenden Schutzbedarfe, angewandt, je nachdem welche Schutzzielklasse der Angriff bedroht. Die Bedrohungen können nach Common Criteria [4] bewertet werden, um den Angriffsaufwand festzulegen. Zudem können *Schutzmaßnahmen* erstellt werden, die über die Architektur auf Bedrohungen abgebildet werden und entweder einen Einfluss auf den Angriffsaufwand oder auf den Schutzbedarf haben.

Ein Risiko wird meist als eine Wahrscheinlichkeit, dass ein gewisser Schaden eintritt, beschrieben. Da ein Angreifer nicht deterministisch ist, ist es schwierig, im Security-Umfeld eine Wahrscheinlichkeit zu berechnen. Stattdessen wird deshalb eine Risikomatrix definiert, die einer Schadenshöhe und einem Angriffsaufwand ein Risikolevel zuordnet. Ein Risiko beschreibt somit den Angriffsaufwand durch eine oder mehrere Bedrohungen, die unter Umständen von Schutzmaßnahmen erschwert werden, sowie die Schadenshöhe der angegriffenen Assets.

Im letzten Schritt werden die Risiken analysiert, um eine erste Risikobehandlung nach ISO 27005 [5] vorzunehmen. Es können z. B. weitere Schutzmaßnahmen definiert werden, um die Risiken zu reduzieren. Um einen Vergleich der Risiken mit jeweils unterschiedlichen umgesetzten Maßnahmen durchführen zu können, können Schutzmaßnahmen in unterschiedliche Gruppen gegliedert werden. Dies ermöglicht, den Nutzen einer Schutzmaßnahmen direkt aus der Risikoanalyse herauszulesen.

3. Größte Risiken

In den folgenden Absätzen werden die wesentlichen Erkenntnisse aus den einzelnen Betrachtungen zusammengefasst. Die ausführlichen Berichte finden sich im Anhang. Zur besseren Integration in dieses Dokument wurden die Berichte teilweise zusammengefasst sowie größtenteils automatisiert aus der sich kontinuierlich weiterentwickelnden Microsoft Excel Vorlage in das PDF-Format konvertiert.

3.1. Szenario 1

Im Folgenden werden die relevantesten Risiken des ersten Szenarios (*Monitoring im Gebäudebetrieb und Wartungsunterstützung*) dargestellt.

3.1.1. Manipulation als MitM auf Bluetooth beim Pairing

Bluetooth-Verbindungen können während des Pairings leicht angegriffen werden. Hier besteht ein sehr hohes Risiko, dass Angreifer sich während des Pairings als MitM etablieren können.

3.1.2. Abhören und Manipulieren von LAN-Verbindungen innerhalb des Gebäudes, beim Planer und im Internet

Da die Verbindungen innerhalb des Gebäudes, beim Planer sowie über das Internet zum Zeitpunkt der Betrachtung gänzlich ungeschützt sind, besteht ein sehr hohes Risiko, dass Kommunikation dort abgehört oder manipuliert werden kann. Das Risiko kann durch die Verwendung von Transport Layer Security (TLS) zur Authentifizierung und Verschlüsselung deutlich reduziert werden.

3.1.3. Angriffe auf die Sensoren im Isoshade-Element und die IT-Infrastruktur

Da die Sensoren im Isoshade-Element über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren. Dasselbe Risiko besteht auch bei den IT-Infrastrukturen von Gebäude und Planer.

3.2. Szenarien 2 und 3

Die Szenarien 2 (*Schweißprüfung*) und 3 (*Virtuelle Montageunterstützung*) ähneln sich in ihrer Struktur und dadurch auch in den zugehörigen Security-Betrachtungen sehr. Sie bauen auf der Infrastruktur aus Szenario 1 auf und implizieren entsprechend auch diese Risiken. Zusätzlich entstehen in Szenario 2 und 3 weitere, zueinander ähnliche Risiken, die für beide Szenarien nachfolgend betrachtet werden.

3.2.1. Angriffe auf die Datenemitter

Da die Datenemitter über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

3.2.2. Angriffe auf die IT-Infrastruktur Bereich 1 und 2

Da die IT-Infrastruktur im Bereich 1 über keine Schutzmechanismen verfügt und zudem wichtige Daten liefert, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

4. Schutzkonzept

Im Folgenden wird das Schutzkonzept skizziert, das sich aus der Betrachtung der Risiken ergibt, sowie weitere, sich daraus ergebende Prozesse beschrieben.

4.1. Wichtige Maßnahmen

Die Kommunikation innerhalb des Gebäudes sowie beim Planer muss vor Manipulation und Abhören geschützt werden. Dies kann unter anderem durch die Verwendung von TLS geschehen. Hierbei ist auf geeignete TLS Cipher Suites zu achten (siehe hierzu auch Anhang D). Bei der Verwendung von TLS ist außerdem die sichere Ablage des Schlüsselmaterials wichtig.

Im Kontext von DigitalTWIN müssen daher insbesondere alle Hardware-Systeme, die vor Ort auf einer Baustelle zu finden sind und an der TLS-Kommunikation teilnehmen, ein Hardware Security Module (HSM) oder eine vergleichbare Technologie verwenden. Andernfalls kann ein Angreifer durch physikalischen Zugriff auf die Systeme zu leicht an das Schlüsselmaterial gelangen.

Alternativ lassen sich Gebäude und andere IT-Infrastrukturen auch mittels Virtual Private Network (VPN) sicher miteinander verbinden (z. B. per IPsec, SSH-Tunnel, Wireguard). Bei der Verwendung von Funkschnittstellen ist generell zu bedenken, dass diese sich nur unzureichend gegen kurzfristige Unterbrechungen schützen lassen. Zudem ist bei der Nutzung von Bluetooth darauf zu achten, dass zwischen Level und Modi unterschieden wird. Für eine vertrauliche und integre Kommunikation sollte hierbei der Security Level 4 verwendet werden.

Da Sensorik in allen Szenarien eine zentrale Rolle spielt, ist die Integrität sowie Authentizität der von ihnen gelieferten Daten sehr wichtig. Die Sensoren der Isoshade-Elemente dürfen für einen Angreifer daher physisch nicht zugänglich sein. Sowohl für die Sensoren und Datenemitter als auch für die IT-Infrastrukturen muss eine System-Härtung vorgenommen werden. Eine solche System-Härtung enthält unter anderem:

- Beschränkung von Privilegien durch restriktives Nutzer- und Rollenkonzept;
- Entfernen unnötiger Software(-schnittstellen) wie z. B. Hintergrunddienste;
- Entfernen aller unnötigen physikalischen Schnittstellen;
- Entfernen eventuell vorhandener Debugschnittstellen;
- Erzwingen von Authentifizierung für vorhandene Wartungsschnittstellen;

- Kontinuierliche Aktualisierung aller verwendeten Software;
- Zeitnahes Fixen bekannter Security-Schwachstellen verwendeter Software.

Es ist möglich, dass gerade die Sensoren nicht alle diese Anforderungen erfüllen können. In diesem Fall bleiben Restrisiken bestehen.

4.2. Sichere Update-Prozesse für Sensorik

Gerade bei kleinen Sensoren stellen regelmäßige Security-Updates eine Herausforderung dar. Hierfür muss ein Update-Paket mit einer Signatur sowie ein zentraler und zugänglicher Ablageort bereitgestellt werden. Im einfachsten Fall können die Sensoren selbständig in regelmäßigen Abständen bei einem Webserver nach neuen Updates anfragen. Das laufende System des Sensors muss dann die Signatur prüfen. Hier ist es wichtig sicherzustellen, dass die Signatur zur ausgelieferten Datei und das Zertifikat zum Server (z. B. Abgleich der URL) passt. Eine solche Signatur darf nur dann akzeptiert werden, wenn sie von einer vertrauenswürdigen Stelle stammt. Hierfür können öffentliche Certification Authorities (CA) oder aber auch eigens für das Projekt aufgesetzte Public Key Infrastrukturen (PKI) als Vetrauensanker (engl. *trust anchor*) verwendet werden. Erst nach dieser Prüfung darf das Update installiert werden.

Da Security-Updates oft vor Angriffen auf die Sensorik selbst schützen sollen, muss auch der Update-Prozess beschützt werden. Dies erfordert einen sicheren Speicher für erlaubte Zertifikate oder Vertrauensanker, der hardwareseitig vor Manipulation geschützt ist. HSMs, Trusted Platform Modules (TPMs) und Produkte einzelner Hersteller (z. B. ARM TrustZone) können hierfür Lösungen bereitstellen.

Literatur

[1] Daniel Angermeier, Kristian Beilke, Gerhard Hansch und Jörn Eichler. "Modeling security risk assessments". In: *17th escar Europe : embedded security in cars (Konferenzveröffentlichung)*. 2019. DOI: 10.13154/294-6670.

[2] Daniel Angermeier, Alexander Nieding und Jörn Eichler. "Supporting Risk Assessment with the Systematic Identification, Merging and Validation of Security Goals". In: *Risk Assessment and Risk-Driven Testing: 4. International Workshop, RISK 2016, Revised Selected Papers*. 2016.

[3] *BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise*. Version 2.0. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile&v=3.

[4] *Common Criteria for Information Technology Security Evaluation*. Version 3.1 Revision 5. 2017. URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf.

[5] *ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management*. Standard. International Organization for Standardization, Juli 2018.

[6] Microsoft. *The STRIDE Threat Model*. 2009. URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

Anhang

A. Monitoring im Gebäudebetrieb und Wartungsunterstützung

A.1. Komponenten

Nachfolgend werden alle in der Analyse berücksichtigten Komponenten aufgelistet. Dieser Teil dient als Referenz für die spätere Zuordnung von Maßnahmen zu Komponenten.

Tabelle A.1.: IDs und Namen der Komponenten.

ID	Name
CP1	Isoshade-Element
CP2	Sensoren (inklusive Sensorelektronik / Datenlogger und Funkmodul zuzüglich USB-Anschluss)
CP4	Funkmodul
CP5	Bereich / Raum / Stockwerk / Gebäude
CP6	Desktop / Tablet
CP7	VR / AR / MR Devices
CP8	ScaleIT Edge-Server
CP9	IT-Infrastruktur Gebäude
CP10	Unternehmen / Gebäude
CP11	IT-Infrastruktur Unternehmen
CP14	IT-Infrastruktur Planer
CP17	Desktop / Tablet
CP18	ScaleIT Enterprise Server

Die Komponenten kommunizieren untereinander wie in Abbildung A.1 skizziert.

