



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

IT-Grundschutz-Profil „Chemie“

Version 2025



Änderungshistorie

<i>Version</i>	<i>Datum</i>	<i>Beschreibung</i>
1.0	19.01.2023	Freigabe
2.0	15.01.2025	Freigabe

Tabelle 1: Beschriftung

Danksagung

Version 2 wurde in einem BSI-Arbeitskreis mit folgenden Personen weiterentwickelt (in alphabetischer Reihenfolge):

- Anders, Ferdinand (Merck KGaA)
- Cordt, Jens (Bundesamt für Sicherheit in der Informationstechnik)
- Kleine Büning, Klaus (TÜV NORD InfraChem GmbH & Co. KG)
- Kluge, Jens (Bundesamt für Sicherheit in der Informationstechnik)
- Manske, Hartmut (Merck KGaA)
- Rudolph, Heiko (admeritia GmbH)
- Russmann, Jan (Dow Deutschland Anlagengesellschaft mbH)
- Sturm, Thomas
- Thiedemann, Maximilian (BASF SE)
- Wehn, Christoph (focus Industrieautomation GmbH)

Das BSI dankt allen Teilnehmenden für die konstruktive Mitarbeit.

Version 1 wurde mit Personen aus dem NAMUR Arbeitskreis 4.18 entwickelt (in alphabetischer Reihenfolge):

- Anders, Ferdinand (Merck KGaA)
- Biß, Klaus (Bundesamt für Sicherheit in der Informationstechnik)
- Bittcher, Benedikt (Wacker Chemie AG)
- Cordt, Jens (Bundesamt für Sicherheit in der Informationstechnik)
- Lipp, Jakob (IGR Interessengemeinschaft Regelwerke Technik e.V.)
- Kleine Büning, Klaus (TÜV NORD InfraChem GmbH & Co. KG)
- Linnartz, Markus (Evonik Operations GmbH)
- Manske, Hartmut (Merck KGaA)
- Rudolph, Heiko (admeritia GmbH)
- Russmann, Jan (Dow Deutschland Anlagengesellschaft mbH)
- Speth, Walter (Bayer AG)
- Sturm, Thomas
- Pöschko, Pascal (BYK-Chemie GmbH)
- Winkel, Detlef (Bayer AG)

Inhalt

1	Vorbemerkungen.....	6
2	Formale Aspekte.....	7
3	Management Summary.....	8
3.1	Zielgruppe	8
3.2	Zielsetzung	8
4	Geltungsbereich.....	9
4.1	Schutzbedarf.....	9
4.2	IT-Grundschutz-Vorgehensweise	9
5	Abgrenzung des Informationsverbunds	10
5.1	Bestandteile des Informationsverbunds.....	10
5.2	Nicht berücksichtigte Objekte	10
6	Referenzarchitektur.....	11
6.1	Integrierte Komponenten.....	11
6.2	Hinweise zu den Modellarchitekturen.....	11
6.3	Anwendbarkeit der Modellarchitekturen.....	11
6.4	Einteilung der Modellarchitekturen	11
6.4.1	Zone A – Kern SIS.....	11
6.4.2	Zone B – Erweitertes SIS	12
6.4.3	Zone C – Produktionsumgebung	12
6.4.4	Zone IT-Infrastruktur.....	12
6.4.5	Elemente der Modellarchitekturen	12
6.5	Hinweis zu gemeinsam genutzten Komponenten.....	12
6.6	Varianten der Modellarchitekturen	13
6.6.1	Modellarchitektur 1 – Separierte Nutzung.....	13
6.6.2	Modellarchitektur 2 – Gemeinsame Nutzung.....	14
6.6.3	Modellarchitektur 3 – Vollintegrierte Komponenten	15
7	Untersuchungsgegenstand	16
7.1	Infrastruktur.....	16
7.1.1	Zuordnung der Zielobjekte	17
7.1.2	Untersuchungsgegenstand.....	17
7.1.3	Zuordnung der Zielobjekte und Schränke zu den Räumen	18
8	Auswahl relevanter Bausteine	20
8.1	Prozess-Bausteine	20
8.2	System-Bausteine.....	21
8.2.1	APP: Anwendungen	22
8.2.2	SYS: IT-Systeme	23

8.2.3	IND: Industrielle IT	26
8.2.4	NET: Netze und Kommunikation	27
8.2.5	INF: Infrastruktur.....	28
9	Restrisikobetrachtung/Risikobehandlung.....	29
9.1	Analyse und Definition der Restrisiken.....	29
9.2	Mitigierende Maßnahmen zur Restrisikobehandlung	29
9.3	Ausnahmeprozesse.....	30
10	Unterstützende Informationen.....	32
11	Anhang.....	34
11.1	Anhang A Schutzbedarfszuweisungen für chemische Produktionsanlagen	34
11.1.1	Auswirkung auf SIS.....	34
11.1.2	Schadensszenarien.....	35
11.1.3	Schutzbedarfsfestlegung	37
11.2	Anhang B Gefährdungsbetrachtung der Komponenten	37
11.2.1	IT1 – Sensor	38
11.2.2	IT2 – Aktor	40
11.2.3	IT3 – Logiksysteme.....	42
11.2.4	IT4 – Programmierstation.....	44
11.2.5	IT5 – Bedienstation	44
11.2.6	IT6 – Konfigurationsgerät	45
11.2.7	IT7 –Servicegeräte	46
11.2.8	IT8 – Betriebsdateninformationssystem.....	47
11.2.9	IT9b Sprungserver	48
11.2.10	IT9d Datensicherung	48
11.2.11	IT9f Updateservice.....	49
11.2.12	IT9g Verzeichnisdienst.....	49
11.2.13	Weitere Dienste IT9h.....	50
11.2.14	IT10 – IT-Infrastruktur	52
11.2.15	Netzwerkkomponenten.....	52
11.3	Anhang C Mapping.....	53
11.4	Anhang D Glossar.....	54
	Literaturverzeichnis	59

1 Vorbemerkungen

Der Schutz von Menschen und Umwelt wird in der chemischen Industrie häufig mit entsprechenden Einrichtungen der Betriebseinrichtungen der Prozessleittechnik (PLT-B) durch Sicherheitseinrichtungen der Prozessleittechnik (im folgenden PLT-Sicherheitseinrichtung (PLT-S) genannt bzw. englisch: Safety Instrumented Systems; SIS) erreicht.

Neben dem Schutz vor Gefahren, die sich aus dem Produktionsprozess selbst ergeben, sind durch die zunehmende Vernetzung mit wachsender Priorität auch Aspekte der Cybersicherheit bei der Funktionalen Sicherheit zu berücksichtigen. Das bedeutet konkret, dass PLT-S sowie PLT-Betriebseinrichtungen mit Sicherheitsfunktion (PLT-BS) in geeigneter Weise zu schützen sind, um ihre Funktion und damit den Schutz vor den genannten Gefahren auch angesichts zunehmender Cyberbedrohungen zu gewährleisten.

In Abgrenzung zur IT verwendet das vorliegende Dokument den Begriff „Operational Technology“ (OT).

Obgleich OT-Systeme sich zum Teil der gleichen Komponenten (z. B. Server und Workstations) und der gleichen Betriebssysteme wie die IT bedienen, gelten für OT-Systeme andere bzw. zusätzliche Anforderungen hinsichtlich Funktionaler Sicherheit und Cybersicherheit ebenso wie der Notwendigkeit, Produktionsstillstände zu vermeiden, falls Änderungen an OT-Systemen vorgenommen werden müssen. Es gilt daher die Verfügbarkeit und Integrität der OT-Systeme sicherzustellen, um insbesondere die korrekte Funktionsweise der PLT-S zu gewährleisten. Zusätzlich dient dies dem Aufrechterhalten der Produktion an sich. Ergänzend werden im OT-Umfeld Komponenten eingesetzt, die mit klassischen IT-Sicherheitsmaßnahmen aufgrund technologischer Einschränkungen nicht geschützt werden können.

Gemäß dieser Definition beschreibt das vorliegende Dokument ein „OT-Grundsicherheits-Profil“. Aufgrund des Eigennamens „IT-Grundsicherheits-Profil“ des BSI bleibt es allerdings bei dieser Namensgebung.

Im Anhang befinden sich weitere Überlegungen und Hintergründe zur Schutzbedarfsfestlegung, Anforderungsauswahl aus dem IT-Grundsicherheits-Kompendium sowie eine Übersicht der Gefährdungen, denen einzelne Prozesse ausgesetzt sein können.

Die Vorgehensweise des IT-Grundsicherheits stellt eine Lösungsvariante für die Erfüllung der Anforderungen aus dem KAS-51 dar.

2 Formale Aspekte

Titel:	IT-Grundschatz-Profil für Produktionsanlagen der chemischen Industrie
Versionsstand:	2.0.0
Revisionszyklus:	alle 2 Jahre
Vertraulichkeit:	öffentlich

3 Management Summary

3.1 Zielgruppe

Dieses IT-Grundsicherungs-Profil richtet sich primär an Betreiber von Chemieanlagen, welche PLT-S und PLT-BS zur Verhinderung von Störfällen einsetzen. Unter dem Begriff Chemieanlagen werden in diesem IT-Grundsicherungsverfahrenstechnische Produktionsanlagen zur Herstellung von Stoffen, Gemischen und Erzeugnissen verstanden.

Das Dokument richtet sich vorrangig an Personen, die für alle Lebensphasen der OT verantwortlich sind, als auch an Personen die IT-Services für die OT zur Verfügung stellen.

3.2 Zielsetzung

Der Fokus dieses IT-Grundsicherungs-Profiles liegt auf der Absicherung von PLT-S in Chemieanlagen gegenüber Cyberangriffen. Hierzu werden die bestehenden Leitfäden, Empfehlungen und Arbeitsblätter KAS-51, TRBS 1115-1, VDI/VDE 2182, NA 163, NE 165 und NA 169 berücksichtigt und teilweise konkretisiert (beispielsweise in Bezug auf eine Dokumentation des Schutzbedarfs). Dabei werden Gefährdungen betrachtet, die direkt oder indirekt zu einer Kompromittierung der PLT-S führen können.

Das IT-Grundsicherungs-Profil soll den Betreibern von Chemieanlagen die Umsetzung des IT-Grundsicherungs erleichtern, um den IT-Grundsicherungs zur Gewährleistung der Funktionalen Sicherheit zu verwenden. Dabei wird zwischen Modellarchitekturen unterschieden, um jeweils zweckmäßige Maßnahmen (auch Kombinationen von Maßnahmen und ggf. unterschiedliche Optionen) zur Reduzierung des Risikos abzuleiten.

Auch ohne eine gesonderte Betrachtung von Cyberangriffen werden für Chemieanlagen systematische, ganzheitlich angelegte Gefahrenanalysen, z. B. mittels PAAG-Verfahren (siehe Glossar) durchgeführt. Derlei Gefahrenanalysen der chemisch-verfahrenstechnischen Prozesse münden in eine belastbare Risikobewertung, sodass bereits wesentliche Aspekte einer IT-Risikoanalyse (begrenzt auf die Schutzziele von 12. BImSchV¹, GefStoffV² und BetrSichV³, d. h. Aspekte der Anlagenverfügbarkeit, des Knowhow-Schutzes usw. bleiben normalerweise unberücksichtigt) vorweggenommen und entsprechende Schutzmaßnahmen ergriffen werden.

Das IT-Grundsicherungs-Profil erweitert die verfahrenstechnischen Gefahrenanalysen und Schutzkonzepte um Anforderungen zum Schutz der Funktion von PLT-S und PLT-BS vor Cyberangriffen und Beeinträchtigungen der IT. Dabei wird berücksichtigt, dass diese Anforderungen die Funktionalität der PLT-S nicht beeinflussen.

Ziel ist es nicht, Betreibern von Chemieanlagen einen weiteren Anforderungskatalog aufzuerlegen, den diese zusätzlich zu anderen Empfehlungen erfüllen sollen. Stattdessen dient dieses Profil dazu, Mehraufwand für den Betreiber zu reduzieren und aufzuzeigen, welche Aspekte durch die Befolgung anderer Standards und Regularien bereits erfüllt sein sollten. Dadurch ist bei Betreibern ein geringerer Aufwand für Vorbereitung von Audits zu erwarten.

¹ https://www.gesetze-im-internet.de/bimschv_12_2000/

² https://www.gesetze-im-internet.de/gefstoffv_2010/

³ https://www.gesetze-im-internet.de/betrsv_2015/

4 Geltungsbereich

4.1 Schutzbedarf

Im vorliegenden IT-Grundschutz-Profil ist ein Schutzniveau beschrieben, das über dem normalen Schutzbedarf liegt. Das ist deshalb der Fall, weil sich dies aufgrund der erhöhten Schutzanforderungen für die PLT-S ergibt. Dieser erhöhte Schutzbedarf ist bei der Anwendung des IT-Grundschutz-Profiles zu berücksichtigen.

4.2 IT-Grundschutz-Vorgehensweise

Grundlage für das vorliegende IT-Grundschutz-Profil ist die IT-Grundschutz-Vorgehensweise der Standard-Absicherung. In Anhang C Mapping werden Beziehungen zwischen KAS-51, ISO/IEC 27001:2018 und dem IT-Grundschutz dargestellt.

Abdeckung Vorgehensweise ⁴ : Schutzbedarf	Standard-Absicherung mit hohem & sehr hohem
ISO 27001-Kompatibilität:	Ja
Verweis auf andere IT-Grundschutz-Profile:	entfällt

⁴ Aussage darüber, welches Schutzniveau im Vergleich zu den Vorgehensweisen des IT-Grundschatzes mit dem IT-Grundschutz-Profil erreicht wird.

5 Abgrenzung des Informationsverbunds

5.1 Bestandteile des Informationsverbunds

Zur Abgrenzung des Geltungsbereiches in Chemieanlagen muss zwischen Anwendungsfällen unterschieden werden, die in den Modellarchitekturen näher erläutert werden. Diese Fälle haben eventuell unterschiedliche Schutzbedarfskategorien für einzelne Komponenten zur Folge. Weiterhin kann sich eine Erweiterung auf die Produktionsumgebung ergeben, wenn eine PLT-Betriebseinrichtung mit Sicherheitsfunktion verwendet wird. Gemäß VDI/VDE 2180 Teil 1 muss für diese eine IT-Risikobeurteilung durchgeführt werden. Wenn eine IT-Risikobeurteilung des Betreibers bei einer PLT-BS ergibt, dass durch den Ausfall oder durch ein Kompromittieren der PLT-BS die Anlagensicherheit nicht maßgeblich beeinträchtigt würde, ist keine besondere Betrachtung im Sinne der Cybersicherheit notwendig.