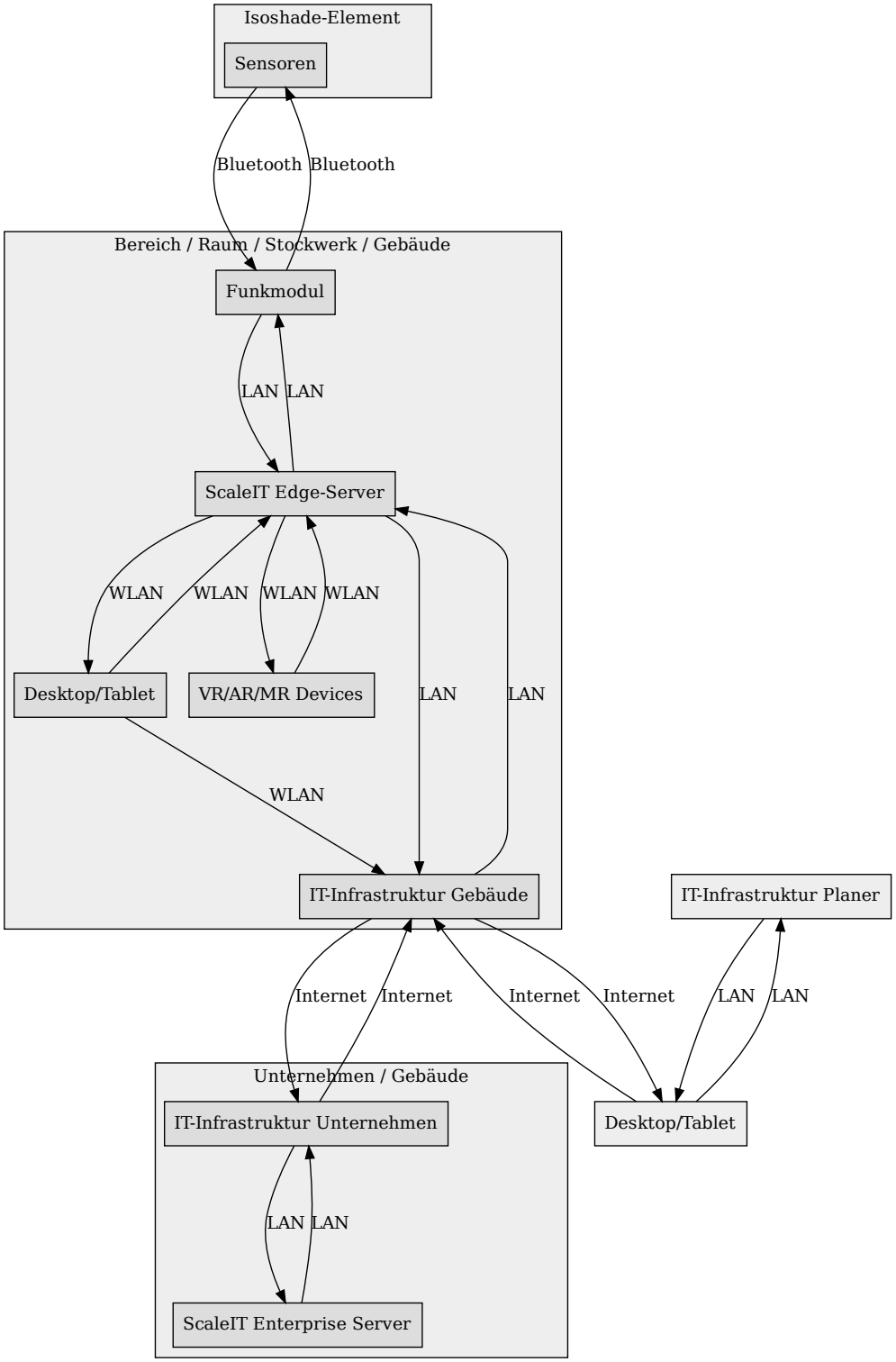

Abbildung A.1.: Systemarchitektur Use Case 1.

A.2. Datenflüsse

Im Detail werden die folgenden Kommunikationspfade und Technologien berücksichtigt:

Tabelle A.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N1	Die Sensoren senden D1 Sensordaten zum Funkmodul unter Benutzung von Bluetooth.
N2	Das Funkmodul sendet D1 Sensordaten zum ScaleIT Edge-Server unter Benutzung von LAN.
N3	Das Desktop / Tablet sendet D2 Steuerung Sonnenschutz zum ScaleIT Edge-Server unter Benutzung von WLAN.
N4	Der ScaleIT Edge-Server sendet D2 Steuerung Sonnenschutz zum Funkmodul unter Benutzung von LAN.
N5	Das Funkmodul sendet D2 Steuerung Sonnenschutz zu den Sensoren unter Benutzung von Bluetooth.
N6	Der ScaleIT Edge-Server sendet D3 Daten zur Auswertung, Archivierung / Speicherung zur IT-Infrastruktur Gebäude unter Benutzung von LAN.
N7	Die IT-Infrastruktur Gebäude sendet D3 Daten zur Auswertung, Archivierung / Speicherung zur IT-Infrastruktur Unternehmen unter Benutzung des Internets.
N8	Das Desktop / Tablet sendet D2 Steuerung Sonnenschutz zur IT-Infrastruktur Gebäude unter Benutzung von WLAN.
N9	Die IT-Infrastruktur Gebäude sendet D2 Steuerung Sonnenschutz zum ScaleIT Edge-Server unter Benutzung von LAN.
N10	Der ScaleIT Edge-Server sendet D2 Steuerung Sonnenschutz zum Funkmodul unter Benutzung von LAN.
N11	Das Funkmodul sendet D2 Steuerung Sonnenschutz zu den Sensoren unter Benutzung von Bluetooth.
N12	Der ScaleIT Edge-Server sendet D3 Daten zur Auswertung, Archivierung / Speicherung zur IT-Infrastruktur Gebäude unter Benutzung von LAN.
N13	Die IT-Infrastruktur Gebäude sendet D3 Daten zur Auswertung, Archivierung / Speicherung zur IT-Infrastruktur Unternehmen unter Benutzung des Internets.

Tabelle A.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N14	Die IT-Infrastruktur Unternehmen sendet D3 Daten zur Auswertung, Archivierung / Speicherung zum ScaleIT Enterprise Server unter Benutzung von LAN.
N15	Das Desktop / Tablet sendet D9 Anfrage der Daten zum Monitoring zur IT-Infrastruktur Gebäude unter Benutzung des Internets.
N16	Die IT-Infrastruktur Gebäude sendet D9 Anfrage der Daten zum Monitoring zum ScaleIT Edge-Server unter Benutzung von LAN.
N17	Der ScaleIT Edge-Server sendet D5 Daten zum Monitoring zur IT-Infrastruktur Gebäude unter Benutzung von LAN.
N18	Die IT-Infrastruktur Gebäude sendet D5 Daten zum Monitoring zum Desktop / Tablet unter Benutzung von Internet.
N19	Der ScaleIT Enterprise Server sendet D4 Daten zur Wartung zur IT-Infrastruktur Unternehmen unter Benutzung von LAN.
N20	Die IT-Infrastruktur Unternehmen sendet D4 Daten zur Wartung zur IT-Infrastruktur Gebäude unter Benutzung von Internet.
N21	Die IT-Infrastruktur Gebäude sendet D4 Daten zur Wartung zum ScaleIT Edge-Server unter Benutzung von LAN.
N22	Der ScaleIT Edge-Server sendet D4 Daten zur Wartung zum Desktop / Tablet unter Benutzung von WLAN.
N23	Der ScaleIT Edge-Server sendet D4 Daten zur Wartung zu den VR / AR / MR Devices unter Benutzung von WLAN.
N24	Das Desktop / Tablet sendet D8 Anfrage der Daten zur Wartung zum ScaleIT Edge-Server unter Benutzung von WLAN.
N25	Die VR / AR / MR Devices senden D8 Anfrage der Daten zur Wartung zum ScaleIT Edge-Server unter Benutzung von WLAN.
N26	Der ScaleIT Edge-Server sendet D8 Anfrage der Daten zur Wartung zur IT-Infrastruktur Gebäude unter Benutzung von LAN.
N27	Die IT-Infrastruktur Gebäude sendet D8 Anfrage der Daten zur Wartung zur IT-Infrastruktur Unternehmen unter Benutzung des Internets.
N28	Die IT-Infrastruktur Unternehmen sendet D8 Anfrage der Daten zur Wartung zum ScaleIT Enterprise Server unter Benutzung von LAN.
N29	Das Desktop / Tablet sendet D10 Anfrage der Planungsdaten zur IT-Infrastruktur Planer unter Benutzung von LAN.

Tabelle A.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N30	Die IT-Infrastruktur Planer sendet D10 Anfrage der Planungsdaten zur IT-Infrastruktur Gebäude unter Benutzung von Internet.
N31	Die IT-Infrastruktur Gebäude sendet D10 Anfrage der Planungsdaten zum ScaleIT Edge-Server unter Benutzung von LAN.
N32	Der ScaleIT Edge-Server sendet D6 Planungsdaten zur IT-InfrastrukturGebäude unter Benutzung von LAN.
N33	Die IT-Infrastruktur Gebäude sendet D6 Planungsdaten zur IT-Infrastruktur Planer unter Benutzung des Internets.
N34	Die IT-Infrastruktur Planer sendet D6 Planungsdaten zum Desktop / Tablet unter Benutzung von LAN.

A.3. Schutzziele

Im Folgenden wird der Schutzbedarf aufgezeigt. Für jedes Schutzziel der betrachteten Funktionen wird die maximale Schadenshöhe und die möglichen Schäden in Schadenskategorien geordnet aufgelistet. Die Schutzziele der Daten und Komponenten unterscheiden sich kaum von denen der Funktionen und werden deshalb zur besseren Übersichtlichkeit nicht extra aufgelistet.

CNF.F1: Vertraulichkeit der Nutzung von Messdaten durch Nutzer

Schadenshöhe: Very Low

- Laws and Privacy: Personally identifiable information (PII)

Erklärung:
PII: Personenbeziebare Daten, z. B. Anwesenheitszeiten

INT.F1: Integrität der Nutzung von Messdaten durch Nutzer

Schadenshöhe: Low

- Quality: Service required (QSV)

Erklärung:
QSV: Reparatur notwendig

AVA.F1: Verfügbarkeit der Nutzung von Messdaten durch Nutzer

Schadenshöhe: Low

- Quality: Service required

CNF.F2: Vertraulichkeit der Nutzung von Messdaten durch Betreiber

Schadenshöhe: Very Low

- Laws and Privacy: Personally identifiable information

INT.F2: Integrität der Nutzung von Messdaten durch Betreiber

Schadenshöhe: Moderate

- Financial: Small damages to building
- Laws and Privacy: Service-level agreement violation
- Quality: Service required (QSV)

Erklärung:
QSV: Reparatur beauftragen

AVA.F2: Verfügbarkeit der Nutzung von Messdaten durch Betreiber

Schadenshöhe: Low

- Quality: Service required

CNF.F3: Vertraulichkeit der Nutzung von Messdaten durch Produkthersteller

Schadenshöhe: Very Low

- Laws and Privacy: Personally identifiable information

INT.F3: Integrität der Nutzung von Messdaten durch Produkthersteller

Schadenshöhe: High

- Financial: Severe damages to building
- Laws and Privacy: Service-level agreement violation (SLA)
- Quality: Service required

Erklärung:
SLA: Wartungsvertrag

AVA.F3: Verfügbarkeit der Nutzung von Messdaten durch Produkthersteller

Schadenshöhe: Low

- Quality: Service required

CNF.F4: Vertraulichkeit der Nutzung von Messdaten durch Planer

Schadenshöhe: Very Low

- Laws and Privacy: Personally identifiable information

INT.F4: Integrität der Nutzung von Messdaten durch Planer

Schadenshöhe: Low

- Financial: Low financial damage (FLO)

Erklärung:
FLO: falsche Messdaten fließen in Folgeplanungen ein

AVA.F4: Verfügbarkeit der Nutzung von Messdaten durch Planer

Schadenshöhe: Low

- Quality: Service required (QSV)

Erklärung:
QSV: Messdaten für Planung benötigt

A.4. Maßnahmen

Maßnahmen beschreiben die (technische) Implementierung von Sicherheitsanforderungen, um Risiken zu verringern. Im Folgenden werden die Maßnahmen gemäß ihrer Zuordnung zu den Gruppen aufgelistet. Jede einzelne Maßnahme ist als Kombination von ID und Name aufgeführt. Falls vorhanden, werden die beschützten Technologien, geschützte Archtiketurelemente und die Schutzzielklasse, gefolgt von einer Beschreibung, angegeben.

Verfügbare Maßnahmen sind wie folgt gruppiert:

- Basis: Basis-Maßnahmen
- Erweitert: Zusätzlich vorgeschlagene Maßnahmen, um Restrisiken zu reduzieren

A.4.1. Basis-Maßnahmen

C1: WPA2-Enterprise

Beschützte Technologien: WLAN

Bei Komponenten / Datenflüssen:

- N3 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [WLAN],
- N8 CP6 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D2 Steuerung Sonnenschutz [WLAN],
- N22 CP8 ScaleIT Edge-Server -> CP6 Desktop / Tablet: D4 Daten zur Wartung [WLAN],
- N23 CP8 ScaleIT Edge-Server -> CP7 VR / AR / MR Devices: D4 Daten zur Wartung [WLAN],
- N24 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N25 CP7 VR / AR / MR Devices -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

Bemerkung: Wenn darauf geachtet wird, dass sichere Passwörter verwendet werden, wird WPA2-Enterprise als sichere State-of-the-Art/(SotA)-Maßnahme gesehen.

C3: Bluetooth-Sicherheit

Beschützte Technologien: Bluetooth

Bei Komponenten / Datenflüssen:

- N1 CP2 Sensoren -> CP4 Funkmodul: D1 Sensordaten [Bluetooth],
- N5 CP4 Funkmodul -> CP2 Sensoren: D2 Steuerung Sonnenschutz [Bluetooth],
- N11 CP4 Funkmodul -> CP2 Sensoren: D2 Steuerung Sonnenschutz [Bluetooth]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solang das Pairing sicher abläuft.