PLT-S sind nicht zwangsläufig sicherheitsrelevante Anlagenteile im Sinne der 12. BImSchV. Selbst in Betriebsbereichen der oberen Klasse kann es PLT-S geben, die nicht der Verhinderung von Störfällen im Sinne der 12. BImSchV dienen, vor allem, wenn sie nicht zur Sicherung sicherheitsrelevanter Teile von Betriebsbereichen vorgesehen sind (vgl. KAS-1 „Sicherheitsrelevante Teile eines Betriebsbereiches und Richtwerte für sicherheitsrelevante Anlagenteile (SRA)“). Nur wenn bei Versagen oder Fehlen einer PLT-S ein Störfall nicht auszuschließen ist, handelt es sich nach der „Vollzugshilfe zur Störfall-Verordnung vom März 2004“ um ein sogenanntes (sicherheitsrelevantes) Anlagenteil mit besonderer Funktion, das gemäß Anhang II 12. BImSchV im Sicherheitsbericht zu beschreiben ist.

Da sie ungeachtet dieser Unterscheidung i. A. gleichfalls für die Anlagensicherheit kritische Funktionen erfüllen, kann auch auf solche PLT-S, die nicht sicherheitsrelevante Anlagenteile im Sinne der 12. BImSchV sind, das vorliegende IT-Grundschutz-Profil angewendet werden.

Auf diese Weise kann im Übrigen der Forderung nach Berücksichtigung von Cyberbedrohungen im Rahmen der – aus Sicht des Arbeitsschutzes relevanten – Gefährdungsbeurteilungen (vgl. TRBS 1115-1) in Bezug auf „sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ Rechnung getragen werden, soweit diese als PLT-S ausgeführt sind. Zudem wird damit die Forderung aus der IEC 61511 nach einer IT-Risikobetrachtung erfüllt.

5.2 Nicht berücksichtigte Zielobjekte

Eine Betrachtung der IT-Infrastruktur der Institution erfolgt nicht. Der Informationsverbund umfasst die prozesstechnische Anlage bis hin zu den Schnittstellen zur allgemeinen IT-Infrastruktur.

Darüber hinaus liegt es im Ermessen des Betreibers, solche Komponenten zu identifizieren und gegen Cyberangriffen und -beeinträchtigungen abzusichern, die nur im Fall des Versagens einer oder mehrerer Sicherheitsfunktionen einen Störfall nach 12. BImSchV herbeiführen können.

Verweis auf andere IT-Grundschutz-Profile: entfällt.

6 Referenzarchitektur

Chemieanlagen sind in der Regel aus Komponenten unterschiedlicher Technologiegenerationen aufgebaut. Diese reichen von verbindungsprogrammierten Steuerungen, die für sicherheitsrelevante Aufgaben eingesetzt werden, bis hin zu vollintegrierten Systemen. Diese modernen Systeme übernehmen nicht nur betriebliche Steuerungsaufgaben, sondern auch Sicherheitsfunktionen innerhalb der Anlage.

Die Realisierung einer PLT-S in Chemieanlagen präsentiert eine Vielzahl an Varianten und Facetten. Diese Komplexität lässt sich nicht abschließend zusammenfassen. Besonders hervorzuheben ist die gemeinsame Nutzung von Komponenten durch die PLT-B und PLT-S. Diese gemeinsame Nutzung ist entscheidend, um die zentralen Aspekte der Cybersicherheit für Anlagenbetreiber zu adressieren (siehe 6.5 Hinweis zu gemeinsam genutzten Komponenten).

6.1 Integrierte Komponenten

In diesem Dokument trifft dies auf folgende Komponenten zu:

- Bedienstationen
- Logiksysteme
- Netzwerk / Bus

Bedienstationen werden in Verbindung mit PLT-S-Logiksystemen verwendet, um sicherheitsrelevante Eingaben zu tätigen. Hierunter fallen z. B. rezepturabhängige Grenzwertschaltungen. Eine weitere Nutzung kann darin bestehen, sicherheitsrelevante Alarme darzustellen oder zu quittieren oder Sicherheitsschaltungen zurückzusetzen. Im integrierten Fall sind zusätzlich Prozessbeobachtungen und sonstige Bedienungen möglich.

6.2 Hinweise zu den Modellarchitekturen

Da nicht alle Varianten gemeinsam genutzter Komponenten illustriert werden können, werden in diesem Dokument drei Modellarchitekturen beschrieben. Diese zeigen verschiedene typische Fälle mit zunehmend gemeinsamer Nutzung von Komponenten. Zweck ist es, Unterschiede bei der Auswirkung von Gefährdungen aufzuzeigen.

6.3 Anwendbarkeit der Modellarchitekturen

Da nicht alle Varianten gemeinsam genutzter und integrierter Komponenten illustriert werden können, kann es in den realen Anlagen zu Mischformen der unterschiedlichen Modellarchitekturen kommen.

Anhand der Modellarchitekturen kann sich der Betreiber bei der individuellen Bewertung seiner Anlage hinsichtlich des Einsatzes der Komponenten orientieren. Daraus folgt die Notwendigkeit der individuellen Risikobeurteilung sowie der individuellen Festlegung geeigneter Gegenmaßnahmen. Die beschriebenen Varianten sollen hierfür als Hilfe dienen.

6.4 Einteilung der Modellarchitekturen

Die Modellarchitekturen unterteilen sich in 5 Zonen.

6.4.1 Zone A – Kern PLT-S

Die Zone Kern-PLT-S, auch als Zone A bezeichnet, umfasst die wesentlichen Komponenten der PLT-S. Dazu gehören das Logiksystem, die Ein- und Ausgabebaugruppen, Remote-I/O sowie die Aktoren und Sensoren. Auch Verbindungs- und Netzwerkkomponenten, die für die Kommunikation zwischen Geräten notwendig sind (wie Kabel und Switches), zählen zu dieser Zone. Entscheidend ist, dass alle Hardware-, Software- oder

Netzwerkkomponenten, die für die Ausführung der Sicherheitsfunktion unerlässlich sind, der Zone A angehören.

6.4.2 Zone B – Erweiterte PLT-S

Zone B beinhaltet Komponenten, die nicht direkt für die Ausführung der Sicherheitsfunktion erforderlich sind, aber dennoch Einfluss auf die Zone A – Kern PLT-S haben können. Beispiele hierfür sind Bedienstationen, Programmierstationen (Engineering Station) für PLT-S und Konfigurationsgeräte. Diese Elemente sind Teil der erweiterten PLT-S und beeinflussen indirekt die Sicherheitsfunktionen.

6.4.3 Zone C – Produktionsumgebung (PLT-B)

In der Produktionsumgebung sind alle allgemein für den Produktionsprozess notwendigen Komponenten verortet. Es existieren dort auch Komponenten, die nicht direkt zu den PLT-S zählen, aber dennoch mit der Sicherheitsfunktion in Verbindung stehen können, wie beispielsweise Reset-Anforderungen oder die Visualisierung des Zustands von Sicherheitsfunktionen. Der Fokus der Risikobeurteilung liegt auf den Kern- und erweiterten PLT-S, einschließlich aller damit verbundenen Hardware, Software, Daten, Prozesse, Personen und Organisationen sowie den Kommunikationslinien zu anderen Einrichtungen in der Produktionsumgebung.

6.4.4 Zone OT-Infrastruktur & DMZ

Hier sind den Produktionsprozess und die PLT-S-Komponenten unterstützende Dienste verortet. Dazu gehören beispielsweise Datensicherung und die Anbindung an zentrale IT-Systeme.

6.4.5 Zone IT-Infrastruktur

Dies sind allgemein die zentralen IT-Systeme und Arbeitsplätze. Dieser Teil wird im Rahmen des IT-Grundsatzprofils nicht betrachtet, sondern nur der Vollständigkeit dargestellt. Es wird davon ausgegangen, dass für den Bereich ein entsprechendes ISMS vorhanden ist.

6.4.6 Elemente der Modellarchitekturen

Die drei Modellarchitekturen illustrieren verschiedene typische Fälle mit zunehmend gemeinsamer Nutzung und Integration von Komponenten. Zweck ist es, Unterschiede bei der Auswirkung von Gefährdungen aufzuzeigen.

Die Modellarchitekturen stellen eine logische Sicht auf die Komponenten und Kommunikationsverbindungen dar.

Die Komponenten werden als Kästen dargestellt und beziehen sich auf jeweils ein Gerät mit der entsprechenden Funktion. Es wird darauf hingewiesen, dass interne Signalverarbeitungen innerhalb der Komponenten nicht von außen angreifbar sind, wie etwa durch Cyberangriffe, und auch nicht durch externe Sicherheitsmaßnahmen wie Firewalls geschützt werden können. Das bedeutet, die internen Prozesse jeder Komponente werden als sicher und isoliert von externen Einflüssen betrachtet.

Die Verbindungen stellen Kommunikationsverbindungen zwischen den jeweiligen Endpunkten dar. Es wird mit dieser Darstellung absichtlich von der physischen Verkabelung, Switchen und Routern abstrahiert, um Technologieneutral zu bleiben und die Komplexität etwas zu reduzieren. Zudem liegt der Fokus auf dem Bewerten der Daten, die über die jeweiligen Verbindungen ausgetauscht werden.

6.5 Hinweis zu gemeinsam genutzten Komponenten

Gemeinsam genutzten Komponenten erhöhen grundsätzlich das Risiko bei einem Cyberangriff. Durch den zusätzlichen Funktionsumfang auf einer Komponente steht die Komponente mehr anderen Komponenten

in Verbindung als separierte Varianten, ist ggf. Zugriff durch mehr Personen bzw. andere Komponenten möglich und steigt das Schadensrisiko im Falle einer Kompromittierung.

6.6 Varianten der Modellarchitekturen

Im Text werden die Komponenten mit „IT und einer Nummer“ bezeichnet. Beispielsweise IT3a für das PLT-S-Logiksystem. Gleiches gilt für die Verbindungen, die mit „K und einer Nummer“ referenziert werden. Beispielsweise K3 für die Verbindung zwischen IT1a PLT-S-Sensor und IT3a PLT-S-Logiksystem.

In Abbildung 1, Abbildung 2 und Abbildung 3 wurde auf die Kürzel „IT“ bei den Komponenten und „K“ bei den Verbindungen aus Gründen der Übersichtlichkeit verzichtet.

Die einzelnen Kommunikationsverbindungen (K) und OT-/IT-Komponenten (IT) sind in Anhang B Gefährdungsbetrachtung der Komponenten und der zugehörigen Exceltabelle näher beschrieben.

Für IT 7 Servicegeräte wird auf das Darstellen der Verbindung zu Zone A, B und C verzichtet, da diese in allen Zonen mobil verwendet werden können. Es handelt sich beispielsweise um Laptops, Smartphones oder andere mobile Geräte für Wartung und Parametrierung von einzelnen Komponenten. Dies können eigene Geräte vom Betreiber sein oder externe Geräte von Dienstleistern sein (siehe 11.2.7).

6.6.1 Modellarchitektur 1 – Separierte Nutzung

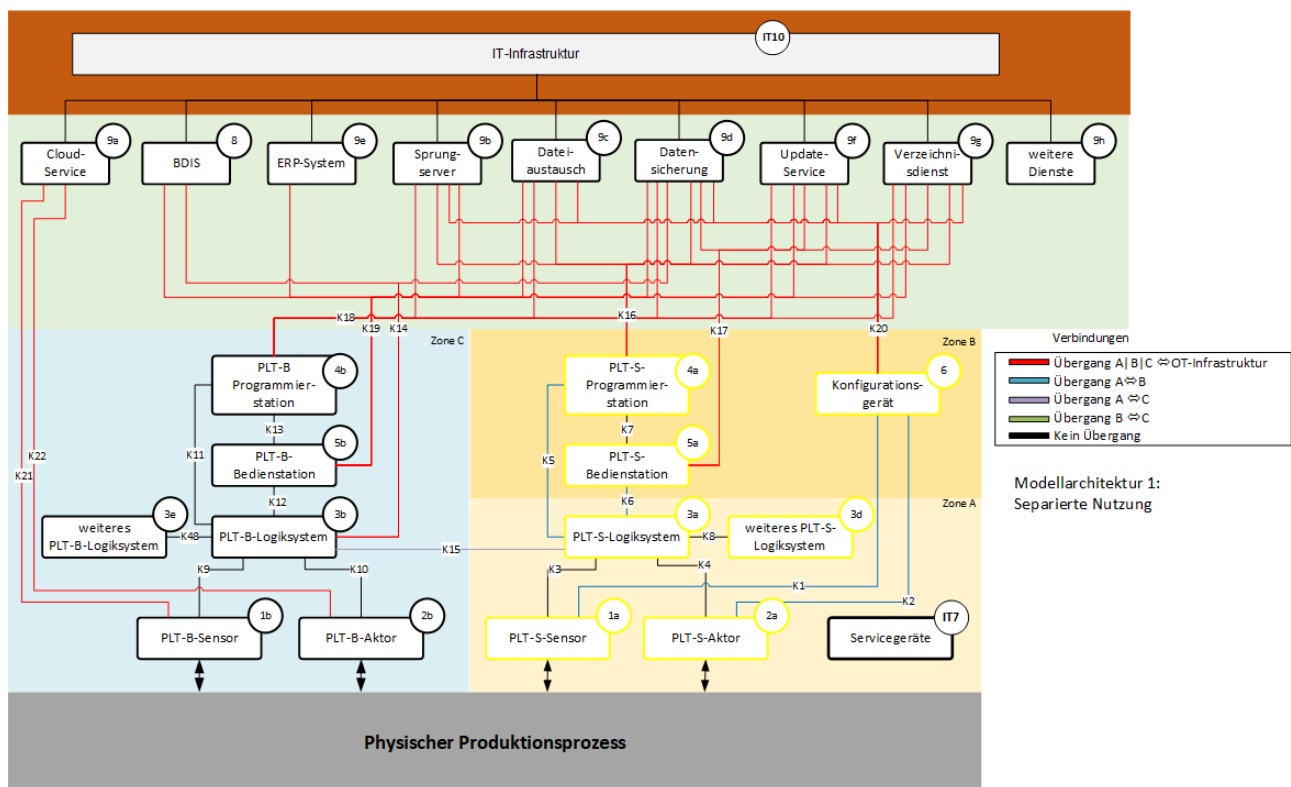


Abbildung 1 Modellarchitektur 1

Abbildung 1 zeigt ein PLT-S mit von den PLT-B separierten Komponenten zur Gewährleistung der Sicherheitsfunktion.

Wesentliches Merkmal dieser Architektur ist die separierte Umsetzung der Aufgaben der PLT-B und der PLT-S. Sie sind funktional getrennt (Ausnahme K15 zum Prozessdatenaustausch). Bei dieser Architektur verfügen PLT-B und PLT-S sowohl über separate Logiksysteme, Sensoren und Aktoren als auch über separate Programmierstationen und Bedienstation. Jedes PLT-S-Logiksystem (IT3a) kann in Verbindung (K8) mit anderen PLT-S-Logiksystemen (IT3d) in Zone A stehen, die z. B. ein anderes Anlagenteil absichern.