C4: Firewall

Beschützte Technologie: Internet

Bei Komponenten / Datenflüssen:

- N7 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N13 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N15 CP17 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D9 Anfrage der Daten zum Monitoring [Internet],
- N18 CP9 IT-Infrastruktur Gebäude -> CP17 Desktop / Tablet: D5 Daten zum Monitoring [Internet],
- N20 CP11 IT-Infrastruktur Unternehmen -> CP9 IT-Infrastruktur Gebäude: D4 Daten zur Wartung [Internet],
- N27 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D8 Anfrage der Daten zur Wartung [Internet],
- N30 CP14 IT-Infrastruktur Planer -> CP9 IT-Infrastruktur Gebäude: D10 Anfrage der Planungsdaten [Internet],
- N33 CP9 IT-Infrastruktur Gebäude -> CP14 IT-Infrastruktur Planer: D6 Planungsdaten [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential Basic

Bemerkung: Keine Einschätzung möglich, da keine Angaben über die Konfiguration der Firewall gemacht wurden.

C5: Virtualisierung durch Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP8 ScaleIT Edge-Server,
- CP18 ScaleIT Enterprise Server

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: High

C6: Zugriffsschutz für ScaleIT / Username + Passwort

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP8 ScaleIT Edge-Server,
- CP18 ScaleIT Enterprise Server

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: Enhanced-Basic

Bemerkung: Da wir keine Informationen über eine Passwort-Policy oder eine Beschränkung der Login-Versuche haben, ist die Maßnahme mit geringem Angriffsaufwand bewertet.

C10: HTTP Auth Token basiert

Beschützte Technologie: WLAN, LAN, Internet

Bei Komponenten / Datenflüssen:

- N3 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [WLAN],
- N8 CP6 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D2 Steuerung Sonnenschutz [WLAN],
- N22 CP8 ScaleIT Edge-Server -> CP6 Desktop / Tablet: D4 Daten zur Wartung [WLAN],

- N23 CP8 ScaleIT Edge-Server -> CP7 VR / AR / MR Devices: D4 Daten zur Wartung [WLAN],
- N24 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N25 CP7 VR / AR / MR Devices -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N2 CP4 Funkmodul -> CP8 ScaleIT Edge-Server: D1 Sensordaten [LAN],
- N4 CP8 ScaleIT Edge-Server -> CP4 Funkmodul: D2 Steuerung Sonnenschutz [LAN],
- N6 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N9 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [LAN],
- N10 CP8 ScaleIT Edge-Server -> CP4 Funkmodul: D2 Steuerung Sonnenschutz [LAN],
- N12 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N14 CP11 IT-Infrastruktur Unternehmen -> CP18 ScaleIT Enterprise Server: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N16 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D9 Anfrage der Daten zum Monitoring [LAN],
- N17 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D5 Daten zum Monitoring [LAN],
- N19 CP18 ScaleIT Enterprise Server -> CP11 IT-Infrastruktur Unternehmen: D4 Daten zur Wartung [LAN],
- N21 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D4 Daten zur Wartung [LAN],
- N26 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D8 Anfrage der Daten zur Wartung [LAN],
- N28 CP11 IT-Infrastruktur Unternehmen -> CP18 ScaleIT Enterprise Server: D8 Anfrage der Daten zur Wartung [LAN],
- N29 CP17 Desktop / Tablet -> CP14 IT-Infrastruktur Planer: D10 Anfrage der Planungsdaten [LAN],
- N31 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D10 Anfrage der Planungsdaten [LAN],
- N32 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D6 Planungsdaten [LAN],

- N34 CP14 IT-Infrastruktur Planer -> CP17 Desktop / Tablet: D6 Planungsdaten [LAN],
- N7 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N13 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N15 CP17 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D9 Anfrage der Daten zum Monitoring [Internet],
- N18 CP9 IT-Infrastruktur Gebäude -> CP17 Desktop / Tablet: D5 Daten zum Monitoring [Internet],
- N20 CP11 IT-Infrastruktur Unternehmen -> CP9 IT-Infrastruktur Gebäude: D4 Daten zur Wartung [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential: Enhanced-Basic

C11: 5G-Sicherheit

Beschützte Technologie: WLAN

Bei Komponenten / Datenflüssen:

- N3 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [WLAN],
- N8 CP6 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D2 Steuerung Sonnenschutz [WLAN],
- N22 CP8 ScaleIT Edge-Server -> CP6 Desktop / Tablet: D4 Daten zur Wartung [WLAN],
- N23 CP8 ScaleIT Edge-Server -> CP7 VR / AR / MR Devices: D4 Daten zur Wartung [WLAN],
- N24 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N25 CP7 VR / AR / MR Devices -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN]

Betroffene Schutzzielklassen: INT Integrity, CNF Confidentiality

Benötigtes Angriffspotential: Moderate

Bemerkung: Diese Maßnaßme ist auf WLAN angewandt, da zum Zeitpunkt der Erstellung der Analyse nicht bekannt ist, ob das Netzwerk auf WLAN oder 5G-Technologie basiert.

A.4.2. Erweiterte Maßnahmen

C2: TLS

Beschützte Technologien: LAN, WLAN, Internet

Bei Komponenten / Datenflüssen:

- N2 CP4 Funkmodul -> CP8 ScaleIT Edge-Server: D1 Sensordaten [LAN],
- N4 CP8 ScaleIT Edge-Server -> CP4 Funkmodul: D2 Steuerung Sonnenschutz [LAN],
- N6 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N9 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [LAN],
- N10 CP8 ScaleIT Edge-Server -> CP4 Funkmodul: D2 Steuerung Sonnenschutz [LAN],
- N12 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N14 CP11 IT-Infrastruktur Unternehmen -> CP18 ScaleIT Enterprise Server: D3 Daten zur Auswertung, Archivierung / Speicherung [LAN],
- N16 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D9 Anfrage der Daten zum Monitoring [LAN],
- N17 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D5 Daten zum Monitoring [LAN],
- N19 CP18 ScaleIT Enterprise Server -> CP11 IT-Infrastruktur Unternehmen: D4 Daten zur Wartung [LAN],
- N21 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D4 Daten zur Wartung [LAN],
- N26 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D8 Anfrage der Daten zur Wartung [LAN],
- N28 CP11 IT-Infrastruktur Unternehmen -> CP18 ScaleIT Enterprise Server: D8 Anfrage der Daten zur Wartung [LAN],
- N29 CP17 Desktop / Tablet -> CP14 IT-Infrastruktur Planer: D10 Anfrage der Planungsdaten [LAN],
- N31 CP9 IT-Infrastruktur Gebäude -> CP8 ScaleIT Edge-Server: D10 Anfrage der Planungsdaten [LAN],
- N32 CP8 ScaleIT Edge-Server -> CP9 IT-Infrastruktur Gebäude: D6 Planungsdaten [LAN],

- N34 CP14 IT-Infrastruktur Planer -> CP17 Desktop / Tablet: D6 Planungsdaten [LAN],
- N3 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D2 Steuerung Sonnenschutz [WLAN],
- N8 CP6 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D2 Steuerung Sonnenschutz [WLAN],
- N22 CP8 ScaleIT Edge-Server -> CP6 Desktop / Tablet: D4 Daten zur Wartung [WLAN],
- N23 CP8 ScaleIT Edge-Server -> CP7 VR / AR / MR Devices: D4 Daten zur Wartung [WLAN],
- N24 CP6 Desktop / Tablet -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N25 CP7 VR / AR / MR Devices -> CP8 ScaleIT Edge-Server: D8 Anfrage der Daten zur Wartung [WLAN],
- N7 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N13 CP9 IT-Infrastruktur Gebäude -> CP11 IT-Infrastruktur Unternehmen: D3 Daten zur Auswertung, Archivierung / Speicherung [Internet],
- N15 CP17 Desktop / Tablet -> CP9 IT-Infrastruktur Gebäude: D9 Anfrage der Daten zum Monitoring [Internet],
- N18 CP9 IT-Infrastruktur Gebäude -> CP17 Desktop / Tablet: D5 Daten zum Monitoring [Internet],
- N20 CP11 IT-Infrastruktur Unternehmen -> CP9 IT-Infrastruktur Gebäude: D4 Daten zur Wartung [Internet]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

C7: Verschlüsselung der Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP8 ScaleIT Edge-Server,
- CP18 ScaleIT Enterprise Server

Betroffene Schutzzielklassen: CNF Confidentiality

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C8: Backup in der Cloud

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP8 ScaleIT Edge-Server,
- CP18 ScaleIT Enterprise Server

Betroffene Schutzzielklassen: AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: Angenommen, dass das Backup automatisch und häufig genug stattfindet, schützt die Maßnahme effektiv gegen Ausfälle am Edge-Server

C9: VPN

Beschützte Technologie: VPN

Betroffene Schutzzielklassen: INT Integrity, AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C12: Härtung der Komponenten

Bei Komponenten / Datenflüssen:

- CP2 Sensoren,
- CP4 Funkmodul,
- CP6 Desktop / Tablet,
- CP7 VR / AR / MR Devices,
- CP8 ScaleIT Edge-Server,
- CP9 IT-Infrastruktur Gebäude,
- CP11 IT-Infrastruktur Unternehmen,
- CP14 IT-Infrastruktur Planer,
- CP17 Desktop / Tablet,
- CP18 ScaleIT Enterprise Server

Betroffene Schutzzielklassen: INT Integrity, CNF Confidentiality, AVA Availability

Beispiele: Secure Boot, HSM zur Ablage von kryptografischem Material, Schließen von unnötigen Schnittstellen, Zugriffsschutz, ...

Benötigtes Angriffspotential: Moderate

A.5. Identifizierte Risiken

Ein Risiko besteht aus einer Bedrohung, die nach ihrem benötigten Angriffspotential, um den Angriff durchzuführen, und möglichen Schäden durch die Verletzung der betroffenen Schutzziele ausgewertet wurde. Risiken werden charakterisiert durch mögliche Vorfälle und ihre Konsequenzen und werden gemäß des benötigten Angriffspotentials und des Schadenspotentials bewertet.

Die aufgelisteten Risiken beginnen mit der ID, gefolgt von dem Namen für die entsprechende Bedrohung. Falls anwendbar, werden vorbereitende Angriffe angegeben. Diese sollten als Bedrohungen angesehen werden, die zuvor realisiert werden müssen. Normalerweise werden vorbereitende Angriffe benutzt, um bestehende Maßnahmen in ihrer Wirkung zu hindern. Durch diese Verknüpfung ist die Modellierung komplexer Angriffe möglich.

Nach dem erläuternden Kommentar zeigt eine Tabelle die bewerteten Risiken. Die einzelnen Szenarien unterscheiden sich durch die berücksichtigten Maßnahmengruppen.

R1: Manipulation als MitM auf Bluetooth beim Pairing

Bluetooth-Verbindungen können aufgrund fehlender Verifikationsmöglichkeiten, wie z. B. einem Zahlenfolgenvergleich o. ä., während des Pairings leicht angegriffen werden. Hier besteht ein sehr hohes Risiko, dass Angreifer sich während des Pairings als MitM etablieren können.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL		Very High

R2: Manipulation als MitM auf Bluetooth zwischen Sensoren und Funkmodul oder Spoofen einer der beiden Kommunikationsteilnehmer

Angriffe auf eine bestehende Bluetooth-Verbindung sind verhältnismäßig schwierig. Aufgrund des hohen möglichen Schadens besteht dennoch ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C3 Bluetooth-Sicherheit	Moderate
ALL	C3 Bluetooth-Sicherheit	Moderate

R3: Abhören der Bluetooth-Übertragung

Angriffe auf eine bestehende Bluetooth-Verbindung sind verhältnismäßig schwierig. Das Abhören der Daten stellt nur einen geringen Schaden dar, was in einem geringen Risiko resultiert.