Durch die klare Trennung von PLT-B und PLT-S beschränkt sich der erhöhte Schutzbedarf auf Zone A und B. Über die PLT-S-Bedienstation (IT5a) lässt sich die Sicherheitsfunktion unmittelbar z. B. durch eine

routinemäßige, jedoch rezepturabhängig vorzunehmende Grenzwertänderung beeinflussen. Des Weiteren kritisch zu betrachten sind die Verbindungen aus der Zone C in Zone B sowie direkt zum PLT-S-Logiksystem (IT3a).

6.6.2 Modellarchitektur 2 – Gemeinsame Nutzung

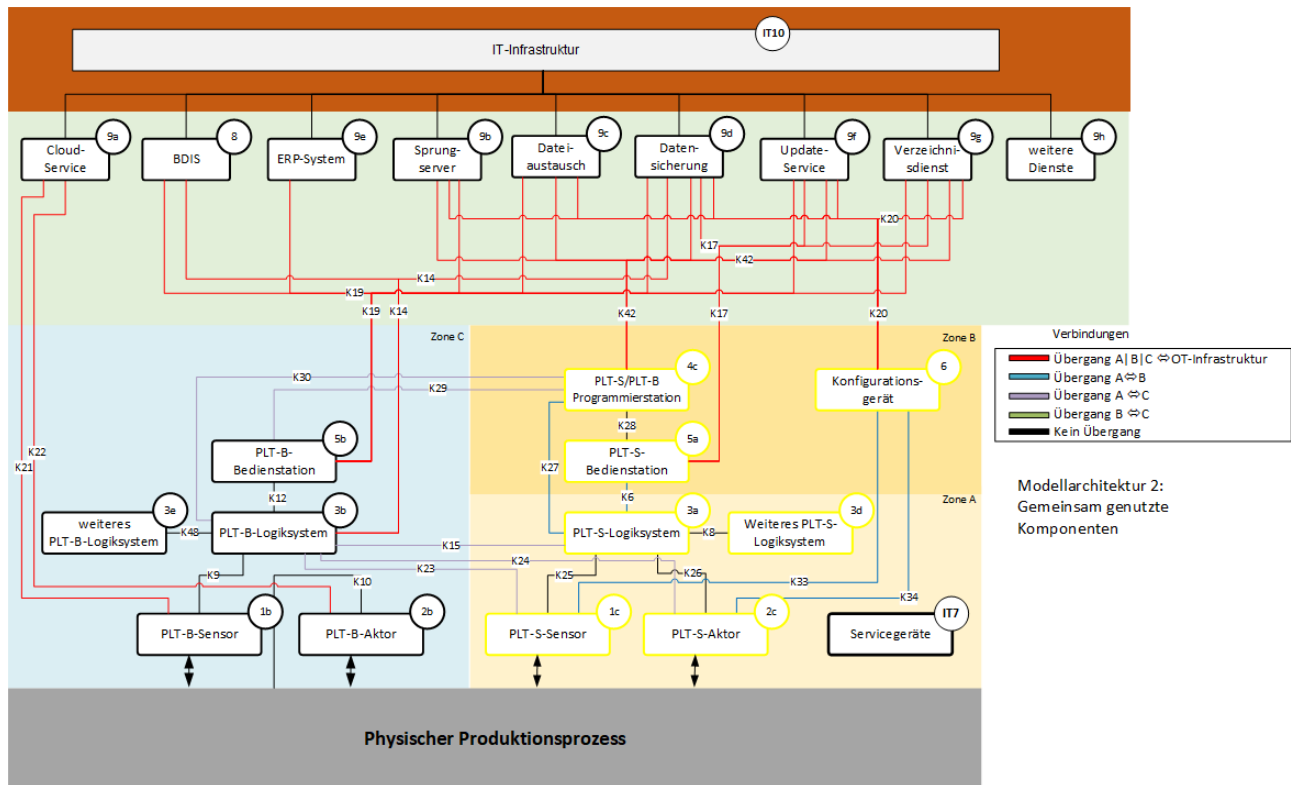


Abbildung 2 Modellarchitektur 2

Abbildung 2 zeigt ein PLT-S, die über eine gemeinsame Programmierstation, aber separate Logiksysteme für PLT-B und PLT-S verfügt.

Diese Architektur unterscheidet sich von Modellarchitektur 1 dadurch, dass die Unabhängigkeit von PLT-B und dem Logiksystem des PLT-S nicht gegeben ist. Während die Funktionen getrennt sind, kann die Konfiguration des PLT-S-Logiksystems wie auch des PLT-B-Logiksystems mit der gleichen PLT-S/PLT-B-Programmierstation (IT4c) erfolgen. Dies hat den Vorteil, nur eine einzige Programmierstation für PLT-B und PLT-S aufsetzen, nutzen, warten und hinsichtlich der Cybersicherheit prüfen zu müssen. Daraus ergibt sich jedoch ein erhöhter Schutzbedarf für die PLT-S/PLT-B-Programmierstation (IT4c) und die Verbindungen (K29 und K30) im Vergleich zu einer Verwendung von der PLT-S-Programmierstation (IT4b) in Modellarchitektur 1.

Die gemeinsame Nutzung von Sensor und Aktor führt dazu, dass sich der Schutzbedarf dieser auf die Verbindungen K23 und K24 vererbt. Denn es sind über diese Zugriffe von der Zone C in die Zone A möglich ist.

6.6.3 Modellarchitektur 3 – Vollintegrierte Komponenten

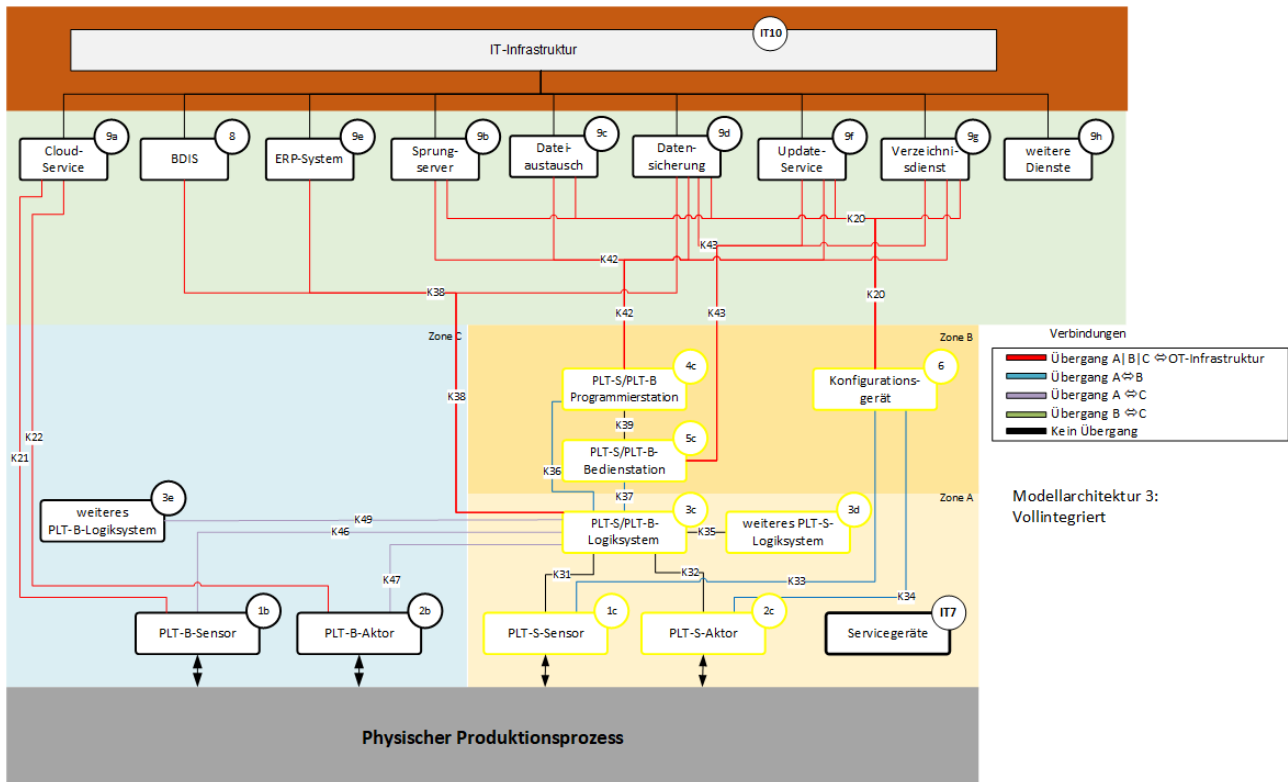


Abbildung 3 Modellarchitektur 3

Abbildung 3 zeigt ein PLT-S, das über ein gemeinsames Programmier- und Konfigurationsgerät für PLT-B und PLT-S verfügt und die deren Logiksysteme in einer Komponente vereint. Weiterhin erfolgt die Bedienung über eine gemeinsame Bedienstation.

Diese Architektur unterscheidet sich von Modellarchitektur 2 dadurch, dass die Unabhängigkeit von PLT-B und PLT-S auf Ebene der Hardware aufgeweicht wird. Beispielsweise kommunizieren die Logiksysteme über feste, durch den Hersteller vorgegebene Schnittstellen sowie mit unterschiedlichen Ein-/Ausgabebaugruppen (andere Varianten siehe Komponentenbeschreibung IT3c im Anhang). Ein Kompromittieren des PLT-S/ PLT-B-Logiksystems (IT3c) eröffnet u. U. die Möglichkeit, sowohl den Anforderungsfall als auch das Versagen des PLT-S hervorzurufen. Dies gilt es bei der Risikobewertung von IT3c und IT5c zu berücksichtigen.

7 Untersuchungsgegenstand

Das zentrale System dieses Dokuments stellt das PLT-S dar. Es dient der Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein PLT-S besteht aus Sensor(en) IT1, einem Logiksystem IT3 und Aktor(en) IT2.

Tabelle 2 Zielobjekte

<i>ID</i>	<i>Zielobjekt</i>
IT1a	PLT-S-Sensor
IT1b	PLT-B-Sensor
IT1c	PLT-S/PLT-B-Sensor
IT2a	PLT-S-Aktor
IT2b	PLT-B-Aktor
IT2c	PLT-S/PLT-B-Aktor
IT3a	PLT-S-Logiksystem
IT3b	PLT-B-Logiksystem
IT3c	PLT-S/PLT-B-Logiksystem
IT4a	PLT-S-Programmiersstation
IT4b	PLT-B-Programmiersstation
IT4c	PLT-S/PLT-B-Programmiersstation
IT5a	PLT-S-Bedienstation
IT5b	PLT-B-Bedienstation
IT5c	PLT-S/PLT-B-Bedienstation
IT6	Konfigurationsgerät
IT7	Servicegeräte
IT8	Betriebsdateninformationssystem (BDIS)
IT9a	Cloud-Service
IT9b	Sprung-Server
IT9c	Dateiaustausch-Service
IT9d	Datensicherung-Service
IT9e	ERP-System
IT9f	Update-Service
IT9g	Verzeichnisdienst
IT9h	Weitere Dienste
IT10	IT-Infrastruktur

Weitere Informationen zu den Komponenten sind im Anhang A Schutzbedarfzuweisungen für chemische Produktionsanlagen zu finden.

7.1 Infrastruktur

In diesem Zielbereich werden die baulichen Gegebenheiten erfasst. Aufgrund der gewachsenen Strukturen in Altanlagen ist eine bauliche Trennung entsprechend der Zoneneinteilung (A, B und Produktionsumgebung) nicht immer möglich oder praktikabel. Damit werden die Modellarchitekturen hinsichtlich ihrer baulichen Realisierung ergänzt.

7.1.1 Zuordnung der Zielobjekte

Im Folgenden werden die Objekte den Infrastrukturelementen (Schränken, Räumen, Gebäuden) zugewiesen. Weiterhin wird mit Abbildung 4 illustriert, wo sich die entsprechenden Räume verorten. Jeder Zonenübergang stellt eine Möglichkeit dar, den Zutritt Unbefugter einzuschränken.

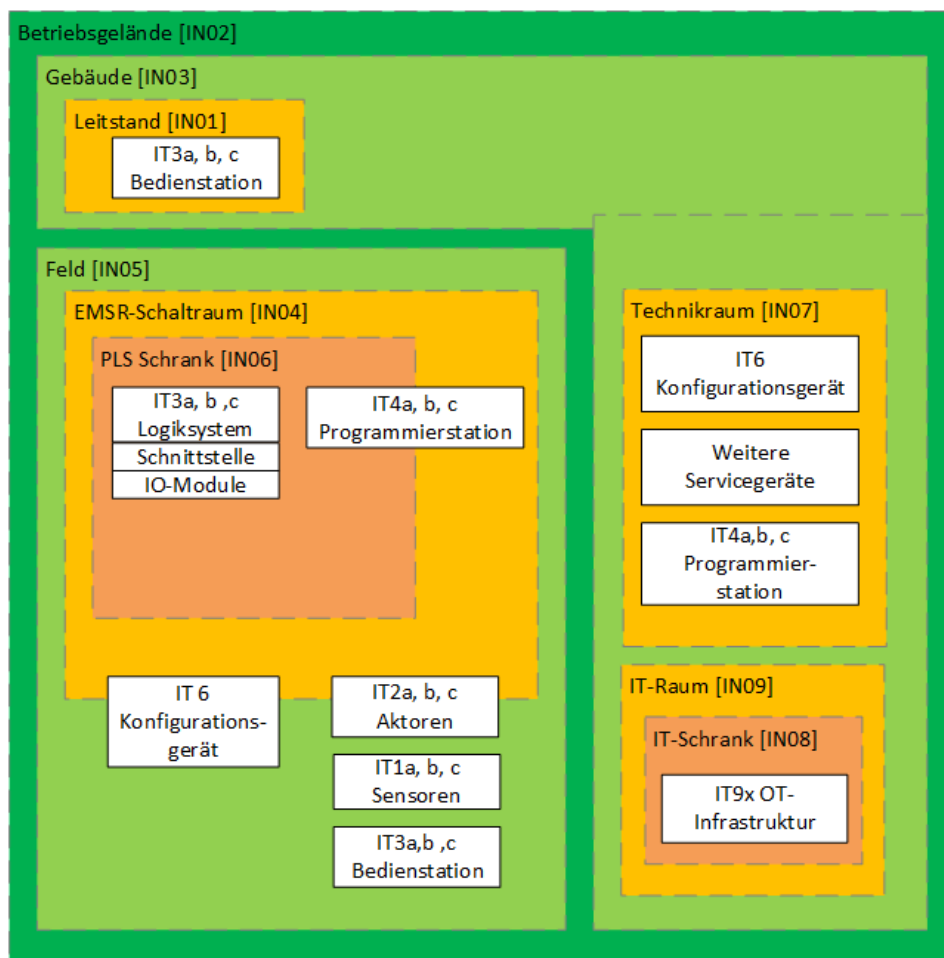


Abbildung 4 Darstellung eines Infrastrukturmodells mit einer Zuordnung von Infrastruktur und Komponenten

In Abbildung 4 werden Zielobjekt-Zuordnung zu Räumen und Gebäuden sowie eine farbliche Darstellung der infrastrukturellen Zonenübergänge dargestellt. Diese gehen meist mit einer Einschränkung des Personenkreises mit Zutrittsrechten einher.

Die Komponenten IT2 und IT6 sind auf der Grenze zwischen Feld und EMSR-Schaltraum platziert, um zu zeigen, dass diese sowohl in dem einen als auch dem anderen Bereich anzutreffen sind. Gleiches gilt für IT4.

7.1.2 Untersuchungsgegenstand

Tabelle 3 Räume und Schränke, die für die Modellarchitektur relevant sind

ID	Zielobjekt	Beschreibung
IN01	Leitstand	Räumlichkeit, in der die Bedienstationen teilweise oder komplett aufgestellt sind. Von diesem Raum aus beobachtet und steuert das Bedienpersonal die Chemieanlage.
IN02	Betriebsgelände	Gelände, welches alle Infrastrukturen beherbergt. Gelände ist eingefriedet und mit einem Pfortnerdienst gesichert.

ID	Zielobjekt	Beschreibung
IN03	Gebäude	Nicht näher spezifizierte Behausung für den Leitstand und Technikraum.
IN04	EMSR-Schaltraum	Räumlichkeit, in der die verbauten Komponenten sowohl aus der Kategorie MSR-Raum, als auch aus der Kategorie E-Schaltraum sind.
IN05	Feld	Als Feld wird der Bereich der Anlage bezeichnet, in dem sich das verfahrenstechnische Equipment der Produktionsanlage (u.a. Behälter, Rohrleitungen und Feldgeräte) befindet. Dies kann ein Gebäude aber auch den Außenbereich umfassen.
IN06	PLS-Schrank	Schrank, in dem die Logiksysteme, IO-Ebene oder sonstige Komponenten zur Signalerfassung und Verarbeitung verbaut sind. Hiermit sind ebenso offene PLS-Schränke, sogenannte PLS-Racks, gemeint.
IN07	Technikraum	In diesem Raum werden Konfigurationsgeräte, weitere Servicegeräte oder Programmierstationen (sofern diese mobile eingesetzt werden können) gelagert.
IN08	IT-Schrank	Schrank, in dem IT-Komponenten verbaut sind, wie. Z.B. Rechner, Netzwerkkomponenten oder KVM.
IN09	IT-Raum	Komponenten der OT-Infrastruktur IT9.x

7.1.2.1 Unterbringung der Schränke

Der PLS-Schrank kann im EMSR-Schaltraum sowie im Feld untergebracht sein. Als Referenz wird der EMSR-Schaltraum angenommen.

Als Verwahrungsort der mobilen Servicegeräte wird der Technikraum IN07 angenommen, zu dem ausschließlich Personal der EMSR-Technik Zutritt haben. Der Technikraum beherbergt entweder einen separaten verschließbaren Technikschränk oder wird bei Verlassen abgeschlossen.

7.1.3 Zuordnung der Zielobjekte und Schränke zu den Räumen

Die Zielobjekte OT-/IT-Hardware können sich in mehreren Räumen befinden. Für die Risikobetrachtung ist es grundsätzlich notwendig, eine eindeutige Zuordnung vorzunehmen, da diese Zuordnung zu unterschiedlichen Schutzniveaus führen kann.

Sensoren (IT1a, IT1b, IT1c) finden sich überwiegend im Feld wieder.

Aktoren (IT2a, IT2b, IT2c) setzen Steuerungsanweisungen um. Sie sind daher vorrangig im Feld zu finden. Aber auch im E-Raum übernehmen sie wesentliche Aufgaben. Zum Beispiel sind in diesem Raum Motorschütze für Pumpen untergebracht. Es werden bei der Risikobetrachtung nur Sensoren im Feld betrachtet, da diese leichter zugänglich sind.

Logiksysteme (IT3a, IT3b oder IT3c) sind im PLS-Schrank untergebracht, der im EMSR-Raum steht. Kleinere Logiksysteme und dezentralen I/O-Peripheriegeräte für das PLT-S im Feld sind gegen Zugriff Unbefugter zu sichern (z. B. abgeschlossene Feldinstallation).

Programmierstationen (IT 4a, IT4b, IT4c) werden im PLS-Schrank aufbewahrt (und werden bei Bedarf entnommen) oder sind im EMSR-Raum fest aufgestellt.

Bedienstationen (IT5a, IT5b, IT5c) befinden sich zur Steuerung zentral im Leitstand. Eine zusätzliche Verwendung direkt im Feld ist jedoch gängig. Beide Situationen werden betrachtet, da sich unterschiedliche Gefährdungsszenarien aus diesen ergeben. Dies folgt aus der Gegebenheit, dass in der Leitwarte mehrere Bedienstationen zugänglich sind, während ein Gerät im Feld leichter zugänglich ist.

Die Konfigurationsgeräte (IT6 und IT7) und Servicegeräte werden im Technikraum gelagert und werden für die Modellarchitekturen als mobile Geräte angenommen.

8 Auswahl relevanter Bausteine

Die Auswahl der Bausteine bezieht sich auf der IT-Grundschutzkompendium Version 2023. In den folgenden Tabellen werden alle Bausteine den einzelnen Zielobjekten zugeordnet. Es werden nur die Bausteine ausgewählt, die für eine Mehrheit der Anlagen zur Anwendung kommen. Bei der konkreten Umsetzung sind ggf. zusätzliche Bausteine zu wählen (z.B. bei BDIS wird als allgemeiner Server (Baustein SYS.1.1) modelliert. Weitere Bausteine zu Betriebssystem und ggf. Anwendungen sind selbst zu ergänzen). Ebenso kann bei der konkreten Umsetzung auf Grundlage einer systemischen Risikobeurteilung auf die Umsetzung von bausteinspezifischen Anforderungen verzichtet werden.

8.1 Prozess-Bausteine

Die folgenden Prozess-Bausteine sind auf den Informationsverbund anzuwenden. Wenn nicht anders angegeben, müssen alle Basis- und Standard-Anforderungen der Bausteine auf geeignete Weise erfüllt werden.

Um grundlegende Risiken abzudecken und eine ganzheitliche Informationssicherheit aufzubauen, müssen die essenziellen Sicherheitsanforderungen frühzeitig erfüllt und entsprechende Sicherheitsmaßnahmen umgesetzt werden. Daher wird im IT-Grundschutz mit R1, R2 und R3 eine Reihenfolge für die umzusetzenden Bausteine vorgeschlagen (siehe (1) Modellierung und Bearbeitungsreihenfolge der Bausteine).

- R1: Diese Bausteine sollten vorrangig umgesetzt werden, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden.
- R2: Diese Bausteine sollten als nächstes umgesetzt werden, da sie in wesentlichen Teilen des Informationsverbundes für nachhaltige Sicherheit erforderlich sind.
- R3: Diese Bausteine werden zur Erreichung des angestrebten Sicherheitsniveaus ebenfalls benötigt und müssen umgesetzt werden. Es wird empfohlen, diese erst nach den anderen Bausteinen zu betrachten.

Tabelle 4 Relevante Prozessbausteine

Baustein	Priorität	Umsetzung
ISMS.1 ISMS(Sicherheitsmanagement)	R1	Folgende Anforderung muss über die Basis- und Standard-Anforderungen erfüllt werden: •ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien
ORP.1 Organisation	R1	
ORP.2 Personal	R1	
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	R1	
ORP.4 Identitäts- und Berechtigungsmanagement	R1	
ORP.5 Anforderungsmanagement (Compliance)	R3	
CON.1 Kryptokonzept	R3	
CON.2 Datenschutz	R2	Im Kontext von 12. BImSchV nicht relevant. Kontext von personenbezogenen Daten der Mitarbeiter ist zu prüfen.
CON.3 Datensicherungskonzept	R1	
CON.6 Löschen und Vernichten	R1	

Baustein	Priorität	Umsetzung
CON.7 Informationssicherheit auf Auslandsreisen	N/A	Sensible Informationen werden nicht auf Dienstreisen mitgeführt
CON.8 Software-Entwicklung	R3	Anzuwenden, wenn eigene Entwicklung stattfindet
CON.9 Informationsaustausch	R3	
CON.10 Entwicklung von Webanwendungen	R3	Anzuwenden, wenn eigene Entwicklung von Webanwendungen stattfindet
OPS.1.1.2 Ordnungsgemäße IT-Administration	R1	
OPS.1.1.3 Patch- und Änderungsmanagement	R1	
OPS.1.1.4 Schutz vor Schadprogrammen	R1	
OPS.1.1.5 Protokollierung	R1	
OPS.1.1.6 Software-Tests und -Freigaben	R1	
OPS.1.1.7 Systemmanagement	R2	
OPS.1.2.2 Archivierung	R3	
OPS.1.2.4 Telearbeit	R2	Anzuwenden, wenn ein Zugriff auf die Anlage über Telearbeitsplätze möglich ist.
OPS.1.2.5 Fernwartung	R3	
OPS.1.2.6 NTP – Zeitsynchronisation	R2	
OPS.2.1 Outsourcing für Kunden	R2	
OPS.2.2 Cloud-Nutzung	R2	
OPS.3.1 Outsourcing für Dienstleister	R2	Anzuwenden, wenn Dienstleistungen für andere Betreiber angeboten werden.
DER.1 Detektion von sicherheitsrelevanten Ereignissen	R1	
DER.2.1 Behandlung von Sicherheitsvorfällen	R1	
DER.2.2 Vorsorge für die IT-Forensik	R3	
DER.2.3 Bereinigung weitreichender Sicherheitsvorfällen	R3	
DER.3.1 Audits und Revisionen	R2	
DER.3.2 Revisionen auf Basis des Leitfadens	N/A	Der Leitfaden IS-Revision erfüllt nicht die Anforderungen, die für eine Nachweisprüfung nach §8a BSIG notwendig sind
DER.4 Notfallmanagement	R3	

Diese Kennzeichnung zeigt eine sinnvolle zeitliche Reihenfolge für die Umsetzung der Anforderungen des jeweiligen Bausteins auf und stellt keine Gewichtung der Bausteine untereinander dar. Grundsätzlich müssen alle für den jeweiligen Informationsverbund relevanten Bausteine des IT-Grundschutz-Kompends umgesetzt werden.

8.2 System-Bausteine

Darüber hinaus sind alle Bausteine umzusetzen, die sich im Rahmen der Anwendung der IT-Grundschutz-Vorgehensweise, insbesondere bei der Modellierung des Informationsverbunds, ergeben.

Die folgenden obligatorischen System-Bausteine sind auf die genannten Zielobjekte (siehe Referenzarchitektur) anzuwenden. Wenn nicht anders angegeben, müssen alle Basis- und Standard-Anforderungen der Bausteine erfüllt werden.

8.2.1 APP: Anwendungen

Tabelle 5 System-Bausteine APP

Baustein	Relevant	Komponenten⁶
APP.1.1 Office-Produkte	Ja, ggf. im Rahmen von speziellen Anwendungen	IT4a PLT-S-Programmierstation IT4b PLT-B-Programmierstation IT4c PLT-S/PLT-B-Programmierstation IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT6 Konfigurationsgerät IT 7 Servicegerät IT8 BDIS IT9x OT-Infrastruktur
APP.1.2 Webbrowser	Ja	IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmierstation IT4b PLT-B-Programmierstation IT4c PLT-S/PLT-B-Programmierstation IT6 Konfigurationsgerät IT7 Servicegerät
APP.1.4 Mobile Anwendung (Apps)	Ja	IT6 Konfigurationsgerät IT7 Servicegerät
APP.2.1 Allgemeiner Verzeichnisdienst	Ja	IT9g Verzeichnisdienst
APP.2.2 Active Directory	Ja, ggf. im Rahmen von speziellen Anwendungen	IT9g Verzeichnisdienst
APP.2.3 OpenLDAP	Ja, ggf. im Rahmen von speziellen Anwendungen	IT9g Verzeichnisdienst
APP.3.1 Webanwendungen und Webservices	Ja, ggf. im Rahmen von speziellen Anwendungen	IT8 BDIS IT9x OT-Infrastruktur
APP.3.2 Webserver	Ja, ggf. im Rahmen von speziellen Anwendungen	IT8 BDIS IT9x OT-Infrastruktur
APP.3.3 Fileserver	Ja	IT9c Dateiaustausch

⁶ Sofern ein Zuordnen eines Bausteins zu einer Komponente in der OT-Infrastruktur möglich war, wird „IT9x OT-Infrastruktur“ verwendet. Dies bedeutet, dass dies für alle Komponenten der OT-Infrastruktur relevant sein kann.

Baustein	Relevant	Komponenten⁶
APP.3.4 Samba	Ja, ggf. im Rahmen von speziellen Anwendungen	IT9c Dateiaustausch
APP.3.6 DNS-Server	Ja, ggf. im Rahmen von speziellen Anwendungen	IT9h Weitere Dienste
APP.4.2 SAP-ERP-System	Ja, ggf. im Rahmen von speziellen Anwendungen	IT9e ERP-System
APP.4.3 Relationale Datenbanksysteme	Ja, ggf. im Rahmen von speziellen Anwendungen	IT8 BDIS IT9h Weitere Dienste
APP.4.4 Kubernetes	Ja	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur
APP.4.6 SAP ABAP-Programmierung	Nein	
APP.5.2 Microsoft Exchange und Outlook	Nein	
APP.5.3 Allgemeiner E-Mail-Client und -Server	Nein	
APP.7 Entwicklung von Individualsoftware	Ja, ggf. im Rahmen von speziellen Anwendungen	IT8 BDIS IT9x OT-Infrastruktur

8.2.2 SYS: IT-Systeme

Tabelle 6 System-Bausteine SYS

Baustein	Relevant	Komponenten⁷
SYS.1.1 Allgemeiner Server	Ja	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur
SYS.1.2.2 Windows Server 2012	Ja, ggf. im Rahmen von speziellen Anwendungen	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur

⁷ Sofern ein Zuordnen eines Bausteins zu einer Komponente in der OT-Infrastruktur möglich war, wird „IT9x OT-Infrastruktur“ verwendet. Dies bedeutet, dass dies für alle Komponenten der OT-Infrastruktur relevant sein kann.