Gruppen	Maßnahmen	Risiko
Basis	C3 Bluetooth-Sicherheit	Low
ALL	C3 Bluetooth-Sicherheit	Low

R4: Unterbrechen der Bluetooth-Übertragung

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R5: Manipulation als MitM auf LAN innerhalb des Gebäudes

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R6: Abhören der LAN-Verbindung innerhalb des Gebäudes

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Low

R7: Unterbrechen der LAN-Verbindung innerhalb des Gebäudes

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R8: Manipulation als MitM auf WLAN innerhalb des Gebäudes

Aufgrund der zusätzlichen WPA2-Enterprise Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C2 TLS, C10 HTTP Auth Token basiert	Moderate

R9: Abhören der WLAN-Verbindung innerhalb des Gebäudes

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise Verbindungsverschlüsselung schwer und resultiert somit in einem geringen Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Low
ALL	C1 WPA2-Enterprise, C2 TLS	Low

R10: Unterbrechen der WLAN-Verbindung innerhalb des Gebäudes

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R11: Manipulation als MitM auf LAN innerhalb des Unternehmens

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R12: Abhören der LAN-Verbindung innerhalb des Unternehmens

Da die Verbindungen innerhalb des Unternehmens unverschlüsselt sind, besteht ein moderates Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS weiter reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Moderate
ALL	C2 TLS	Low

R13: Unterbrechen der LAN-Verbindung innerhalb des Unternehmens

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R14: Manipulation als MitM auf LAN beim Planer

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R15: Abhören der LAN-Verbindung beim Planer

Da die Verbindungen beim Planer unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Low

R16: Unterbrechen der LAN-Verbindung beim Planer

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R17: Manipulation als MitM im Internet

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C4 Firewall, C10 HTTP Auth Token basiert	High
ALL	C2 TLS, C4 Firewall, C10 HTTP Auth Token basiert	Moderate

R18: Abhören der Internet-Verbindung

Da die Verbindungen über das Internet unverschlüsselt sind, besteht ein Risiko, dass Verbindungen dort abgehört werden können. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Moderate
ALL	C2 TLS	Low

R19: Unterbrechen der Internetverbindung bzw. Denial of Service eines Endpunktes

Unterbrechungen von Verbindungen sind hier leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R20: Angriffe auf die Sensoren im Isoshade-Element

Da die Sensoren im Isoshade-Element über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R21: Angriffe auf die IT-Infrastruktur im Gebäude

Da die IT-Infrastruktur über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R22: Angriffe auf die IT-Infrastruktur im Unternehmen

Da die IT-Infrastruktur über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R23: Kompromittieren eines Scale-IT Edge Servers

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C12 Härtung der Komponenten	High

R24: Auslesen von gespeicherten Daten aus einem Scale-IT Edge Server

Die Vertraulichkeit der Daten auf dem Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung von SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container, C12 Härtung der Komponenten	Moderate

R25: Unterbrechen der Verfügbarkeit eines Scale-IT Edge Servers

Die Verfügbarkeit des Scale-IT Edge Servers ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein moderates Risiko.

Durch die Verwendung von Backups in die Cloud lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	Moderate
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud, C12 Härtung der Komponenten	Low

R26: Kompromittieren eines Scale-IT Enterprise Servers

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Härtung der verwendeten Komponenten sowie die Verschlüsselung der Container lässt sich dieses Risiko weiter reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container, C8 Backup in der Cloud, C12 Härtung der Komponenten	Moderate

R27: Auslesen von gespeicherten Daten aus einem Scale-IT Enterprise Server

Die Vertraulichkeit der Daten auf dem Scale-IT Enterprise Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung von SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container, C12 Härtung der Komponenten	Moderate

R28: Unterbrechen der Verfügbarkeit eines Scale-IT Enterprise Servers

Die Verfügbarkeit des Scale-IT Enterprise Servers ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein moderates Risiko. Durch die Verwendung von Backups in die Cloud lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	Moderate
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud, C12 Härtung der Komponenten	Low

R29: Angriffe auf die IT-Infrastruktur des Planers

Da die IT-Infrastruktur über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R30: Zutritt ins Gebäude erlangen als Angriffsvorbereitung

Nur Angriffsvorbereitung.

Gruppen	Maßnahmen	Risiko
Basis		Low
ALL		Low

R31: Manipulation als MitM auf 5G innerhalb des Gebäudes

Angriffe auf eine bestehende 5G-Verbindung sind moderat schwierig. Aufgrund des hohen möglichen Schadens besteht ein hohes Risiko. Durch die Verwendung von TLS kann dieses auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert, C11 5G-Sicherheit	High
ALL	C2 TLS, C10 HTTP Auth Token basiert, C11 5G-Sicherheit	Moderate

R32: Abhören der 5G-Verbindung innerhalb des Gebäudes

Das Abhören von 5G-Verbindungen ist aufgrund der Verbindungsverschlüsselung schwer und trägt somit nur ein geringes Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C11 5G-Sicherheit	Low
ALL	C2 TLS, C11 5G-Sicherheit	Low

R33: Unterbrechen der 5G-Verbindung innerhalb des Gebäudes

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R34: Manipulation als MitM auf WLAN zwischen Sensoren und Funkmodul oder Spoofen einer der beiden Kommunikationsteilnehmer

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise	Moderate

R35: Abhören der WLAN-Übertragung zwischen Sensoren und Funkmodul

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise Verbindungsverschlüsselung schwer und trägt somit nur ein geringes Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Low
ALL	C1 WPA2-Enterprise	Low

R36: Unterbrechen der WLAN-Übertragung zwischen Sensoren und Funkmodul

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

A.6. Risikoübersicht

	Basis	ALL
Low	5	11
Moderate	7	11
High	14	13
Very High	10	1

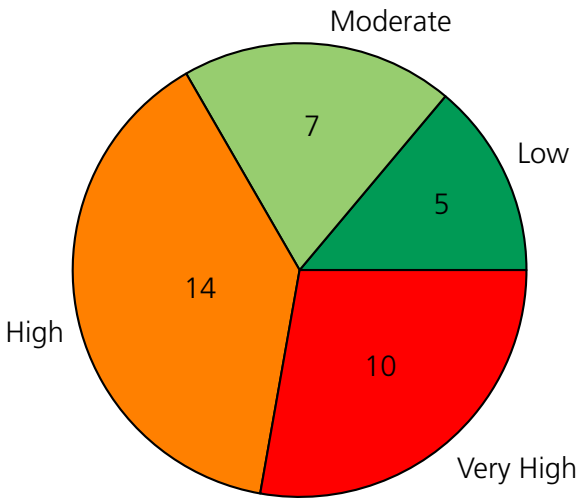

Abbildung A.2.: Control Groups: Basis

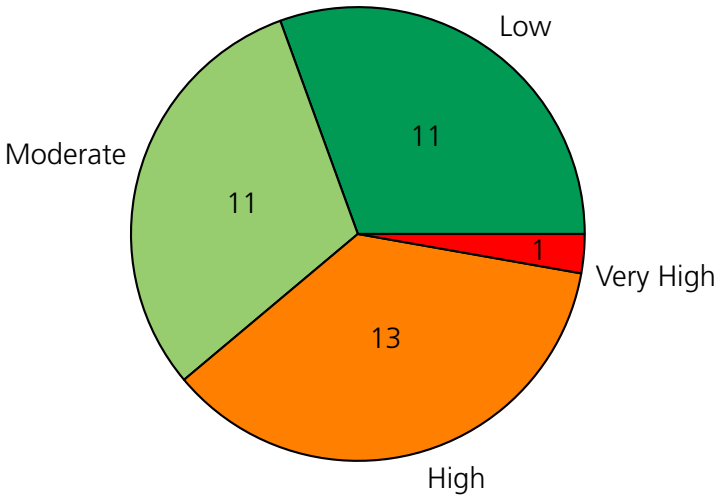

Abbildung A.3.: Control Groups: ALL

B. Schweißprüfung

B.1. Komponenten

Nachfolgend werden alle in der Analyse berücksichtigten Komponenten aufgelistet. Dieser Teil dient als Referenz für die spätere Zuordnung von Maßnahmen zu Komponenten.

Tabelle B.1.: IDs und Namen der Komponenten.

ID	Name
CP1	Datenemitter / -konsument
CP2	Softwareanwendung
CP3	Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner)
CP4	RFID-Tag / QR-Code / Tagging / ID-Lösung
CP6	IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen)
CP7	Desktop / Tablet
CP8	VR / AR / MR Devices
CP9	ScaleIT Edge Server
CP10	IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen)
CP11	ScaleIT Cloud Cluster
CP12	VR / AR / MR Devices
CP13	Desktop / Tablet
CP14	Endgeräte in Bereich 1
CP15	Endgeräte im Bereich 2

Die Komponenten kommunizieren untereinander wie in Abbildung B.1 skizziert.

Abbildung B.1.: Systemarchitektur Use Case 2.

B.2. Datenflüsse

Im Detail werden die folgenden Kommunikationspfade und Technologien berücksichtigt:

Tabelle B.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N1	Die Softwareanwendung sendet D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten zum Endgeräte in Bereich 1 unter Benutzung von WLAN.
N2	Die Endgeräte in Bereich 1 senden D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) und D10 Video-Streamingdaten zum ScaleIT Edge Server unter Benutzung von WLAN.
N3	Die Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) sendet D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro zum ScaleIT Edge Server unter Benutzung von WLAN.
N4	Der RFID-Tag / QR-Code / Tagging / ID-Lösung sendet D3 Daten zum Lokalisierungsstatus, Produktinformationen zum Endgeräte in Bereich 1.
N5	Das Endgeräte in Bereich 1 sendet D3 Daten zum Lokalisierungsstatus, Produktinformationen zum ScaleIT Edge Server unter Benutzung von WLAN.
N6	Der Datenemitter / -konsument sendet D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen und D10 Video-Streamingdaten zum ScaleIT Edge Server unter Benutzung von LAN.
N7	Der Datenemitter / -konsument sendet D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen und D10 Video-Streamingdaten zum ScaleIT Edge Server unter Benutzung von WLAN.
N8	Der ScaleIT Edge Server sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von LAN.

Tabelle B.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N9	Die Endgeräte in Bereich 1 senden D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) und D10 Video-Streamingdaten zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N10	Der ScaleIT Edge Server sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von LAN.
N11	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von Internet.
N12	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N13	Das Endgeräte in Bereich 1 sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N14	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von Internet.
N15	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D4 Daten für eine langfristige Speicherung und den Abruf von Daten zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N16	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D8 Synchronisationsdaten zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von Internet.
N17	Der ScaleIT Cloud Cluster sendet D9 Synchronisation Planungsdaten zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von LAN.
N18	Die Endgeräte im Bereich 2 senden D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von WLAN und LAN.

B.3. Schutzziele

Im Folgenden wird der Schutzbedarf aufgezeigt. Für jedes Schutzziel der betrachteten Funktionen wird die maximale Schadenshöhe und die möglichen Schäden in Schadenskategorien geordnet aufgelistet. Die Schutzziele der Daten und Komponenten unterscheiden sich kaum von denen der Funktionen und werden deshalb zur besseren Übersichtlichkeit nicht extra aufgelistet.

CNF.F1: Vertraulichkeit der Nutzung von Schweißdaten (Checklisten, Protokolle) durch den Schweißer

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Know-how

AVA.F1: Verfügbarkeit der Nutzung von Schweißdaten (Checklisten, Protokolle) durch den Schweißer

Schadenshöhe: Low

- Quality: Production delay (QPD)

Erklärung:
QPD: Verzögerung der Produktion durch fehlende Schweißdaten

INT.F1: Integrität der Nutzung von Schweißdaten (Checklisten, Protokolle) durch den Schweißer

Schadenshöhe: High

- Financial: Small damages to building (FSD)
- Quality: Production stop (QPS)

Erklärung:
FSD: Fehlerhafte Schweißnähte, nur kleine Schäden, da größere vermutlich dem Prüfer auffallen
QPS: Produktionsstop wegen falscher/fehlender Schweißdaten

CNF.F2: Vertraulichkeit der Nutzung von Schweißdaten (Checklisten, Protokolle) durch das Unternehmen

Schadenshöhe: Very Low

- Financial: Very low financial damage

AVA.F2: Verfügbarkeit der Nutzung von Schweißdaten (Checklisten, Protokolle) durch das Unternehmen

Schadenshöhe: Low

- Quality: Production delay

INT.F2: Integrität der Nutzung von Schweißdaten (Checklisten, Protokolle) durch das Unternehmen

Schadenshöhe: High

- Financial: Small damages to building (FSD)
- Quality: Production stop (QPS)

Erklärung:
FSD: Fehlerhafte Schweißnähte, Prüfer erhält falsche Daten und kann den Fehler im schlimmsten Fall nicht ermitteln
QPS: Produktionsstop wegen falscher/fehlender Schweißdaten

CNF.F3: Vertraulichkeit der Nutzung von Fertigungsdaten durch den Planer/Konstrukteur

Schadenshöhe: High

- Financial: High financial damage (FHI)