Baustein	Relevant	Komponenten⁷
SYS.1.3 Server unter Linux und Unix	Ja, ggf. im Rahmen von speziellen Anwendungen	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur
SYS.1.5 Virtualisierung	Ja	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur
SYS.1.6 Containerisierung	Ja	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT8 BDIS IT9x OT-Infrastruktur
SYS.1.7 IBM Z	Nein	
SYS.1.8 Speicherlösungen	Ja	IT9x OT-Infrastruktur
SYS.2.1 Allgemeiner Client ⁸	Ja	IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmiersstation IT4b PLT-B-Programmiersstation IT4c PLT-S/PLT-B-Programmiersstation IT6 Konfigurationsgerät IT7 Servicegerät
SYS.2.2.2 Clients unter Windows 8.1 (wurde gestrichen)	Ja, ggf. im Rahmen von speziellen Anwendungen	Siehe Allgemeiner Client
SYS.2.2.3 Clients unter Windows ⁹	Ja, ggf. im Rahmen von speziellen Anwendungen	Siehe Allgemeiner Client
SYS.2.3 Clients unter Linux und Unix	Ja, ggf. im Rahmen von speziellen Anwendungen	Siehe Allgemeiner Client
SYS.2.4 Clients unter MacOS	Ja, ggf. im Rahmen von speziellen Anwendungen	Siehe Allgemeiner Client

⁸ Der Baustein wurde überarbeitet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Drafts/Final-Drafts/final_drafts_node.html

⁹ Es gibt aktuelle Hilfsmittel zu Umsetzung unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Hilfsmittel_Anforderungen_des_IT_Grundschutzes_fuer_Windows_10.html

Baustein	Relevant	Komponenten⁷
SYS.3.1 Laptops	Ja	IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmierstation IT4b PLT-B-Programmierstation IT4c PLT-S/PLT-B-Programmierstation IT6 Konfigurationsgerät IT7 Servicegerät
SYS.3.2.1 Allgemeine Smartphones und Tablets	Ja	IT6 Konfigurationsgerät IT7 Servicegerät
SYS.3.2.2 Mobile Device Management (MDM)	Ja	IT9h weitere Dienste
SYS.3.2.3 iOS (for Enterprise)	Ja	IT6 Konfigurationsgerät IT7 Servicegerät
SYS.3.2.4 Android	Ja	IT6 Konfigurationsgerät IT7 Servicegerät
SYS.3.3 Mobiltelefon	Ja	IT6 Konfigurationsgerät IT7 Servicegerät
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	Ja	IT9x OT-Infrastruktur
SYS.4.3 Eingebettete Systeme	Ja, sofern nicht über IND abgedeckt	IT1a PLT-S-Sensor IT1b PLT-B-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2b PLT-B-Aktor IT2c PLT-S/PLT-B-Aktor
SYS.4.4 Allgemeines IoT-Gerät	Ja, sofern nicht über IND abgedeckt	IT1a PLT-S-Sensor IT1b PLT-B-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2b PLT-B-Aktor IT2c PLT-S/PLT-B-Aktor
SYS.4.5 Wechseldatenträger	Ja	IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmierstation IT4b PLT-B-Programmierstation IT4c PLT-S/PLT-B-Programmierstation IT6 Konfigurationsgerät IT7 Servicegerät IT 9x OT-Infrastruktur

8.2.3 IND: Industrielle IT

Tabelle 7 System-Bausteine IND

Baustein	Relevant	Komponenten
IND.1 Prozessleit- und Automatisierungstechnik	Ja	Übergreifend
IND.2.1 Allgemeine ICS-Komponente	Ja	IT1a PLT-S-Sensor IT1b PLT-B-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2b PLT-B-Aktor IT2c PLT-S/PLT-B-Aktor IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT5a PLT-S-Bedienstation IT5b PLT-B-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmiersstation IT4b PLT-B-Programmiersstation IT4c PLT-S/PLT-B-Programmiersstation IT6 Konfigurationsgerät IT7 Servicegerät
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	Ja	IT3a PLT-S-Logiksystem IT3b PLT-B-Logiksystem IT3c PLT-S/PLT-B-Logiksystem
IND.2.3 Sensoren und Aktoren	Ja	IT1a PLT-S-Sensor IT1b PLT-B-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2b PLT-B-Aktor IT2c PLT-S/PLT-B-Aktor
IND.2.4 Maschine	Ja	Anwendung auf komplexere Teile einer Anlage IT1a PLT-S-Sensor IT1b PLT-B-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2b PLT-B-Aktor IT2c PLT-S/PLT-B-Aktor

Baustein	Relevant	Komponenten
IND.2.7 Safety Instrumented Systems	Ja	IT1a PLT-S-Sensor IT1c PLT-S/PLT-B-Sensor IT2a PLT-S-Aktor IT2c PLT-S/PLT-B-Aktor IT3a PLT-S-Logiksystem IT3c PLT-S/PLT-B-Logiksystem IT5a PLT-S-Bedienstation IT5c PLT-S/PLT-B-Bedienstation IT4a PLT-S-Programmiersstation IT4c PLT-S/PLT-B-Programmiersstation IT6 Konfigurationsgerät IT7 Servicegerät
IND.3.2 Fernwartung im industriellen Umfeld	Ja	IT9b Sprungserver

8.2.4 NET: Netze und Kommunikation

Tabelle 8 System-Bausteine NET

Baustein	Relevant	Komponenten
NET.1.1 Netzarchitektur und -design	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.1.2 Netzmanagement	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.2.1 WLAN-Betrieb	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.2.2 WLAN-Nutzung	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.3.1 Router und Switches	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.3.2 Firewall	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.3.3 VPN	Ja	IT9h OT-Infrastruktur IT10 IT-Infrastruktur
NET.4.1 TK-Anlagen	Nein	
NET.4.2 VoIP	Nein	
NET.4.3 Faxgeräte und Faxserver	nein	

8.2.5 INF: Infrastruktur

Tabelle 9 System-Bausteine INF

Baustein	Relevant	Komponenten
INF.1 Allgemeines Gebäude	Ja	IN01 Leitwarte IN02 Betriebsgelände IN03 Gebäude IN04 EMSR-Schaltraum IN05 Feld
INF.2 Rechenzentrum sowie Serverraum	Ja	IN08 IT-Raum
INF.5 Raum sowie Schrank für technische Infrastruktur	Ja	IN04 EMSR-Schaltraum IN06 PLS-Schrank IN07 Technikraum
INF.6 Datenträgerarchiv	Nein	IN08 IT-Raum
INF.7 Büroarbeitsplatz	Anwendbarkeit für Leitwarte ist im Einzelfall zu prüfen	IN01 Leitwarte
INF.8 Häuslicher Arbeitsplatz	Ja, falls ein Zugriff auf die Anlage möglich ist	IN01 Leitwarte
INF.9 Mobiler Arbeitsplatz	Ja, falls ein Zugriff auf die Anlage möglich ist	IN01 Leitwarte
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum	Anwendbarkeit für Leitwarte ist im Einzelfall zu prüfen	IN01 Leitwarte
INF.11 Allgemeines Fahrzeug	Nein	
INF.12 Verkabelung	Ja	Übergreifend
INF.13 Technisches Gebäudemanagement	Ja	Übergreifend
INF.14 Gebäudeautomation	Ja	IN03 Gebäude

9 Restrisikobetrachtung/Risikobehandlung

9.1 Analyse und Definition der Restrisiken

Unterschieden werden muss zwischen generischen und spezifischen Restrisiken:

- **Generische Restrisiken**
Das sind Risiken, welche per Definition der Maßnahmenkataloge typischerweise auch nach deren Umsetzung teilweise oder in Gänze bestehen bleiben. Maßnahmenkataloge repräsentieren häufig die Mindestanforderungen. Die Gründe hierfür liegen zumeist in der Definition der Maßnahmenkataloge. Diese sind in der Komplexität und Tiefe der Maßnahmen, als auch in der Breite der abgedeckten Szenarien häufig ein Mittelmaß. Dieses soll den größtmöglichen Teil der Risiken über alle Einrichtungen und Betriebe in dem gewählten Bereich minimieren.
Ein wichtiger, differenzierender Faktor für generische Restrisiken ist, dass diese bereits im Vorfeld anhand der Definition der Maßnahmenkataloge abgeleitet werden können und somit für alle Betriebe bzw. Bereiche definierbar sind. Typischerweise werden generische Restrisiken mit der Entwicklung der Maßnahmenkataloge definiert und mit der Abnahme und Inkraftsetzung dieser durch entsprechende Gremien und Funktionen (siehe Abschnitt 9.3 Ausnahmeprozesse) akzeptiert bzw. mitigierende Maßnahmen werden ergriffen (siehe Abschnitt 9.2 Mitigierende Maßnahmen zur Restrisikobehandlung).
- **Spezifische Restrisiken**
Hierunter fallen Risiken, welche anhand der spezifischen Herausforderungen und Risiken der gewählten Betriebe und Bereiche auch nach Implementierung der Maßnahmenkataloge noch bestehen bleiben, jedoch im Gegensatz zu den generischen Restrisiken, spezifisch für den jeweiligen Bereich bzw. Betrieb sind. Alternativ lassen spezifische Gegebenheiten eine Umsetzung von bestimmten Maßnahmen nicht zu.
Diese Restrisiken lassen sich in der Regel nicht im Vorfeld aus den Maßnahmenkatalogen ableiten, sondern meist lediglich durch Risikoanalysen oder Assessments in einzelnen Bereichen bzw. Betrieben aufdecken. Spezifische Restrisiken sind in der Regel nicht übertragbar auf andere Bereiche bzw. Betriebe. Die Ursache spezifischer Restrisiken liegen im Vergleich zu den generischen Restrisiken meist weniger in der Definition der Maßnahmenkataloge, sondern in den spezifischen Anforderungen und Gegebenheiten einzelner Bereiche bzw. Betriebe. Spezifische Restrisiken werden zumeist erst nach der Implementierung der Maßnahmenkataloge erkannt und müssen nach Erkennung entweder durch entsprechende mitigierende Maßnahmen (siehe Abschnitt 9.2 Mitigierende Maßnahmen zur Restrisikobehandlung) beseitigt werden oder aber bedürfen einer Ausnahmeregelung, welche durch entsprechende Prozesse erteilt werden kann (siehe Abschnitt 9.3 Ausnahmeprozesse).

9.2 Mitigierende Maßnahmen zur Restrisikobehandlung

Im Kontext der Restrisikobetrachtung ist zu überprüfen, ob das Risiko in einer Risikotoleranz der Institution entsprechenden Weise behandelt wurde. Das passiert in der Regel durch Erfüllung von Mindestanforderungen, die beispielsweise in Anforderungskatalogen oder Richtlinien und organisationsinternen Standards definiert sind, z. B. indem Schwachstellen und/oder Bedrohungen abgestellt oder Auswirkungen abgeschwächt wurden.

Ist eine Umsetzung der Mindestanforderungen nicht möglich, ist die Umsetzung anderer Maßnahmen (compensating measures) zu prüfen, um das verbleibende Restrisiko zu reduzieren. Beispiele für solche kompensierenden Gegenmaßnahmen sind:

- Wenn man ein System nicht aktualisieren kann, dann kann es in ein eigenes Netzsegment mit vorgeschalteter DMZ platziert werden.
- Wenn man ein bestimmtes Kommunikationsprotokoll in der Firewall nicht unterbinden kann, kann der Netzwerkverkehr über den zugehörigen Port überwacht werden.

- Wenn man keine personalisierten Accounts anlegen kann, können Schichttagebücher helfen, das Restrisiko organisatorisch zu kompensieren.

Kompensierende Gegenmaßnahmen sind keinesfalls Ausnahmen von den Mindestanforderungen und Maßnahmenkatalogen oder ein Verzicht auf diese. Vielmehr sind es Maßnahmen zur zusätzlichen Absicherung oder Gegenmaßnahmen, die helfen die ursprüngliche Intention der im Einzelfall nicht umsetzbaren Mindestanforderungsmaßnahme zu erreichen.

Kompensierende Gegenmaßnahmen können auch helfen, die Mindestanforderungsmaßnahmen zu erweitern. Es gibt Organisationen, die einen eigenen Katalog solcher „Enhanced Security Controls“ haben. Das ist gerade in der OT-Security angeraten, weil sich so signifikant Aufwände und Zeit im erforderlichen Fall sparen lassen.

Unabhängig davon sind kompensierende Gegenmaßnahmen häufig ein Kompromiss zwischen dem zu akzeptierenden Risiko und der Benutzbarkeit (usability) oder der Funktionalität. Daher sollte die Entscheidung für oder gegen eine kompensierende Gegenmaßnahme immer im Kontext der Funktion oder des Anwendungsfalles stehen, in welchem das zu betrachtende System eingebunden ist (im Sinne „wer macht was wann mit welchem System zu welchem Zweck?“). Auf diese Weise ist die Entscheidung, wieviel Restrisiko tolerierbar und welche Funktionalität verzichtbar ist, am besten im Sinne einer informierten Entscheidung, also frei von Emotionen und Befindlichkeiten in angemessenem Aufwand zu treffen.

Weiterführende Informationen sind in (2) sowie insbesondere zur Thematik „Enhanced Security Controls“ im Abschnitt „tailoring controls“ in (3) zu finden.

9.3 Ausnahmeprozesse

Für die OT-Security ist die Etablierung eines OT-Security Management Systems (OTSMS) unerlässlich, welches in den Betrieben durch den Betreiber umzusetzen ist und dessen Rahmenbedingungen durch das OT-Security Regelwerk definiert werden (siehe (1) IND1.A1 Einbindung in die Sicherheitsorganisation).

Die relevanten Rollen müssen dabei zentral, oder, je nach Unternehmensgröße, durch die jeweiligen Managementeinheiten zugewiesen werden. Dabei muss sichergestellt sein, dass miteinander im Zielkonflikt stehende Rollen bzgl. OT-Security getrennt sind (siehe (1) ISMS.1 Sicherheitsmanagement und (1) IND.1.A1 Einbindung in die Sicherheitsorganisation).

Das Ziel dieser OT-Security Organisation ist die Sicherstellung der Umsetzung der OT-Security Vorgaben. Aus ihnen soll sich ein benanntes Expertengremium zusammensetzen, welches Ausnahmen genehmigen kann. Alle Ausnahmen, die nicht eindeutig einer Managementeinheit (falls vorhanden) zugeordnet werden können, müssen zentral genehmigt werden.

Das Expertengremium ist dabei sowohl für Ausnahmen gegenüber dem OTSMS (Compliance Ausnahmen), als auch für Ausnahmen, die sich aus der Risikoanalyse (wenn das Restrisiko auch nach Umsetzung aller mitigierender Maßnahmen höher als das akzeptable Risiko ist) ergeben (Risiko Ausnahmen) zuständig (siehe auch (1) ORP.5.A5 Ausnahmegenehmigungen).

Die Genehmigung der Ausnahmen erfolgt durch das Expertengremium, in Zusammenarbeit mit dem betroffenen Betreiber. Dabei müssen folgende Punkte geklärt und dokumentiert werden:

- Wurden alle umsetzbaren mitigierenden Maßnahmen bereits umgesetzt?
- Warum wurden ggf. einzelne Maßnahmen nicht / nicht vollständig umgesetzt?
- Wodurch die kompensierende Gegenmaßnahme tauglich ist, um eine der Mindestanforderung oder dem Risiko gegenüberstehende, äquivalente Absicherung zu erreichen?
- Wie soll die Sicherheit nach Ablauf der Ausnahmedauer umgesetzt werden?
- Ist sich der Betreiber über das Ausmaß der Risiken bewusst und akzeptiert er diese?

- Alle Ausnahmen müssen zeitlich begrenzt erteilt werden. Nach Ablauf des Ausnahmezeitraums muss durch das Expertengremium erneut geprüft werden, ob die Gründe für die Ausnahme weiterhin bestehen. Dabei ist zu prüfen:
- Gibt es mitigierende Maßnahmen, die bisher noch nicht in Betracht gezogen wurden
- Gibt es neue Bedrohungen und / oder Schwachstellen, durch die das Risiko anders bewertet werden muss
- Gibt es einen Zeitplan, um die Risiken zu beseitigen
- Alle erteilten Ausnahmen müssen zentral gespeichert werden, um Sicherzustellen, dass die regelmäßige Neubetrachtung stattfindet.
- Im Ereignisfall konsultiert werden zu können
- Die Verantwortlichkeiten klar zu dokumentieren

10 Unterstützende Informationen

Für diese Arbeit wurden folgende Dokumente verwendet:

KAS-38 Bericht des Ausschusses Erfahrungsberichte Auswertung der Erfahrungsberichte über Prüfungen der Sachverständigen im Sinne von § 29a BImSchG im Jahr 2014 und Veranstaltungen zum Meinungs- und Erfahrungsaustausch, <https://www.kas-bmu.de/kas-berichte.html>

KAS-51 Leitfaden des Arbeitskreises Eingriffe Unbefugter "Maßnahmen gegen Eingriffe Unbefugter" <https://www.kas-bmu.de/nachricht/kas-51.html>

TRBS 1115 Teil 1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen, <https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html>

NA 163 IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen, 2024-11-23, <https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html>

NE 165 PLT-Betriebseinrichtungen mit Sicherheitsfunktion, 2019-12-13, <https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html>

NA 169 Automation Security Management in der Prozessindustrie, 2019-12-19, <https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html>

VDI 2180 Blatt 1 – 4 Funktionale Sicherheit in der Prozessindustrie, <https://www.vdi.de/richtlinien>

VDI 2182 Blatt 4 - Informationssicherheit in der industriellen Automatisierung - Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen, 2020-04, <https://www.vdi.de/richtlinien>

IEC TR 63069 - Industrial-process measurement, control and automation - Framework for functional safety and security

Der technische Bericht enthält Leitlinien für die Bewertung und das Management von Risiken der funktionalen Sicherheit und der Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen. Er unterstützt Organisationen bei der Identifizierung und Bewertung potenzieller Gefahren und Bedrohungen, die sich aus dem Zusammenspiel von Safety und Cybersecurity ergeben. IEC TR 63069 unterstützt Organisationen bei der Implementierung von Risikomanagementprozessen, um sowohl Safety- als auch Cybersecurity auf koordinierte und integrierte Weise anzugehen.

IEC TR 63074 - Safety of machinery - Security aspects related to functional safety of safety-related control systems

Der technische Bericht enthält Leitlinien zu den Lebenszyklusaspekten der Integration von Safety und Cybersecurity in industriellen Automatisierungs- und Steuerungssystemen. Er behandelt die Beziehungen zwischen dem Safety-Lebenszyklus aus IEC 61511 und dem Cybersecurity-Lebenszyklus aus IEC 62443. Das Dokument soll Institutionen dabei helfen, potenzielle Konflikte zwischen Safety- und Cybersecurity Anforderungen zu identifizieren und zu managen, um sicherzustellen, dass beide Aspekte effektiv und koordiniert behandelt werden.

ISA TR 84.00.9-2017 - Cybersecurity Related to the Functional Safety Lifecycle

ISA TR 84.00.9 enthält Leitlinien für die Einbeziehung von Überlegungen zur Cybersicherheit in den Lebenszyklus der funktionalen Sicherheit von sicherheitsgerichteten Systemen (PLT-S), die in industriellen Prozessbereichen eingesetzt werden.

Das Hauptziel von ISA TR 84.00.9 ist es, sicherzustellen, dass die Integrität und Zuverlässigkeit von sicherheitsgerichteten Systemen nicht durch Cybersecurity-Bedrohungen beeinträchtigt wird. Die Norm trägt der zunehmenden Vernetzung und Digitalisierung industrieller Steuerungssysteme

Rechnung, die neue Risiken für die Cybersicherheit mit sich bringen, welche die funktionale Sicherheit dieser Systeme beeinträchtigen können.

ISA TR 84.00.9 steht in Zusammenhang mit den Normen IEC 61508 und IEC 61511, die die Anforderungen an die funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer sicherheitsrelevanter Systeme definieren. Der Bericht bietet praktische Anleitungen zur Integration von Cybersecurity-Maßnahmen in den Lebenszyklus der funktionalen Sicherheit von sicherheitsgerichteten Systemen unter Einhaltung dieser Normen.

11 Anhang

11.1 Anhang A Schutzbedarfszuweisungen für chemische Produktionsanlagen

11.1.1 Auswirkung auf PLT-S

Zur Kategorisierung von Auswirkungen kompromittierter PLT-S wird NA 163 mit Tabelle 10 herangezogen. Die Deaktivierung der PLT-Sicherheitsfunktion (SIF), welche als A2 bezeichnet wird, ist grundsätzlich bei jeder PLT-S möglich. Abhängig von der Realisierung der SIF erfordert der vorsätzlich herbeigeführte Anforderungsfall die Kompromittierung weiterer Komponenten. Dies entfällt, wenn beispielsweise die Steuerungsbefehle an den Aktor über das PLT-S-Logiksystem geleitet werden. Durch das Setzen auf „offen“ an allen Ausgängen des PLT-S-Logiksystems kann der Anforderungsfall bereits eintreten¹⁰ (siehe Variante III in 11.2.2 IT2 - Aktor). Die Kategorie A3 ergibt sich aus der Kompromittierung mehrerer separierter Komponenten oder einer gemeinsam genutzten Komponente. Ein weiteres Beispiel stellt die Manipulation der Messwerte des Sensors bei gemeinsamer Nutzung durch PLT-S und PLT-B dar (siehe 11.2.1 IT1 - Sensor, 11.2.2 IT2 - Aktor und 11.2.3 IT3 - Logiksysteme).

Tabelle 10 Kategorisierung von Auswirkungen kompromittierter PLT-S aus [NA 163]

Auswirkung	Beschreibung	Auswirkung
A1	SIF löst ohne Anforderung.	Nicht gefährlich im Sinne der Funktionalen Sicherheit, kann aber zu Betriebsunterbrechung führen.
A2	SIF ist deaktiviert. Auslösung findet nicht gezielt statt. Allerdings: ein nicht akzeptables Ereignis würde erst dann eintreten, wenn der Anforderungsfall eintritt.	gefährlich
A3	SIF ist deaktiviert und gleichzeitiges Herbeiführen des Anforderungsfalles (z.B. durch Manipulation der PLT-B) führt sofort zu einem nicht akzeptablen Ereignis.	gefährlich

Die Auswirkung A1 hat die Überführung des Produktionsprozesses in einen sicheren Zustand zur Folge obwohl die Prozessbedingungen dies nicht notwendig machen. Die PLT-S löst fälschlicherweise aus (False Positive). Dies kann beispielsweise durch eine Verschiebung der Grenzwerte in der PLT-S-Logik „zur sicheren Seite“, nicht Verfügbarkeit von Messwerten des Sensors oder einem DoS Angriff gegen das PLT-S-Logiksystem erreicht werden. Diese Auswirkung kann je nach Häufigkeit und Art des Produktionsprozesses finanziell beträchtliche oder gar existenzbedrohende Ausmaße annehmen. Die Wirksamkeit der Sicherheitsfunktion bleibt jedoch davon unberührt. Daher wird diese Auswirkung bei der Gefährdungsbetrachtung in 11.2 Anhang B Gefährdungsbetrachtung der Komponenten zwar miteinbezogen und mögliche Szenarien dafür aufgezeigt, diese werden jedoch weder hinsichtlich der Komplexität bewertet noch Anforderungen empfohlen. Zudem gilt zu beachten, dass diese Auswirkung auch durch Manipulation des Produktionsprozesses erreicht werden kann. Sollte der Betreiber sich gegen diese Auswirkung schützen wollen ist der Geltungsbereich entsprechend zu fassen und Maßnahmen nicht nur für die PLT-S zu treffen.

Die Auswirkung A2 führt dazu, dass die PLT-S bei einem Anforderungsfall nicht auslöst (False Negative). Ein schadenswirksamer Erfolg einer solchen Manipulation ist von einem Zufallsereignis, welches den

¹⁰ Es wird vereinfacht angenommen, dass stets genug kritische Prozessmasse vorliegt, um den Anforderungsfall auszulösen. Andernfalls sind weitere Manipulationen notwendig.

Anforderungsfall auslöst, abhängig. Aufgrund der niedrigen Ansprechrate (low demand) der Sicherheitsfunktion findet für gewöhnlich in vergleichsweise kurzen Zeitabständen eine Funktionsprüfung statt bei der die Manipulation mit hoher Wahrscheinlichkeit erkannt würde. Daher stellt diese Auswirkung kein zu unterstellendes abschließendes Ziel eines Cyberangriffs dar. Aus diesem Grund wird bei der Betrachtung im Profil unterstellt, dass eine Manipulation der PLT-S stets die Herbeiführung eines Anforderungsfalles bei deaktivierter SIF zum Ziel hat (A3). Die möglichen Angriffspfade hängen dabei stark von den Realisierungsvarianten der PLT-S ab.

Die Komponenten der Zone-C der Modellarchitekturen können relevant für Auswirkungen auf die PLT-S sein, wenn durch fehlende Verfügbarkeit, Authentizität und Integrität zum Beispiel eine Fehlentscheidung vom Operator getroffen und so die Sicherheit von Menschen und Umwelt gefährdet werden könnte.

11.1.2 Schadensszenarien

Für die dargestellten Schutzbedarfskategorien sind gemäß IT-Grundschutz unterschiedliche Schadensszenarien zu berücksichtigen. Die Beschreibung der Szenarien sind an die chemische Industrie angepasst. Eine Übernahme ist durch den Betreiber jedoch nochmals zu prüfen und zu ergänzen.

Für das vorliegende Profil sind nur die Szenarien „Verstoß gegen Gesetze, Vorschriften oder Verträge“ und „Beeinträchtigung der persönlichen Unversehrtheit“ sowie „Finanzielle Auswirkungen“ relevant (grün hinterlegt) und bei der Schutzbedarfsfestlegung „normal“, „hoch“ und „sehr hoch“ zu berücksichtigen. Bei einer Betrachtung des Produktionsprozesses sind die Szenarien zu berücksichtigen.

Tabelle 11 Schutzbedarf normal

Bereich	Auswirkung
Verstoß gegen Gesetze, Vorschriften oder Verträge	Ein Verstoß gegen Gesetze oder Vorschriften hat nur geringfügige Konsequenzen. Ein Verstoß gegen Verträge, wie die Auslieferung des Endprodukts, hat nur geringe Konventionalstrafen zur Folge. Es ist nicht von einem Absprung des Kunden auszugehen.
Abfluss von Daten	Die vorhandenen Informationen im Informationsverbund wie Produktionsdaten oder -rezepte können bei der Veröffentlichung die Institution nicht oder nur gering schädigen
Beeinträchtigung der persönlichen Unversehrtheit	Der vorhandene Produktionsprozess und die eingesetzten Stoffe können weder die Umwelt noch die Gesundheit von Personen gefährden
Beeinträchtigung des Produktionsprozesses	Bei einer Störung oder einem Ausfall der Anlage hat dieses keinen oder nur einen geringen Einfluss auf die Erstellung des Endproduktes. Die Produktion kann direkt nach der Behebung der Störung ohne lange Anfahrzeiten wieder betrieben werden. Das Endprodukt kann über andere Prozesse erstellt werden.
Negative Innen- oder Außenwirkung (Image)	Bei einer Störung der Anlage ist nicht mit einer Gefährdung innerhalb oder außerhalb der Produktionsanlage auszugehen
Finanzielle Auswirkungen	Der finanzielle Schaden ist für eine Institution hinnehmbar.
NA 163	A1

Tabelle 12 Schutzbedarf hoch

Bereich	Auswirkung
Verstoß gegen Gesetze, Vorschriften oder Verträge	Ein Verstoß gegen Gesetze oder Vorschriften hat erhebliche Auswirkungen. Diese können bis zur kurzfristigen Stilllegung der Produktion führen. Ein Verstoß gegen Verträge, wie die Auslieferung des Endprodukts, hat erhebliche Konventionalstrafen zur Folge. Es ist von einem Absprung des Kunden auszugehen.
Abfluss von Daten	Die vorhandenen Informationen im Informationsverbund, wie Produktionsdaten oder -rezepte können bei der Veröffentlichung die Institution erheblich schädigen. Eine Veröffentlichung von Informationen könnte beispielsweise einer anderen Institution einen Wettbewerbsvorteil verschaffen.
Beeinträchtigung der persönlichen Unversehrtheit	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) können der vorhandene Produktionsprozess oder die eingesetzten Stoffe die Umwelt und die Gesundheit von Personen gefährden.
Beeinträchtigung des Produktionsprozesses	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) oder einem Ausfall der Anlage hat dieses zur Folge, dass die Erstellung des Endproduktes nur noch bedingt bis gar nicht mehr möglich ist.
Negative Innen- oder Außenwirkung (Image)	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) der Anlage ist mit einer Gefährdung innerhalb und außerhalb der Produktionsanlage auszugehen.
Finanzielle Auswirkungen	Der finanzielle Schaden für eine Institution ist beträchtlich, kann aber nicht existenzbedrohend werden.
NA 163	A2, A3

Tabelle 13 Schutzbedarf sehr hoch

Bereich	Auswirkung
Verstoß gegen Gesetze, Vorschriften oder Verträge	Ein Verstoß gegen Gesetze oder Vorschriften hat fundamentale Auswirkungen. Diese können bis zur Stilllegung der gesamten Produktion führen. Ein Verstoß gegen Verträge, wie die Auslieferung des Endprodukts, hat hohe Konventionalstrafen zur Folge. Kunden, die das Endprodukt existenziell benötigen, sind gezwungen, Verträge mit einer anderen Institution abzuschließen.
Abfluss von Daten	Die vorhandenen Informationen im Informationsverbund, wie Produktionsdaten oder -rezepte werden bei der Veröffentlichung die Institution existenziell schädigen. Eine Veröffentlichung von Informationen könnte anderen Institutionen die Produktion des eigenen Produktes ermöglichen.
Beeinträchtigung der persönlichen Unversehrtheit	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) können der vorhandene Produktionsprozess oder die eingesetzten Stoffe die Umwelt und die Gesundheit von Personen langfristig gefährden. Ein Vorfall kann bis zum Tod von Personen führen.
Beeinträchtigung des Produktionsprozesses	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) oder einem Ausfall der Anlage hat dieses zur Folge, dass die Erstellung des Endproduktes langfristig nicht mehr erfolgen kann. Selbst ein kurzfristiger Ausfall ist nicht akzeptabel.