Erklärung:
FHI: Know-how-Abfluss

AVA.F3: Verfügbarkeit der Nutzung von Fertigungsdaten durch den Planer/Konstrukteur

Schadenshöhe: Low

- Quality: Production delay

INT.F3: Integrität der Nutzung von Fertigungsdaten durch den Planer/Konstrukteur

Schadenshöhe: High

- Financial: Severe damages to building (FHD)
- Safety: Severe injury (survival probable)
- Quality: Production stop (QPS)

Erklärung:
FHD: Fehlerhafte Schweißnähte, dem Prüfer werden jedoch geschönte Daten gesendet
QPS: Produktionsstop wegen katastrophalen Daten, die dem Prüfer gesendet werden

AVA.F4: Verfügbarkeit der Nutzung von Lokalisierungsdaten durch die IT

Schadenshöhe: Low

- Quality: Production delay (QPD)

Erklärung:
QPD: Teile müssen aufwändig gesucht werden

INT.F4: Integrität der Nutzung von Lokalisierungsdaten durch die IT

Schadenshöhe: High

- Financial: Severe damages to building (FHD)
- Quality: Production delay (QPD)

Erklärung:
FHD: Nutzung falscher Teile, ohne dass es auffällt
QPD: Geerbt

CNF.F5: Vertraulichkeit der Nutzung von Fertigungsdaten durch das Unternehmen

Schadenshöhe: High

- Financial: High financial damage (FHI)

Erklärung:
FHI: Know-how

AVA.F5: Verfügbarkeit der Nutzung von Fertigungsdaten durch das Unternehmen

Schadenshöhe: Low

- Quality: Production delay

INT.F5: Integrität der Nutzung von Fertigungsdaten durch das Unternehmen

Schadenshöhe: Very High

- Financial: Severe damages to building (FHD)
- Safety: Life-threatening injury
- Quality: Production stop (QPS)

Erklärung:
FHD: Fehlerhafte Schweißnähte, dem Prüfer werden jedoch geschönte Daten gesendet
QPS: Produktionsstop wegen katastrophalen Daten, die dem Prüfer gesendet werden

B.4. Maßnahmen

Maßnahmen beschreiben die (technische) Implementierung von Sicherheitsanforderungen, um Risiken zu verringern. Im Folgenden werden die Maßnahmen gemäß ihrer Zuordnung zu den Gruppen aufgelistet. Jede einzelne Maßnahme ist als Kombination aus ID und Name aufgeführt. Falls vorhanden, werden die beschützten Technologien, geschützte Archtiketurelemente und die Schutzzielklasse gefolgt von einer Beschreibung angegeben.

Verfügbare Maßnahmen sind wie folgt gruppiert:

- Basis: Basis-Maßnahmen
- Erweitert: Zusätzlich vorgeschlagene Maßnahmen, um Restrisiken zu reduzieren

B.4.1. Basis-Maßnahmen

C1: WPA2-Enterprise

Beschützte Technologie: WLAN

Bei Komponenten / Datenflüssen:

- N1 CP2 Softwareanwendung -> CP14 Endgeräte in Bereich 1: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N2 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro [WLAN],
- N5 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],
- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen, D10 Video-Streamingdaten [WLAN],
- N9 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],

- N13 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [WLAN],
- N18 CP15 Endgeräte im Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) [WLAN, LAN]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

Bemerkung: Wenn darauf geachtet wird, dass ein sicheres Passwort verwendet wird, wird WPA2-Enterprise als sichere SotA-Maßnahme gesehen.

C4: Firewall

Beschützte Technologie: Internet

Bei Komponenten / Datenflüssen:

- N11 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N14 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D8 Synchronisationsdaten [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential: Basic

Bemerkung: Keine Einschätzung möglich, da keine Angaben über die Konfiguration der Firewall gemacht wurden.

C5: Virtualisierung durch Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: High

C6: Zugriffsschutz für ScaleIT / Username + Passwort

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: Enhanced-Basic

C10: HTTP Auth Token basiert

Beschützte Technologie: WLAN, LAN, Internet

Bei Komponenten / Datenflüssen:

- N1 CP2 Softwareanwendung -> CP14 Endgeräte in Bereich 1: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N2 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro [WLAN],
- N5 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],
- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen, D10 Video-Streamingdaten [WLAN],
- N9 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N13 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [WLAN],
- N18 CP15 Endgeräte im Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) [WLAN, LAN],

- N6 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen, D10 Video-Streamingdaten [LAN],
- N8 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N10 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N12 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N15 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N17 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D9 Synchronisation Planungsdaten [LAN],
- N11 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N14 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D8 Synchronisationsdaten [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential: Enhanced-Basic

B.4.2. Erweiterte Maßnahmen

C2: TLS

Beschützte Technologie: LAN, WLAN, Internet

Bei Komponenten / Datenflüssen:

- N6 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen, D10 Video-Streamingdaten [LAN],
- N8 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N10 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N12 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N15 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D4 Daten für eine langfristige Speicherung und den Abruf von Daten [LAN],
- N17 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D9 Synchronisation Planungsdaten [LAN],
- N18 CP15 Endgeräte im Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien) [WLAN, LAN],
- N1 CP2 Softwareanwendung -> CP14 Endgeräte in Bereich 1: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N2 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro [WLAN],
- N5 CP14 Endgeräte in Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],
- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und der Planung im Büro, D3 Daten zum Lokalisierungsstatus, Produktinformationen, D10 Video-Streamingdaten [WLAN],

- N9 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D1 Daten für Schweißprüfung (Protokolle, Checklisten, 3D-Informationen / -dateien), D10 Video-Streamingdaten [WLAN],
- N13 CP14 Endgeräte in Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [WLAN],
- N11 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N14 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D4 Daten für eine langfristige Speicherung und den Abruf von Daten [Internet],
- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D8 Synchronisationsdaten [Internet]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

C7: Verschlüsselung der Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C8: Backup in der Cloud

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: Angenommen, dass das Backup automatisch und häufig genug stattfindet, schützt die Maßnahme effektiv gegen Ausfälle am Edge-Server

C9: VPN

Beschützte Technologie: VPN

Betroffene Schutzzielklassen: INT Integrity, AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C12: Härtung der Komponenten

Bei Komponenten / Datenflüssen:

- CP1 Datenemitter / -konsument,
- CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen),
- CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen),
- CP14 Endgeräte in Bereich 1,
- CP15 Endgeräte im Bereich 2

Betroffene Schutzzielklassen: INT Integrity, CNF Confidentiality, AVA Availability

Beispiele: Secure Boot, HSM zur Ablage von kryptografischem Material, Schließen von unnötigen Schnittstellen, Zugriffsschutz, . . .

Benötigtes Angriffspotential: Moderate

B.5. Identifizierte Risiken

Ein Risiko besteht aus einer Bedrohung, die nach ihrem benötigten Angriffspotential, um den Angriff durchzuführen, und möglichen Schäden durch die Verletzung der betroffenen Schutzziele ausgewertet wurde. Risiken werden charakterisiert durch mögliche Vorfälle und ihre Konsequenzen und werden gemäß des benötigten Angriffspotentials und des Schadenspotentials bewertet.

Die aufgelisteten Risiken beginnen mit der ID, gefolgt von dem Namen für die entsprechende Bedrohung. Falls anwendbar, werden vorbereitende Angriffe angegeben. Diese sollten als Bedrohungen angesehen werden, die zuvor realisiert werden müssen. Normalerweise werden vorbereitende Angriffe benutzt, um bestehende Maßnahmen in ihrer Wirkung zu hindern. Durch diese Verknüpfung ist die Modellierung komplexer Angriffe möglich.

Nach dem erläuternden Kommentar zeigt eine Tabelle die bewerteten Risiken. Die einzelnen Szenarien unterscheiden sich durch die berücksichtigten Maßnahmengruppen.

R1: Manipulation als MitM auf der WLAN-Kommunikation zwischen Datenemittern und IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate

R2: Abhören der WLAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise	Moderate

R3: Unterbrechen der WLAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R4: Manipulation als MitM auf der WLAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate

R5: Abhören der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise	Moderate

R6: Unterbrechen der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL		Very High

R7: Manipulation als MitM auf der WLAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 2 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate

R8: Abhören der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise	Moderate

R9: Unterbrechen der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R10: Angriffe auf das Auslesen der RFID-Tags/ der QR-Codes

Hierfür wäre eine Manipulation der Übertragungsstrecke, also zwischen RFID-Tag und Lesegerät, notwendig. Diese erscheint nicht realistisch.

Gruppen	Maßnahmen	Risiko
Basis		Moderate
ALL		Moderate

R11: Manipulation als MitM auf der LAN-Kommunikation zwischen Datenemittern und IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R12: Abhören der LAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Moderate

R13: Unterbrechen der LAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R14: Manipulation als MitM auf der LAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R15: Abhören der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Moderate

R16: Unterbrechen der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL		Very High

R17: Manipulation als MitM auf der LAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 2 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur sehr begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R18: Abhören der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier könnte das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Moderate

R19: Unterbrechen der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL		Very High

R20: Manipulation als MitM im Internet oder Spoofen eines Endpunktes

Die HTTP Auth Tokens schützen nur begrenzt vor einem MitM-Angriff. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C4 Firewall, C10 HTTP Auth Token basiert	High
ALL	C2 TLS, C4 Firewall, C10 HTTP Auth Token basiert	Moderate

R21: Abhören der Internet Verbindung

Da die Verbindungen über das Internet unverschlüsselt sind, besteht ein Risiko, dass Verbindungen dort abgehört werden können. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL	C2 TLS	Moderate

R22: Unterbrechen der Internetverbindung bzw. Denial of Service eines Endpunktes

Unterbrechungen von Verbindungen sind hier leicht zu erreichen.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL		Very High

R23: Angriffe auf die Datenemitter

Da die Datenemitter über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	Very High

R24: Angriffe auf die IT-Infrastruktur Bereich 1 (ScaleIT ausgeschlossen)

Da die IT-Infrastruktur im Bereich 1 über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	Very High

R25: Angriffe auf die IT-Infrastruktur Bereich 2 (ScaleIT ausgeschlossen)

Während die IT-Infrastruktur im Bereich 2 über keine Schutzmechanismen verfügt, werden hier auch keine kritischen Daten verarbeitet.

Gruppen	Maßnahmen	Risiko
Basis		Low
ALL	C12 Härtung der Komponenten	Low

R26: Kompromittieren eines ScaleIT Edge Servers im Bereich 1

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High

R27: Auslesen von gespeicherten Daten aus einem ScaleIT Edge Server im Bereich 1

Die Vertraulichkeit der Daten auf dem Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung vom SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container	Moderate

R28: Unterbrechen der Verfügbarkeit eines ScaleIT Edge Servers im Bereich 1

Die Verfügbarkeit des Scale-IT Edge Servers ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein moderates Risiko. Durch die Verwendung von Backups in die Cloud lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud	Moderate

R29: Kompromittieren eines ScaleIT Cloud Clusters im Bereich 2

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High

R30: Auslesen von gespeicherten Daten aus einem ScaleIT Cloud Cluster im Bereich 2

Die Vertraulichkeit der Daten auf dem Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung von SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container	Moderate

R31: Unterbrechen der Verfügbarkeit eines ScaleIT Cloud Clusters im Bereich 2

Die Verfügbarkeit des Scale-IT Edge Servers ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein moderates Risiko. Durch die Verwendung von Backups in die Cloud lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud	Moderate

B.6. Risikoübersicht

	Basis	ALL
Low	1	1
Moderate	7	19
High	11	5
Very High	12	6

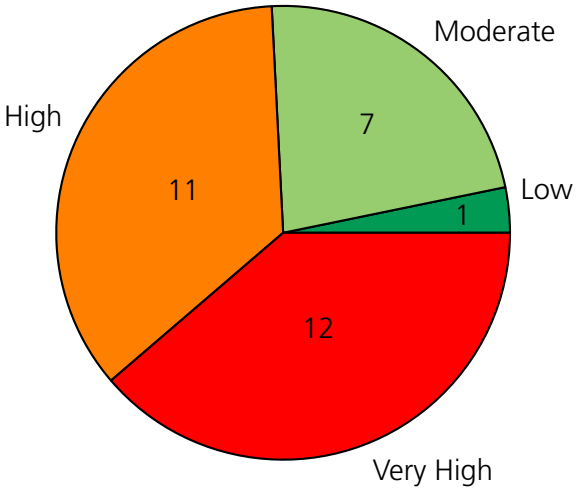

Abbildung B.2.: Control Groups: Basis

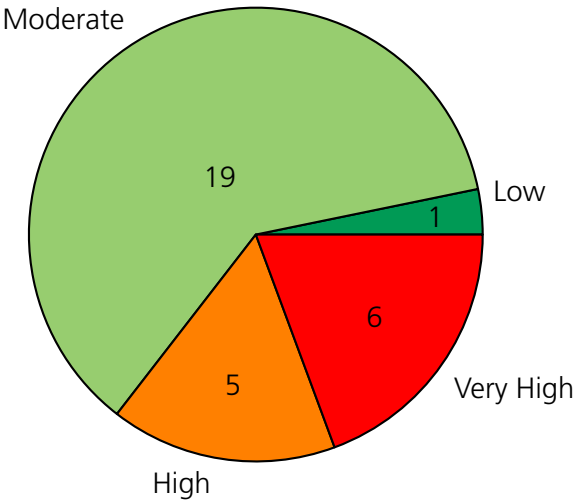

Abbildung B.3.: Control Groups: ALL

C. Virtuelle Montageunterstützung

C.1. Komponenten

Nachfolgend werden alle in der Analyse berücksichtigten Komponenten aufgelistet. Dieser Teil dient als Referenz für die spätere Zuordnung von Maßnahmen zu Komponenten.