Bereich	Auswirkung
Negative Innen- oder Außenwirkung (Image)	Bei einer Störung (z. B. durch einen Angriff oder Manipulation) der Anlage ist mit einer hohen Gefährdung innerhalb und außerhalb der Produktionsanlage auszugehen. Diese kann einen großen Umkreis um die Produktionsanlage betreffen.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für eine Institution existenzbedrohend.
NA 163	A2, A3

11.1.3 Schutzbedarfsfestlegung

In den weiteren Unterkapiteln werden die Komponenten (dem IT-Grundschutz nach Zielobjekte), die zur Umsetzung der verschiedenen Modellarchitekturen notwendig sind, mit Blick auf den Schutzbedarf in den vier Zielbereichen Hardware, Software, Netzwerke und Infrastruktur beschrieben. Eine ausführliche Komponenten-Beschreibung findet sich in 11.2 Anhang B Gefährdungsbetrachtung der Komponenten.

Die Beurteilung des Schutzziels kann sich gemäß den Ausführungen im Anhang gegebenenfalls noch ändern, wenn sich herausstellt, dass Verteilungseffekte anstatt des Maximum-Prinzips angenommen werden können.

Weiterhin gilt zu beachten, dass durch Betriebskonzepte bereits vorliegende Cybersicherheitsmaßnahmen nicht bei der Schutzbedarfsfeststellung berücksichtigt werden. Erst bei der Anforderungsfestlegung wird auf mögliche und übliche organisatorische und technische Maßnahmen eingegangen. Sie werden entsprechend bei der Auswahl der Anforderungen für den erhöhten Schutzbedarf berücksichtigt.

11.1.3.1 Vererbung von Schutzbedarfsfeststellungen

Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines OT-Systems inklusive aller zugehöriger und beteiligter Komponenten (Maximum-Prinzip und Abhängigkeit).

Der Schutzbedarf des IT-Systems kann höher sein als der Schutzbedarf der einzelnen Anwendungen (Kumulationseffekt). Dies ist z. B. der Fall, wenn auf einem nicht redundanten Server mehrere Anwendungen mit normalem Schutzbedarf betrieben werden. Der Ausfall einer dieser Anwendungen könnte überbrückt werden. Wenn aber alle Anwendungen gleichzeitig ausfallen, kann ein hoher Schaden entstehen.

Der Schutzbedarf kann niedriger sein als der Schutzbedarf der zugeordneten Anwendungen, wenn eine Anwendung mit hohem Schutzbedarf auf mehrere Systeme verteilt ist und auf dem betreffenden IT-System nur weniger wichtige Teile dieser Anwendung ausgeführt werden (Verteilungseffekt).

11.2 Anhang B Gefährdungsbetrachtung der Komponenten

Auf der Grundlage der Modellarchitekturen wird in diesem Kapitel die verwendeten Komponenten erläutert sowie Gefährdungen und deren Auswirkungen auf die Sicherheitsfunktion dargestellt. Eine Beurteilung der Gefährdungen und damit eine Risikobewertung findet nicht statt.

Bei der Beschreibung der Komponenten werden auf unterschiedliche Realisierungsmöglichkeiten eingegangen, die im Feld vorzufinden sind. Dies soll dabei helfen effektive Anforderungen und Maßnahmen hinsichtlich der Cybersicherheit auszuwählen und umzusetzen. Eine technische Beschreibung finden nicht statt.

In diesem Abschnitt werden die Komponenten aus Tabelle 2 Zielobjekte näher beschrieben.

11.2.1 IT1 - Sensor

11.2.1.1 Allgemein

Sensoren sind als elektronische Komponente mit Mikroprozessor und Software ausgeführte Messumformer, die eine physikalische Größe in einen elektrischen Ausgabewert wandeln. Dieser wird als normiertes Einheitssignal (häufig 4 bis 20mA, 0 bis 10V) oder als digitale Informationen, die über einen Feldbus oder Ethernet-Protokolle übertragen werden, bereitgestellt. Sensoren stellen neben den Messwerten häufig noch Schnittstellen bereit, über die eine Diagnose und Parametrierung erfolgt. So kann ein Sensor neben einem elektronischen Ausgabewert auch noch über weitere Schnittstellen verfügen, z. B. WLAN-, Bluetooth- oder Wireless-HART-Schnittstellen.

11.2.1.2 Verwendung in Modellarchitekturen

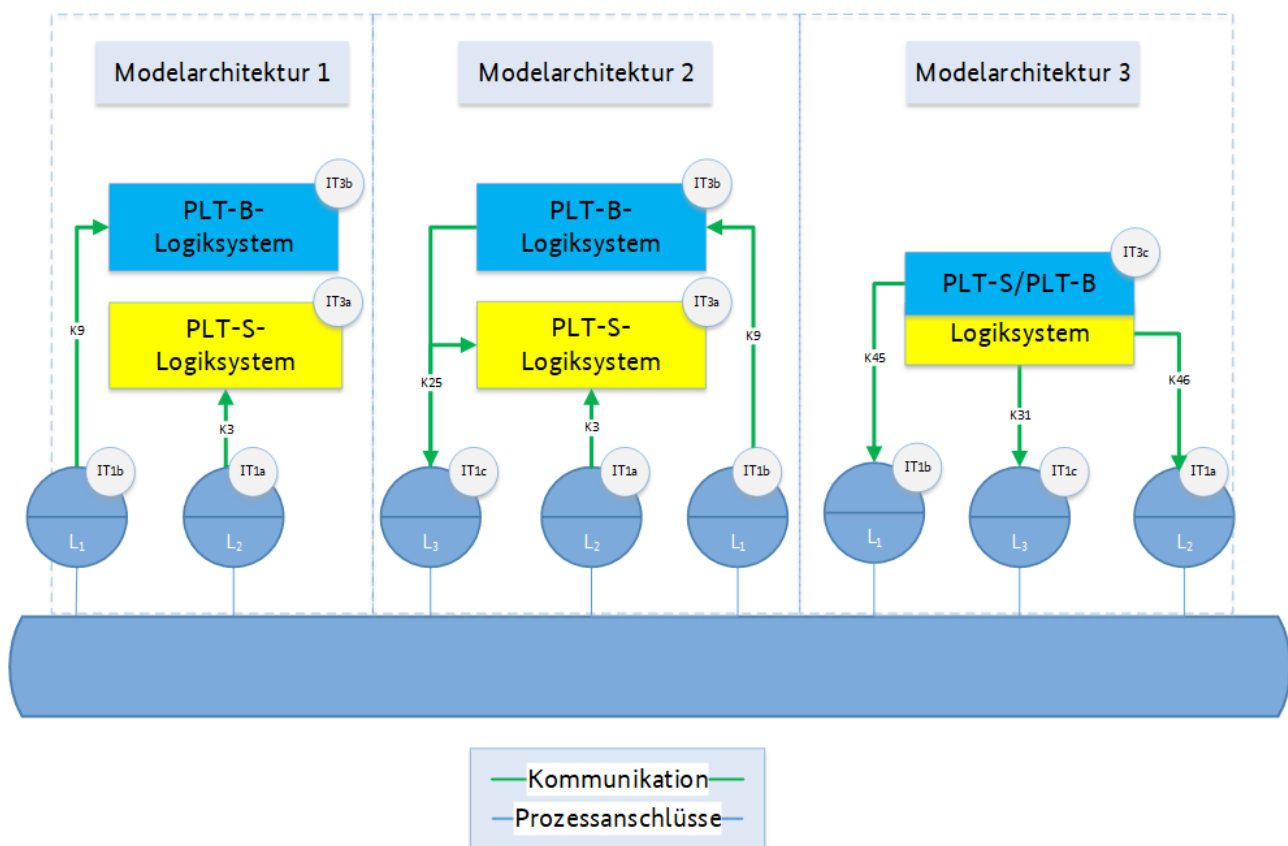


Abbildung 5 Realisierungsvarianten zur Verwendung von Messwerten

Es handelt sich um eine rein schematische Darstellung, die die Kommunikationsverbindungen darstellt.

Modellarchitektur 1 repräsentiert die separierte Nutzung eines PLT-S-Sensors (L2) und PLT-B-Sensors (L1). Findet hingegen eine gemeinsame Nutzung der Sensordaten für beide Funktionsbereiche (Betriebs- und Sicherheitseinrichtungen) statt (L3 in Modellarchitektur 2 und 3). Es ist im Einzelfall zu bewerten, ob die gemeinsame Nutzung zu einem höheren Risiko führt und ob die Trennung und Unabhängigkeit nach IEC 62508/IEC61511 weiterhin gegeben ist.

Die gemeinsame Nutzung führt in der Regel zu Einsparungen und weniger Wartungsaufwand. Beide dargestellten Modellarchitekturen 2 und 3 werden in der Prozessindustrie häufig angetroffen.

In Modellarchitektur 2 schickt der Sensor das Signal an PLT-B- und PLT-S-Logiksysteme. Es ist zu berücksichtigen, dass bei einer Kompromittierung des Sensors PLT-S- und PLT-B-Logiksysteme fehlerhafte oder falsche Daten erhalten.

In Modellarchitektur 3 wird deutlich, dass durch das gemeinsam genutzte PLT-S/ PLT-B-Logiksystem fast kein Unterschied zwischen den separierten und gemeinsam genutzten Sensoren gegeben ist. Alle Informationen laufen in dem gemeinsamen PLT-S/PLT-B-Logiksystem zusammen.

In beiden Fällen der gemeinsamen Nutzung des Sensorsignals kann eine Manipulation des Sensors zu der Auswirkung A3 führen. Durch Manipulation der übermittelten Messwerte (z. B. eingefrorenes Messsignal, wodurch ein Befüllvorgang über den maximalen Füllgrad eines Behälters hinaus fortgesetzt werden könnte) kann ein chemischer Prozess in einen gefährlichen Zustand überführt werden. Da die Messwerte der PLT-B und PLT-S betroffen sind, wird der Anforderungsfall bei deaktivierter Sicherheitsfunktion hervorgerufen.

In Modellarchitektur 3 wird deutlich, dass es keinen Unterschied zwischen separaten und gemeinsam genutzten Sensoren gibt. Die Verarbeitung erfolgt immer in derselben Komponente.

Tabelle 14 Übersicht der Varianten, Gefährdungen und Auswirkungen für Sensoren

Modellarchitektur	Gefährdung für Sensor	Auswirkung
1,2,3	Ausfall, gefälschte Messwert „zur sicheren Seite“	A1
1	Manipulation, Missbrauch der Kommunikation zum PLT-S-Logiksystem	A2
2,3	Manipulation, Missbrauch der Kommunikation zum PLT-S-Logiksystem	A3

11.2.1.3 Gefährdungen

11.2.1.3.1 Physischer Zugang

Der Sensor ist meist "im Feld" verbaut. Viele Anlagen werden "offen" betrieben, sind also meist nicht in abgeschlossenen Gebäuden aufgebaut. Zugang ist für jeden Mitarbeiter und häufig auch jeden autorisierten Besucher des Werks möglich.

11.2.1.3.2 Manipulation der Werte

- Gerät in Testmode setzen
- Durch einen „Man-in-the-middle“-Angriff oder eine Veränderung der Firmware/Konfiguration kann
 - eine Dauerschleife eines aufgezeichneten Messzyklus eingespielt werden (spoofing).
 - Messwerte außerhalb des zulässigen Wertebereich gesendet werden
 - Messwerte gesendet werden, die Anforderungsfall auslösen
 - Messwerte verändert werden, so dass der Anforderungsfall nicht ausgelöst wird.
- Fehlerhafte Kalibrierung durch kompromittiertes Konfigurationsgerät (IT6)

11.2.1.3.3 Software

Bei der Software handelt es sich stets um spezielle Firmware mit eigenen Betriebssystem. Dabei gilt für Sensoren, die für einen hohen SIL Level eingesetzt werden, dass die Verfügbarkeit bei der Codeentwicklung eine hohe Priorität hat. Cybersicherheitsaspekte können hingegen nicht pauschal angenommen werden.

11.2.2 IT2 - Aktor

11.2.2.1 Allgemein

Im OT-Umfeld beschreibt der Aktor ein Element zur Umwandlung elektrischer Signale in Bewegungen oder andere physikalische Größen. Damit wird es möglich, in den physischen Prozess einzugreifen. Aktoren im PLT-S erhalten die elektrischen Signale i. d. R. abhängig über einem Sensor, dessen Signal einem Logiksystem verarbeitet wird. Das Logiksystem erzeugt die vorhergesehene Reaktion zur Anpassung von prozessrelevanten Gegebenheiten (physikalische Größen). Zum Beispiel werden bei der Umsetzung eines Befehls automatisch Schieber, Regler oder Hebel in einem vordefinierten Maß betätigt oder ein Relais geschaltet, das einen Motor ansteuert, um von den Sensoren gemessene grenzüberschreitende Abweichungen an betrieblich vorgesehene Werte anzupassen. Dementsprechend werden beispielsweise zur Senkung von Füllständen in Filtern Kondensat ausgeschleust, zur Steigung von Temperaturen Heizungssysteme geregelt und zur Reduktion der Feuchtigkeit Lüftungen gestartet. Außerdem können Aktoren Statusinformationen und Fehlermeldungen an das PLT-B-Logiksystem zurück übermitteln.