Tabelle C.1.: IDs und Namen der Komponenten.

ID	Name
CP1	Datenemitter / -konsument
CP2	Softwareanwendung
CP3	Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner)
CP4	RFID-Tag / QR- Code / Tagging / ID-Lösung
CP5	Funkmodul
CP6	IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen)
CP7	Desktop / Tablet
CP8	VR / AR / MR Devices
CP9	ScaleIT Edge Server
CP10	IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen)
CP11	ScaleIT Cloud Cluster
CP12	VR / AR / MR Devices
CP13	Desktop / Tablet
CP14	IT-Infrastruktur Öffentliches Netz
CP15	ScaleIT Cloud Cluster
CP16	VR / AR / MR Devices
CP17	Desktop / Tablet
CP18	Endgeräte Bereich 1
CP19	Endgeräte Bereich 2

Tabelle C.1.: IDs und Namen der Komponenten.

ID	Name
CP20	Endgeräte Öffentlich

Die Komponenten kommunizieren untereinander wie in Abbildung C.1 skizziert.

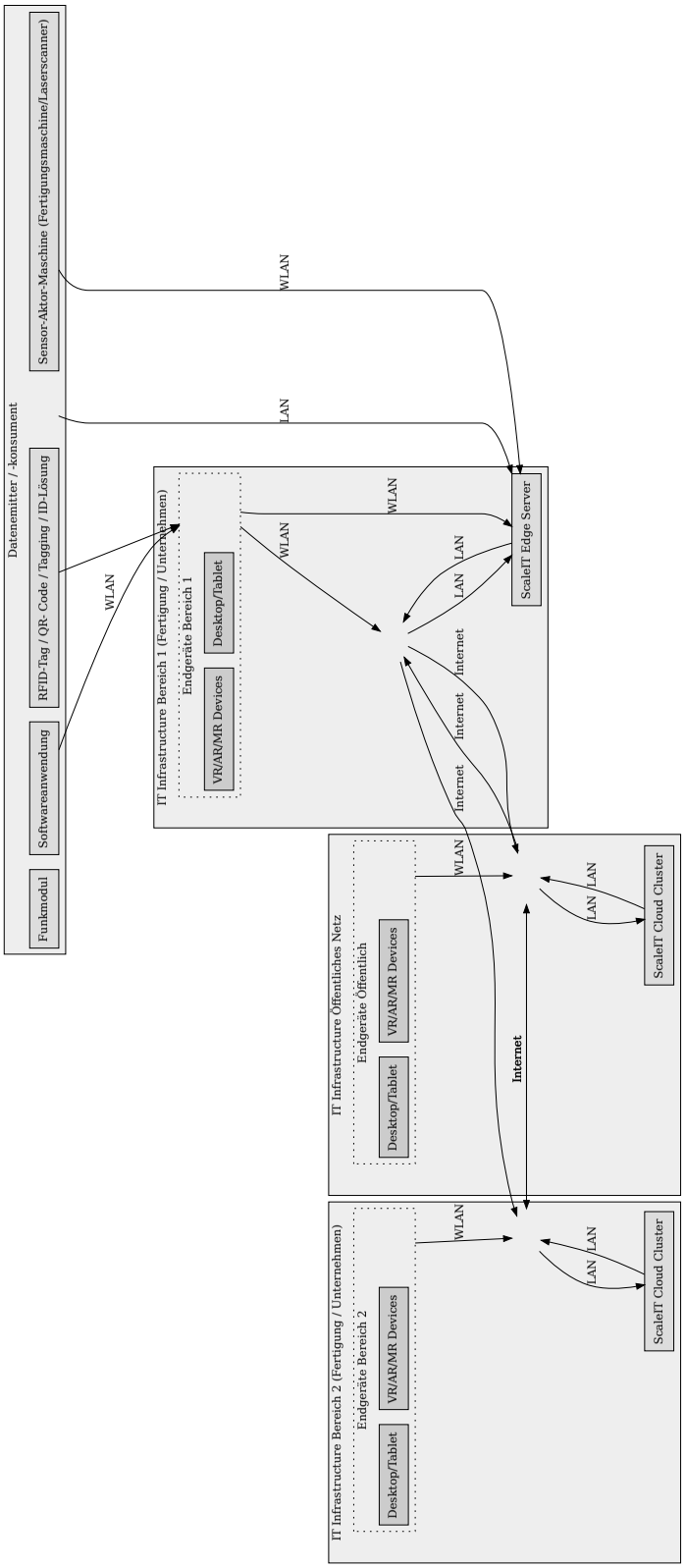

Abbildung C.1.: Systemarchitektur Use Case 3.

C.2. Datenflüsse

Im Detail werden die folgenden Kommunikationspfade und Technologien berücksichtigt:

Tabelle C.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N1	Die Softwareanwendung sendet D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten zum Endgeräte Bereich 1 unter Benutzung von WLAN.
N2	Die Endgeräte Bereich 1 senden D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten zum ScaleIT Edge Server unter Benutzung von WLAN.
N3	Die Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) sendet D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle zum ScaleIT Edge Server unter Benutzung von WLAN.
N5	Die RFID-Tag / QR- Code / Tagging / ID-Lösung sendet D3 Daten zum Lokalisierungsstatus, Produktinformationen zum Endgeräte Bereich 1.
N6	Die Endgeräte Bereich 1 senden D3 Daten zum Lokalisierungsstatus, Produktinformationen zum ScaleIT Edge Server unter Benutzung von WLAN.
N7	Der Datenemitter / -konsument sendet D4 aufbereitete Daten konsumieren (intern): D1, D2 und D3 zum ScaleIT Edge Server unter Benutzung von WLAN.
N8	Der Datenemitter / -konsument sendet D5 Aufbereitete Fertigungsdaten für extern: Ausgewählte Daten aus D1, D2 und D3 zum ScaleIT Edge Server unter Benutzung von LAN.
N10	Der ScaleIT Edge Server sendet D6 Sammlung von internen Daten zur kurzfristigen Speicherung (bis zum Zeitpunkt einer Synchronisation) für Auswertungen und zur Weitergabe an externe Gewerke für deren Auswertungen zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von LAN.
N11	Die Endgeräte Bereich 1 senden D7 Daten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von WLAN.

Tabelle C.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N12	Der ScaleIT Edge Server sendet D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle und D3 Daten zum Lokalisierungsstatus, Produktinformationen zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von LAN.
N13	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle und D3 Daten zum Lokalisierungsstatus, Produktinformationen zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.
N14	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle und D3 Daten zum Lokalisierungsstatus,Produktinformationen zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N15	Die Endgeräte Bereich 1 senden D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N16	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.
N17	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N18	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D10 Synchronisation für die langfristige Speicherung der Baustellendaten zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.
N19	Der ScaleIT Cloud Cluster sendet D11 Synchronisation für die langfristige Speicherung der Daten vom Fertiger zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von LAN.

Tabelle C.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N20	Die Endgeräte Bereich 2 senden D12 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N21	Der ScaleIT Edge Server sendet D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von LAN.
N22	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden zur IT-Infrastruktur Öffentliches Netz unter Benutzung des Internets.
N23	Die IT-Infrastruktur Öffentliches Netz sendet D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N24	Die Endgeräte Bereich 1 senden D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zum IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N25	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zur IT-Infrastruktur Öffentliches Netz unter Benutzung des Internets.
N26	Die IT-Infrastruktur Öffentliches Netz sendet D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N27	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D15 Weitergabe Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zur Auswertung und langfristigen Speicherung zur IT-Infrastruktur Öffentliches Netz unter Benutzung des Internets.
N28	Die IT-Infrastruktur Öffentliches Netz sendet D15 Weitergabe Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zur Auswertung und langfristigen Speicherung zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.
N29	Der ScaleIT Cloud Cluster sendet D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von LAN.

Tabelle C.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N30	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk zur IT-Infrastruktur Öffentliches Netz unter Benutzung de Internets.
N31	Die IT-Infrastruktur Öffentliches Netz sendet D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung des Internets.
N32	Die Endgeräte Bereich 2 senden D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung von WLAN.
N33	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle zur IT-Infrastruktur Öffentliches Netz unter Benutzung des Internets.
N34	Die IT-Infrastruktur Öffentliches Netz sendet D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung des Internets.
N35	Der ScaleIT Cloud Cluster sendet D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger zur IT-Infrastruktur Öffentliches Netz unter Benutzung von LAN.
N36	Die IT-Infrastruktur Öffentliches Netz sendet D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger zur IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.
N37	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N38	Die Endgeräte Öffentlich senden D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) zur IT-Infrastruktur Öffentliches Netz unter Benutzung von WLAN.
N39	Die IT-Infrastruktur Öffentliches Netz sendet D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) to the IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) unter Benutzung des Internets.

Tabelle C.2.: IDs und Beschreibung der Datenflüsse.

ID	Beschreibung
N40	Die IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) sendet D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) zum ScaleIT Cloud Cluster unter Benutzung von LAN.
N41	Der ScaleIT Cloud Cluster sendet D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle zur IT-Infrastruktur Öffentliches Netz unter Benutzung von LAN.
N42	Die IT-Infrastruktur Öffentliches Netz sendet D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle zur IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) unter Benutzung des Internets.
N43	Die IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) sendet D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle zum ScaleIT Edge Server unter Benutzung von LAN.

C.3. Schutzziele

Im Folgenden wird der Schutzbedarf aufgezeigt. Für jedes Schutzziel der betrachteten Funktionen wird die maximale Schadenshöhe und die möglichen Schäden in Schadenskategorien geordnet aufgelistet. Die Schutzziele der Daten und Komponenten unterscheiden sich kaum von denen der Funktionen und werden deshalb zur besseren Übersichtlichkeit nicht extra aufgelistet.

CNF.F1: Vertraulichkeit der Nutzung von Baustellendaten für den Baustellenbetreiber

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Firmen-Know-how

AVA.F1: Verfügbarkeit der Nutzung von Baustellendaten für den Baustellenbetreiber

Schadenshöhe: Low

- Quality: Production delay (QPD)

Erklärung:
QPD: Verzögerungen auf der Baustelle durch fehlende Baustellendaten

INT.F1: Integrität der Nutzung von Baustellendaten für den Baustellenbetreiber

Schadenshöhe: Moderate

- Financial: Small damages to building (FSD)
- Safety: Potentially dangerous situation (SPD)

Erklärung:
FSD: Übertragung falscher Montageinstruktionen könnte zu Beschädigung von Bauteilen führen
SPD: Falsche Informationen zu sicherheitskritischen Baustellenbereichen

CNF.F2: Vertraulichkeit der Nutzung von Fertigungs- und Planungsdaten für den Baustellenbetreiber

Schadenshöhe: High

- Financial: High financial damage (FHI)

Erklärung:
FHI: Know-how

AVA.F2: Verfügbarkeit der Nutzung von Fertigungs- und Planungsdaten für den Baustellenbetreiber

Schadenshöhe: Low

- Quality: Production delay

INT.F2: Integrität der Nutzung von Fertigungs- und Planungsdaten für den Baustellenbetreiber

Schadenshöhe: Moderate

- Financial: Small damages to building

AVA.F3: Verfügbarkeit der Nutzung von Lokalisierungsdaten für den Baustellenbetreiber

Schadenshöhe: Low

- Quality: Production delay

INT.F3: Integrität der Nutzung von Lokalisierungsdaten für den Baustellenbetreiber

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Einbau der Bauteile am falschen Verbauort. Keine Nachverfolgung von fehlerhaften Teilen möglich.

CNF.F4: Vertraulichkeit der Nutzung von Baustellendaten für den Fertiger

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Firmen-Know-how

AVA.F4: Verfügbarkeit der Nutzung von Baustellendaten für den Fertiger

Schadenshöhe: Low

- Quality: Production delay

INT.F4: Integrität der Nutzung von Baustellendaten für den Fertiger

Schadenshöhe: Moderate

- Financial: Small damages to building (FSD)
- Safety: Potentially dangerous situation (SPD)

Erklärung:
FSD & SPD: Qualitätsprüfungen von montierten Bauteilen könnte fehlerhaft abgeschlossen werden

CNF.F5: Vertraulichkeit der Nutzung von Fertigungs- und Planungsdaten für den Fertiger

Schadenshöhe: High

- Financial: High financial damage

AVA.F5: Verfügbarkeit der Nutzung von Fertigungs- und Planungsdaten für den Fertiger

Schadenshöhe: Low

- Quality: Production delay

INT.F5: Integrität der Nutzung von Fertigungs- und Planungsdaten für den Fertiger

Schadenshöhe: High

- Financial: Severe damages to building (FHD)
- Safety: Potentially dangerous situation (SPD)
- Quality: Production delay

Erklärung:
FHD: Nutzung von z. B. falschen Schweißnähten. Die Qualitätsprüfung erhält jedoch geschönte Daten.
SPD: Bauteile sind trotz QS-Prüfung fehlerhaft montiert.

AVA.F6: Verfügbarkeit der Nutzung von Lokalisierungsdaten für den Fertiger

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Verzögerung bei Abgleich SOLL/IST

INT.F6: Integrität der Nutzung von Lokalisierungsdaten für den Fertiger

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Fehler bei Abgleich SOLL/IST anhand falscher Daten

CNF.F7: Vertraulichkeit der Nutzung von Baustellendaten für den Kunden

Schadenshöhe: Very Low

- Financial: Very low financial damage

CNF.F8: Vertraulichkeit der Nutzung von Fertigungs- und Planungsdaten für den Kunden

Schadenshöhe: High

- Financial: High financial damage (FHI)

Erklärung:
FHI: Know-how

AVA.F8: Verfügbarkeit der Nutzung von Fertigungs- und Planungsdaten für den Kunden

Schadenshöhe: Very Low

- Financial: Very low financial damage (FVL)

Erklärung:
FVL: Möglicherweise Terminplanverschiebung

INT.F8: Integrität der Nutzung von Fertigungs- und Planungsdaten für den Kunden

Schadenshöhe: Very Low

- Financial: Very low financial damage

AVA.F9: Verfügbarkeit der Nutzung von Lokalisierungsdaten für den Kunden

Schadenshöhe: Very Low

- Quality: Comfort function affected

Erklärung:
No damages

C.4. Maßnahmen

Maßnahmen beschreiben die (technische) Implementierung von Sicherheitsanforderungen, um Risiken zu verringern. Im Folgenden werden die Maßnahmen gemäß ihrer Zuordnung zu den Gruppen aufgelistet. Jede einzelne Maßnahmen ist als Kombination aus ID und Name aufgeführt. Falls vorhanden, werden die beschützten Technologien, geschützte Archtiketurelemente und die Schutzzielklasse gefolgt von einer Beschreibung angegeben.

Verfügbare Maßnahmen sind wie folgt gruppiert:

- Basis: Basis-Maßnahmen
- Erweitert: Zusätzlich vorgeschlagene Maßnahmen, um Restrisiken zu reduzieren

C.4.1. Basis-Maßnahmen

C1: WPA2-Enterprise

Beschützte Technologie: WLAN

Bei Komponenten / Datenflüssen:

- N1 CP2 Softwareanwendung -> CP18 Endgeräte Bereich 1: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N2 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle [WLAN],
- N6 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],
- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D4 aufbereitete Daten konsumieren (intern): D1, D2 und D3 [WLAN],
- N11 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D7 Daten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N15 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [WLAN],

- N20 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D12 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) [WLAN],
- N24 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [WLAN],
- N32 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle [WLAN],
- N38 CP20 Endgeräte Öffentlich -> CP14 IT-Infrastruktur Öffentliches Netz: D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [WLAN]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

Bemerkung: Wenn darauf geachtet wird, dass ein sicheres Passwort verwendet wird, wird WPA2-Enterprise als sichere SotA-Maßnahme gesehen.

C4: Firewall

Beschützte Technologie: Internet

Bei Komponenten / Datenflüssen:

- N13 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [Internet],
- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [Internet],
- N18 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D10 Synchronisation für die langfristige Speicherung der Baustellendaten [Internet],
- N22 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP14 IT-Infrastruktur Öffentliches Netz: D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden [Internet],

- N25 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP14 IT-Infrastruktur Öffentliches Netz: D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [Internet],
- N27 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP14 IT-Infrastruktur Öffentliches Netz: D15 Weitergabe Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zur Auswertung und langfristigen Speicherung [Internet],
- N28 CP14 IT-Infrastruktur Öffentliches Netz -> CP10 IT Infrastructure Bereich 2 (Fertigung / Unternehmen): D15 Weitergabe Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden zur Auswertung und langfristigen Speicherung [Internet],
- N30 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP14 IT-Infrastruktur Öffentliches Netz: D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk [Internet],
- N31 CP14 IT-Infrastruktur Öffentliches Netz -> CP6 IT Infrastructure Bereich 1 (Fertigung / Unternehmen): D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk [Internet],
- N33 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP14 IT-Infrastruktur Öffentliches Netz: D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle [Internet],
- N34 CP14 IT-Infrastruktur Öffentliches Netz -> CP6 IT Infrastructure Bereich 1 (Fertigung / Unternehmen): D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle [Internet],
- N36 CP14 IT-Infrastruktur Öffentliches Netz -> CP10 IT Infrastructure Bereich 2 (Fertigung / Unternehmen): D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger [Internet],
- N39 CP14 IT-Infrastruktur Öffentliches Netz -> CP10 IT Infrastructure Bereich 2 (Fertigung / Unternehmen): D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [Internet],
- N42 CP14 IT-Infrastruktur Öffentliches Netz -> CP6 IT Infrastructure Bereich 1 (Fertigung / Unternehmen): D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential: Basic

Bemerkung: Keine Einschätzung möglich, da keine Angaben über die Konfiguration der Firewall gemacht wurden.

C5: Virtualisierung durch Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster,
- CP15 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: High

C6: Zugriffsschutz für ScaleIT / Username + Passwort

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster,
- CP15 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity, AVA Availability

Benötigtes Angriffspotential: Enhanced-Basic

C10: HTTP Auth Token basiert

Beschützte Technologie: WLAN, LAN, Internet

Bei Komponenten / Datenflüssen:

- N1 CP2 Softwareanwendung -> CP18 Endgeräte Bereich 1: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N2 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle [WLAN],
- N6 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],

- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D4 aufbereitete Daten konsumieren (intern): D1, D2 und D3 [WLAN],
- N11 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D7 Daten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N15 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [WLAN],
- N20 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D12 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) [WLAN],
- N24 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [WLAN],
- N32 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle [WLAN],
- N38 CP20 Endgeräte Öffentlich -> CP14 IT-Infrastruktur Öffentliches Netz: D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [WLAN],
- N8 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D5 Aufbereitete Fertigungsdaten für extern: Ausgewählte Daten aus D1, D2 und D3 [LAN],
- N10 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D6 Sammlung von internen Daten zur kurzfristigen Speicherung (bis zum Zeitpunkt einer Synchronisation) für Auswertungen und zur Weitergabe an externe Gewerke für deren Auswertungen [LAN],
- N12 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [LAN],
- N14 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [LAN],

- N17 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [LAN],
- N19 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D11 Synchronisation für die langfristige Speicherung der Daten vom Fertiger [LAN],
- N21 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden [LAN],
- N23 CP14 IT-Infrastruktur Öffentliches Netz -> CP15 ScaleIT Cloud Cluster: D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden [LAN],
- N26 CP14 IT-Infrastruktur Öffentliches Netz -> CP15 ScaleIT Cloud Cluster: D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [LAN],
- N29 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk [LAN],
- N35 CP15 ScaleIT Cloud Cluster -> CP14 IT-Infrastruktur Öffentliches Netz: D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger [LAN],
- N37 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger [LAN],
- N40 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [LAN],
- N41 CP15 ScaleIT Cloud Cluster -> CP14 IT-Infrastruktur Öffentliches Netz: D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle [LAN],
- N43 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP9 ScaleIT Edge Server: D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle [LAN],
- N13 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [Internet],

- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [Internet]

Betroffene Schutzzielklassen: INT Integrity

Benötigtes Angriffspotential: Enhanced-Basic

C.4.2. Erweiterte Maßnahmen

C2: TLS

Beschützte Technologie: LAN, WLAN, Internet

Bei Komponenten / Datenflüssen:

- N8 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D5 Aufbereitete Fertigungsdaten für extern: Ausgewählte Daten aus D1, D2 und D3 [LAN],
- N10 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D6 Sammlung von internen Daten zur kurzfristigen Speicherung (bis zum Zeitpunkt einer Synchronisation) für Auswertungen und zur Weitergabe an externe Gewerke für deren Auswertungen [LAN],
- N12 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [LAN],
- N14 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [LAN],
- N17 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [LAN],
- N19 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D11 Synchronisation für die langfristige Speicherung der Daten vom Fertiger [LAN],
- N21 CP9 ScaleIT Edge Server -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden [LAN],

- N23 CP14 IT-Infrastruktur Öffentliches Netz -> CP15 ScaleIT Cloud Cluster: D13 Vom Baustellenbetreiber geteilte Baustellendaten (3D-Informationen, Planungsdaten) für externe Planer oder Kunden [LAN],
- N26 CP14 IT-Infrastruktur Öffentliches Netz -> CP15 ScaleIT Cloud Cluster: D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [LAN],
- N29 CP11 ScaleIT Cloud Cluster -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D16 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) bereitgestellt vom externen Gewerk [LAN],
- N35 CP15 ScaleIT Cloud Cluster -> CP14 IT-Infrastruktur Öffentliches Netz: D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger [LAN],
- N37 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D18 Vom Planer geteilte Informationen zur Auswertung/Ausplanung für den Fertiger [LAN],
- N40 CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen) -> CP11 ScaleIT Cloud Cluster: D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [LAN],
- N41 CP15 ScaleIT Cloud Cluster -> CP14 IT-Infrastruktur Öffentliches Netz: D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle [LAN],
- N43 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP9 ScaleIT Edge Server: D20 Vom Planer bereitgestellte Daten zur Nutzung auf der Baustelle [LAN],
- N1 CP2 Softwareanwendung -> CP18 Endgeräte Bereich 1: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N2 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N3 CP3 Sensor-Aktor-Maschine (Fertigungsmaschine / Laserscanner) -> CP9 ScaleIT Edge Server: D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle [WLAN],
- N6 CP18 Endgeräte Bereich 1 -> CP9 ScaleIT Edge Server: D3 Daten zum Lokalisierungsstatus, Produktinformationen [WLAN],
- N7 CP1 Datenemitter / -konsument -> CP9 ScaleIT Edge Server: D4 aufbereitete Daten konsumieren (intern): D1, D2 und D3 [WLAN],

- N11 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D7 Daten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten [WLAN],
- N15 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [WLAN],
- N20 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D12 Daten für die Planung, 3D-Daten (z. B. für Montageanweisungen auf der Baustelle) [WLAN],
- N24 CP18 Endgeräte Bereich 1 -> CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen): D14 Baustellendaten (3D-Informationen, Planungsdaten) von externen Planern oder Kunden [WLAN],
- N32 CP19 Endgeräte Bereich 2 -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D17 Vom Fertiger geteilte Planungs- und Montageinformationen zur Verwendung auf der Baustelle [WLAN],
- N38 CP20 Endgeräte Öffentlich -> CP14 IT-Infrastruktur Öffentliches Netz: D19 Planungsdaten zur langfristigen Speicherung (intern beim Fertiger) [WLAN],
- N13 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D1 Baustellendaten zur Lokalisierung der Position / Montageprotokolle (QM) / 3D-Daten / Streamingdaten, D2 Daten zur Fertigungs- und Laser-Scankonfiguration in der Fertigung und auf der Baustelle / 3D-Abgleichsdaten von der Baustelle, D3 Daten zum Lokalisierungsstatus, Produktinformationen [Internet],
- N16 CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen) -> CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen): D9 Daten für die Planung, 3D-Daten, Daten für Qualitätssicherung Montage [Internet]

Betroffene Schutzzielklassen: CNF Confidentiality, INT Integrity

Benötigtes Angriffspotential: Beyond High

C7: Verschlüsselung der Docker Container

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster,
- CP15 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: CNF Confidentiality

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C8: Backup in der Cloud

Beschützte Technologie: ScaleIT Plattform

Bei Komponenten / Datenflüssen:

- CP9 ScaleIT Edge Server,
- CP11 ScaleIT Cloud Cluster,
- CP15 ScaleIT Cloud Cluster

Betroffene Schutzzielklassen: AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: Angenommen, dass das Backup automatisch und häufig genug stattfindet, schützt die Maßnahme effektiv gegen Ausfälle am Edge-Server

C9: VPN

Beschützte Technologie: VPN

Betroffene Schutzzielklassen: INT Integrity, AVA Availability

Benötigtes Angriffspotential: Beyond High

Bemerkung: SotA-Absicherung, solange richtig konfiguriert

C12: Härtung der Komponenten

Bei Komponenten / Datenflüssen:

- CP1 Datenemitter / -konsument,
- CP6 IT-Infrastruktur Bereich 1 (Fertigung / Unternehmen),
- CP10 IT-Infrastruktur Bereich 2 (Fertigung / Unternehmen),
- CP18 Endgeräte Bereich 1,
- CP19 Endgeräte Bereich 2

Betroffene Schutzzielklassen: INT Integrity, CNF Confidentiality, AVA Availability

Beispiele: Secure Boot, HSM zur Ablage von kryptografischem Material, Schließen von unnötigen Schnittstellen, Zugriffsschutz, . . .

Benötigtes Angriffspotential: Moderate

C.5. Identifizierte Risiken

Ein Risiko besteht aus einer Bedrohung, die nach ihrem benötigten Angriffspotential, um den Angriff durchzuführen, und möglichen Schäden durch die Verletzung der betroffenen Schutzziele ausgewertet wurde. Risiken werden charakterisiert durch mögliche Vorfälle und ihre Konsequenzen und werden gemäß des benötigten Angriffspotentials und des Schadenspotentials bewertet.

Die aufgelisteten Risiken beginnen mit der ID, gefolgt von dem Namen für die entsprechende Bedrohung. Falls anwendbar, werden vorbereitende Angriffe angegeben. Diese sollten als Bedrohungen angesehen werden, die zuvor realisiert werden müssen. Normalerweise werden vorbereitende Angriffe benutzt, um bestehende Maßnahmen in ihrer Wirkung zu hindern. Durch diese Verknüpfung ist die Modellierung komplexer Angriffe möglich.

Nach dem erläuternden Kommentar zeigt eine Tabelle die bewerteten Risiken. Die einzelnen Szenarien unterscheiden sich durch die berücksichtigten Maßnahmengruppen.

R1: Manipulation als MitM auf der WLAN-Kommunikation zwischen Datenemittern und IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C2 TLS, C10 HTTP Auth Token basiert	Moderate

R2: Abhören der WLAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise,	Moderate
ALL	C1 WPA2-Enterprise, C2 TLS	Moderate

R3: Unterbrechen der WLAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R4: Manipulation als MitM auf der WLAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C2 TLS, C10 HTTP Auth Token basiert	Moderate

R5: Abhören der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise, C2 TLS	Moderate

R6: Unterbrechen der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R7: Manipulation als MitM auf der WLAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 2 oder Spoofen eines Kommunkationsteilnehmers

Aufgrund der zusätzlichen WPA2-Enterprise-Verschlüsselung sind Angriffe auf bestehende WLAN-Verbindungen schwer durchzuführen und es besteht nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate
ALL	C1 WPA2-Enterprise, C10 HTTP Auth Token basiert	Moderate

R8: Abhören der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Das Abhören von WLAN-Verbindungen ist aufgrund der WPA2-Enterprise-Verbindungsverschlüsselung schwer und trägt somit nur ein moderates Risiko.

Gruppen	Maßnahmen	Risiko
Basis	C1 WPA2-Enterprise	Moderate
ALL	C1 WPA2-Enterprise	Moderate

R9: Unterbrechen der WLAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Unterbrechungen von Funkverbindungen sind durch Störungen leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R10: Angriffe auf das Auslesen der RFID-Tags/ der QR-Codes

Hierfür wäre eine Manipulation der Übertragungsstrecke, also zwischen RFID-Tag und Lesegerät, notwendig. Diese erscheint nicht realistisch.

Gruppen	Maßnahmen	Risiko
Basis		Moderate
ALL		Moderate

R11: Manipulation als MitM auf der LAN-Kommunikation zwischen Datenemittern und IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von hoch auf gering reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Low

R12: Abhören der LAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein moderates Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Moderate
ALL	C2 TLS	Low

R13: Unterbrechen der LAN-Verbindung zwischen Datenemittern und IT-Infrastruktur Bereich 1

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R14: Manipulation als MitM auf der LAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 1 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R15: Abhören der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Moderate

R16: Unterbrechen der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 1

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R17: Manipulation als MitM auf der LAN-Kommunikation zwischen Komponenten der IT-Infrastruktur Bereich 2 oder Spoofen eines Kommunkationsteilnehmers

Die HTTP Auth Tokens schützen nur begrenzt vor einem MitM-Angriff. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von sehr hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C10 HTTP Auth Token basiert	Very High
ALL	C2 TLS, C10 HTTP Auth Token basiert	Moderate

R18: Abhören der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Da die Verbindungen innerhalb des Gebäudes unverschlüsselt sind, besteht ein sehr hohes Risiko, dass Verbindungen dort abgehört werden können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C2 TLS	Moderate

R19: Unterbrechen der LAN-Verbindung zwischen Komponenten der IT-Infrastruktur Bereich 2

Unterbrechungen von Verbindungen sind mit physischem Zugriff leicht zu erreichen. Auch wenn der mögliche Schaden gering ist, besteht hier daher ein hohes Risiko.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R20: Manipulation als MitM im Internet oder Spoofen eines Endpunktes

Die HTTP Auth Tokens schützen nur begrenzt vor einem MitM-Angriff. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Durch Anwendung von TLS mit geeigneten Cipher Suites kann das Risiko von hoch auf moderat reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis	C4 Firewall	High
ALL	C2 TLS, C4 Firewall	Moderate

R21: Abhören der Internet Verbindung

Da die Verbindungen über das Internet unverschlüsselt sind, besteht ein Risiko, dass Verbindungen dort abgehört werden können. Allerdings muss der Angreifer erst einmal auf die Verbindung zugreifen können. Auch hier kann das Risiko durch Anwendung von TLS deutlich reduziert werden.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL	C2 TLS	Moderate

R22: Unterbrechen der Internetverbindung bzw. Denial of Service eines Endpunktes

Unterbrechungen von Verbindungen sind hier leicht zu erreichen.

Gruppen	Maßnahmen	Risiko
Basis		High
ALL		High

R23: Angriffe auf die Datenemitter

Da die Datenemitter über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R24: Angriffe auf die IT-Infrastruktur Bereich 1 (ScaleIT ausgeschlossen)

Da die IT-Infrastruktur im Bereich 1 über keine Schutzmechanismen verfügen und zudem wichtige Daten liefern, besteht hier ein sehr hohes Risiko. Durch eine Absicherung der verwendeten Komponenten lässt sich das Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container, C8 Backup in der Cloud, C12 Härtung der Komponenten	Moderate

R25: Angriffe auf die IT-Infrastruktur Bereich 2 (ScaleIT ausgeschlossen)

Während die IT-Infrastruktur im Bereich 2 über keine Schutzmechanismen verfügt, werden hier auch keine kritischen Daten verarbeitet.

Gruppen	Maßnahmen	Risiko
Basis		Very High
ALL	C12 Härtung der Komponenten	High

R26: Kompromittieren eines ScaleIT Edge Servers im Bereich 1

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High

R27: Auslesen von gespeicherten Daten aus einem ScaleIT Edge-Server im Bereich 1

Die Vertraulichkeit der Daten auf dem Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung von SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container	Moderate

R28: Unterbrechen der Verfügbarkeit eines ScaleIT Edge Servers im Bereich 1

Die Verfügbarkeit des Scale-IT Edge Servers ist bereits durch verschiedene Maßnahmen der Plattform abgesichert.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	Low
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud	Low

R29: Kompromittieren eines ScaleIT Cloud Clusters im Bereich 2

Der Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein hohes Risiko, da der Schaden im Falle eines Angriffs hoch ist.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High

R30: Auslesen von gespeicherten Daten aus einem ScaleIT Cloud Cluster im Bereich 2

Die Vertraulichkeit der Daten auf dem Scale-IT Edge Server ist bereits durch verschiedene Maßnahmen der Plattform abgesichert. Dennoch besteht hier ein ho-

hes Risiko, da der Schaden im Falle eines Angriffs hoch ist. Durch die Verwendung von SotA-Verschlüsselung lässt sich dieses Risiko reduzieren.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	High
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C7 Verschlüsselung der Docker Container	Moderate

R31: Unterbrechen der Verfügbarkeit eines ScaleIT Cloud Clusters im Bereich 2

Die Verfügbarkeit des Scale-IT Cloud Clusters ist bereits durch verschiedene Maßnahmen der Plattform abgesichert.

Gruppen	Maßnahmen	Risiko
Basis	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort	Low
ALL	C5 Virtualisierung durch Docker Container, C6 Zugriffsschutz für ScaleIT / Username + Passwort, C8 Backup in der Cloud	Low

C.6. Risikoübersicht

	Basis	ALL
Low	2	4
Moderate	8	16
High	15	11
Very High	6	0

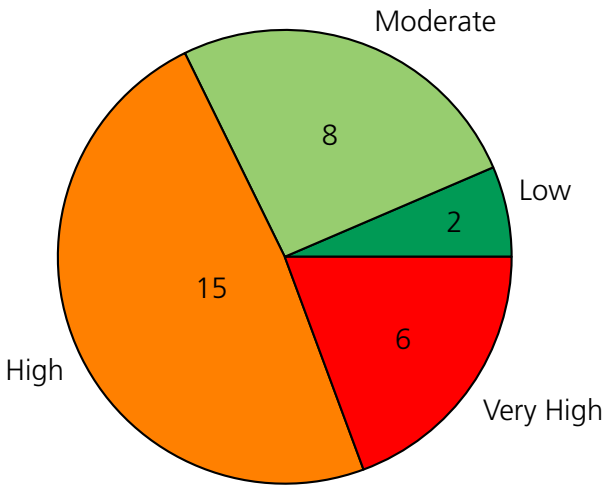

Abbildung C.2.: Control Groups: Basis

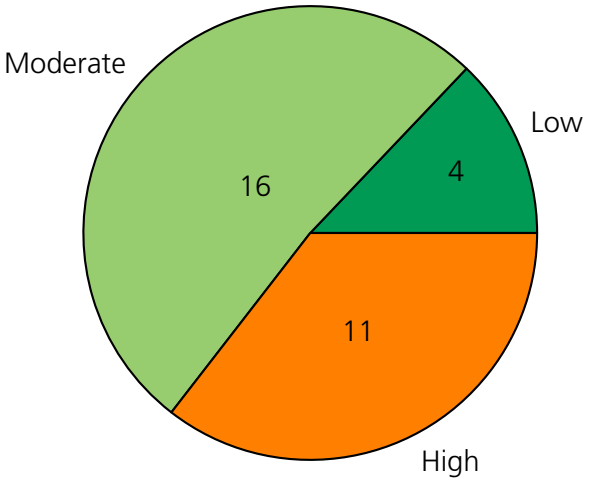

Abbildung C.3.: Control Groups: ALL

D. TLS Cipher Suites

Davon ausgehend, dass TLS sowohl für die Verschlüsselung als auch Authentifizierung verwendet werden soll, ergeben sich folgende mögliche Cipher Suites:

- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM_8
- TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256