11.2.2.2 Verwendung in Modellarchitekturen

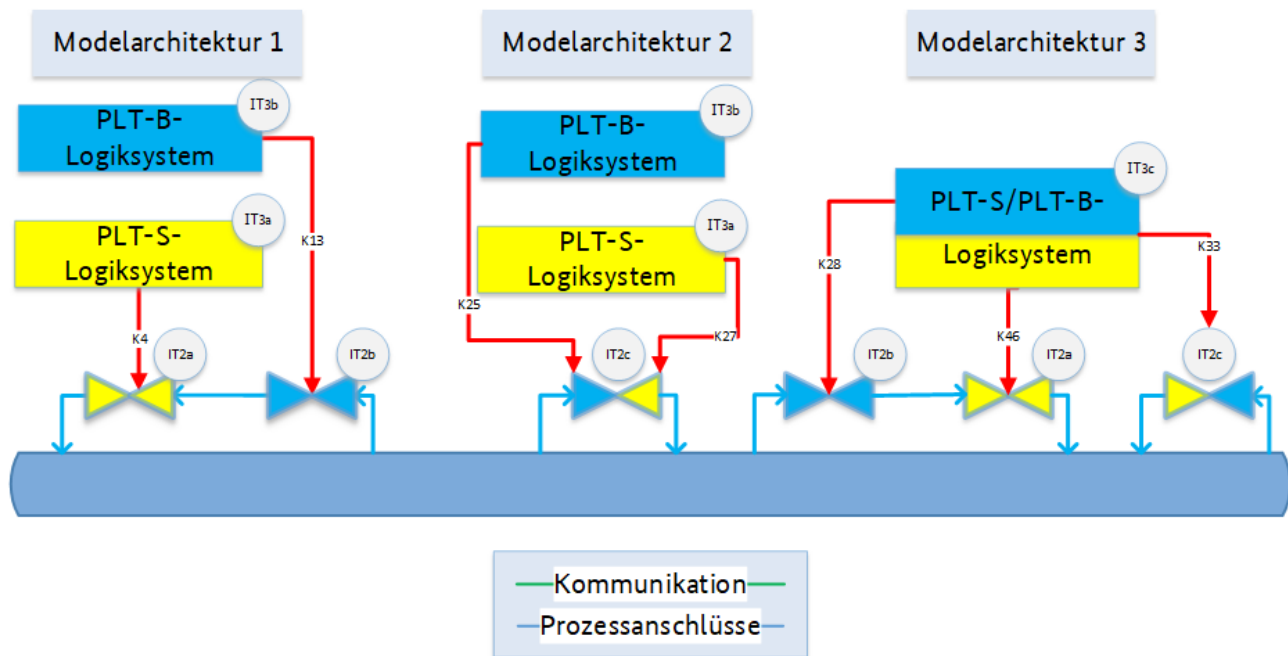


Abbildung 6 Realisierungsvarianten zur Ansteuerung von Aktoren

Die Einfärbungen der Aktoren verdeutlichen die alleinige oder gemeinsame Nutzung durch das PLT-S- oder PLT-B-Logiksystem.

Modellarchitektur 1 stellt die separierte Nutzung von Aktoren dar. Beispielsweise das Füllen des Behälters geschieht durch die PLT-B bei der auch die Signalverarbeitung ausschließlich über die PLT-B läuft. Die Regelung des PLT-B-Aktors würde schließen, bevor ein unzulässiger Zustand (z. B. Überfüllung, Überdruck) entsteht. Dies hat allerdings keine sicherheitstechnische Zuverlässigkeit (im Sinne der Funktionalen Sicherheit) und funktioniert so lange, wie die Regelung der PLT-B durch Automatik oder Auf-Hand-Nehmen (manuell) zuverlässig erfolgt.

Eine Manipulation des PLT-B-Aktors IT2b oder an der Verbindung K13 kann dazu genutzt werden, den Anforderungsfall auszulösen und den Prozess zu unterbrechen (Auswirkung A1). In diesem Fall wäre der Ausfall der Sicherheitsfunktion (Auswirkung A2) nur dann relevant, wenn auch die in den PLT-B hinterlegte Abschaltautomatik nicht funktionieren würde, da erst dann der Anforderungsfall eintreten könnte. Dies verdeutlicht die Notwendigkeit beide Systeme (PLT-S und PLT-B) zu manipulieren.

Durch Manipulation des PLT-S-Aktors IT2a oder an der Verbindung K4 (z. B. Installation eines Signalgebers) kann die Sicherheitsfunktion deaktiviert werden (Auswirkung A2).

Im Unterschied zum Sensor stellt die Unterbrechung der Energiezufuhr durch einen Notschalter oder physisch die Möglichkeit dar, den Aktor direkt in den energielosen sicherheitsgerichteten Zustand zu versetzen.

In Modellarchitektur 2 steuert die PLT-B betriebsbedingt den Aktor. In dem Bild wurde auf die Darstellung von separaten Aktoren (IT2a und IT2b) verzichtet.

In Modellarchitektur 3 erfolgt die betriebsbedingte Steuerung weiterhin über die PLT-B. Jedoch wird diese über das PLT-S/ PLT-B-Logiksystem IT3c geleitet. Diese leitet den Befehl weiter, sofern kein Anforderungsfall vorliegt. Dies bedeutet, dass eine Manipulation der signalgebenden Komponente (IT3c PLT-S/ PLT-B-Logiksystem) oder der Missbrauch der Verbindung zu einer Deaktivierung der Sicherheitsfunktion mit gleichzeitigem Auftreten des Anforderungsfalls führen kann. Dies gilt besonders für den seltenen aber nicht unüblichen Fall, dass die Schaltlogik einer PLT-B im PLT-S-Logiksystem realisiert ist.

Ein Anforderungsfall kann sich beispielsweise dadurch ergeben, dass der Aktor einen Prozess steuert, der eine häufige Energiezufuhr vorsieht und damit bei durchgehender Öffnung des Aktors eine durchgehende Einspeisung erfolgen kann.

Modellarchitektur 3 verdeutlicht, dass eine nach dem Modellarchitektur 1 physikalisch separate Komponente des Aktors IT2a durch die Verarbeitung des Sensorsignals bei dem PLT-S-Logiksystem logisch gemeinsam genutzt wird.

Tabelle 15 Übersicht der Varianten, Gefährdungen und Auswirkungen für Aktoren

Modellarchitektur	Gefährdung für Aktor	Auswirkung
1,2,3	Ausfall	A1
1,2	Manipulation, Missbrauch der Leitung	A2
3	Manipulation, Missbrauch der Leitung	A3

11.2.2.2.1 Protokolle

Üblich:

- Verdrahtung: 4-20mA Signal (HART-Protokoll),
- Binäre Signale (EIN, AUS)
- Vernetzung z.B. Sollwertübertragung für Frequenzumrichter

Möglich:

- WLAN,
- Bluetooth,
- NFC oder
- Wireless-HART-Schnittstellen.

11.2.2.2.2 Software

Software für Parametrierung von Umrichtern, Stellungsreglern von Armaturen

11.2.2.3 Gefährdungen

11.2.2.3.1 Physikalischer Zugang

Der Aktor ist meist "im Feld" verbaut. Prozesschemische Anlagen werden üblicherweise "offen" betrieben, sind also meist nicht in abgeschlossenen Gebäuden aufgebaut. Zugang ist für jeden Mitarbeiter und häufig auch jeden autorisierten Besucher des Werks möglich. Ansteuerungen für Aktoren sind zudem häufig im EMSR-Raum verbaut, um z. B. Motoren zu schalten.

11.2.2.3.2 Manipulation

Die Manipulation kann auf mehreren Wegen erfolgen:

- Manipulation des Signalwegs: Installation eines Signalgebers auf der Leitung. Gerade bei „dummen“ Aktoren (0 oder 1) möglich.
- Manipulation der Konfiguration: Beispielsweise wird bei 4 mA statt 0% Öffnung 100% gesteuert.
- Manipulation der Kalibration oder fehlerhafte Kalibrierung z. B. durch das Konfigurationsgerät (Auswirkung: keine Reaktion A2)
- Übernahme der signalgebenden Komponente (PLT-S oder PLT-B) (keine Reaktion A2)

11.2.3 IT3 - Logiksysteme

11.2.3.1 Allgemein

Ein Logiksystem kann allgemein aus einer nicht programmierbaren Logik, z.B. einem Relais, oder einer SPS bestehen. Die Software ist ein Teil des Logiksystems. Ein PLT-S-Logiksystem (IT3a oder IT3c) wird meist dann verwendet, wenn z. B. die alleinige Verwendung von Sicherheitsventilen zur Störfallvermeidung als nicht mehr ausreichend zu bewerten sind.

SPS sind physisch Echtzeitsysteme, die in industriellen Bedingungen für Steuerungszwecke eingesetzt werden. Eine SPS kommuniziert mit Sensoren und Aktoren. Die SPS empfängt Daten von einem Sensor, die auf Basis einer in der SPS hinterlegten Logik verarbeitet werden. Falls die Daten definierte Bedingungen erfüllen, versendet die SPS den dafür vorhergesehenen Befehl an einen Aktor. Dementsprechend führt der Aktor den Befehl anschließend aus. Die in einer SPS hinterlegte Logik wird an einer Programmierstation erstellt.

Der wesentliche Unterschied zwischen einer SPS (IT3b PLT-B-Logiksystem) und eines PLT-S-Logiksystem (IT3a) ist die Verfügbarkeit und das besondere Maßnahmen getroffen werden, dass die Ausgänge des PLT-S-Logiksystem (IT3a) bei einem Fehler einen sicheren Zustand annehmen. Dieser ist in der Regel der energielose Zustand.

Die Verfügbarkeit und Integrität sind die wichtigsten Schutzziele von PLT-S-Logiksystem (IT3a) oder PLT-S/ PLT-B-Logiksystem (IT3c). Die Vertraulichkeit als weiteres Schutzziel gewährleistet, dass der Angreifer nur mit großem Aufwand an hilfreiche oder notwendige Informationen kommt.

11.2.3.2 Verbindung zwischen PLT-S und PLT-B-Logiksystem

Die Kommunikation zwischen den beiden Komponenten weist eine Vielzahl von Funktionen auf. Neben der Weiterleitung von Sensor- und Befehlsdaten, kann die Verbindung genutzt werden, um:

- Ausgelöste Sicherheitsfunktionen des PLT-S-Logiksystem vom PLT-B-Logiksystem zurücksetzen. Das PLT-B-Logiksystem setzt die Sicherheitsfunktion zurück. Dies ist nur dann möglich, wenn der Anforderungs-/Fehlerfall nicht mehr vorliegt. In der Regel ist dazu ein Aufschalten mit der Programmierstation nötig

- Wartungsfunktionen vom PLT-B-Logiksystem dem PLT-S-Logiksystem mitteilen
Es werden Informationen zwischen PLT-B-Logiksystem und PLT-S-Logiksystem beim Aktivieren und Deaktivieren von Wartungsfunktionen zur Visualisierung und ausgetauscht.
- Auswahl von Rezepturen/Grenzwerten in Batchanlagen
In Batchanlagen ist es für unterschiedliche Rezepte notwendig, dass Grenzwerte im PLT-S-Logiksystem verändert werden. Hierfür werden über eine PLT-S-Bedienstation Grenzwerte für ein Rezept gesetzt. Das PLT-B-Logiksystem prüft über diese Verbindung vor dem Start eines Batches, ob die gesetzten Werte im PLT-S-Logiksystem zu dem Rezept passen und startet erst bei korrekten Werten den Batch. Eine Änderung der Grenzwerte ist danach im PLT-S-Logiksystem gesperrt.

Diese Signale dürfen nie zu einer Kompromittierung der Sicherheitsfunktion führen. Häufig muss zur Bestätigung des via Bus kommunizierten Signals noch ein Hardware Schlüsselschalter betätigt werden.

Zudem erfolgt nur selten ein Zugriff oder Konfiguration des Gerätes, so dass der Netzwerkverkehr hier gut zu überwachen ist. Besonders bei einer Kommunikation über einen Switch (OT-Infrastruktur) sind Maßnahmen zu einer höheren Absicherung zu treffen. Alternativ ist die Verwendung von Switchen ausschließlich für PLT-S-Logiksysteme (Netzwerksegmentierung) zu erwägen. Gängig ist die Punkt-zu-Punkt-Verbindung über z. B. Profibus oder Hartverdrahtung.

11.2.3.3 Verwendung in Modellarchitekturen

Bei der gemeinsamen Nutzung der Komponente ergeben sich je nach Realisierungsvarianten der Sensoren (IT1a, IT1b, IT1c) und Aktoren (IT2a, IT2b, IT2c) unterschiedliche Auswirkungen.

Tabelle 16 Übersicht der Varianten, Gefährdungen und Auswirkungen für getrennte Logiksysteme

Variante Sensor	Variante Aktor	Gefährdung	Auswirkung
V1,2,3	V1,2,3	Ausfall	A1
V1	V1,2	Manipulation, Missbrauch der Leitung	A2
V2,3	V3	Manipulation, Missbrauch der Leitung	A3

In IT3c PLT-S/ PLT-B-Logiksystem führen hingegen alle Varianten bei einer Manipulation zur Auswirkung A3. In diesem System wird die Logik der PLT-S und die Logik des PLT-B betrieben. Die beiden Logikteile werden in getrennten Teilen des Systems verarbeitet.

11.2.3.4 Protokolle

z. B. herstellereigene Kommunikation, Modbus, Profibus, Industrial Ethernet, 4-20mA mit HART (zu den Sensoren/Aktoren)

11.2.3.5 Software

Programmiersoftware mit Betriebssystem, Hersteller spezifisches Programmierwerkzeug

11.2.3.6 Daten

Es werden Daten erzeugt oder gespeichert, die für die Integrität oder Funktionsfähigkeit der PLT-S wesentlich sind.

11.2.3.7 Gefährdungen

- Angreifer nutzen Schwachstellen in veralteten Softwareversionen aus
- Angreifer erraten einfache Administrator Passworte, oder nutzen schlechte/falsche Konfigurationen aus, um die Programmierstation unter ihre Kontrolle zu bringen.
- Änderung der Software über die Programmierstation

- Eine unbemerkte Änderung des Programms oder Änderungen von Sollwerten kann zu einer Nichtabschaltung der Sicherheitsfunktion führen.
- Dauerhaftes Setzen aller Ausgänge (ausgehend vom Ruhestromprinzip) und „gleichzeitige“ Manipulation der PLT-B
- Integriertes PLT-S/PLT-B-Logiksystem (IT3c)
 - unzureichender Schutz der internen Kommunikation (unterlaufen von Maßnahmen bei PLT-S-Logiksystem)
 - Selbiges Passwort für PLT-S und PLT-B-Logiksystem

11.2.4 IT4 – Programmierstation

11.2.4.1 Allgemein

Programmierstationen (PS) sind vorrangig ein stationäres IT-System. Im Fall von Programmierstationen für Komponenten der PLT-B sind auch Virtuelle Maschinen im Einsatz. In Einzelfällen kann es sich um Handgeräte (z. B. Laptop) handeln.

Für Programmierung von PLT-S- (IT3a), PLT-B- (IT3b), bzw. PLT-S/ PLT-B-Logiksystem (IT3c) und PLT-S- (IT5a), PLT-B- (IT5b) oder PLT-S/ PLT-B-Bedienstationen (IT5c) wird jeweils die Software des Herstellers benötigt. Es gelten dann die Vorgaben des jeweiligen Herstellers (hinsichtlich Wartung, Abhängigkeiten der Software usw.). Dies ist ein Grund, der dazu führt, dass getrennte Geräte für die verschiedenen Komponenten genutzt werden. Dies schließt aktuell eine gemeinsame Nutzung in den meisten Fällen aus.

Für die Programmierstation gibt es unterschiedliche Nutzungsszenarien:

1. ausschließliche Nutzung zur Programmierung und Parametrierung. Die Geräte werden nur dazu genutzt und auch nur im Bedarfsfall angeschlossen. Ansonsten findet keine Nutzung/Betrieb statt. Aufbewahrung erfolgt dann z.B. im IT-Schrank oder Technikraum.
2. Es findet ein permanenter Betrieb statt. Gründe dafür sind z.B. der Einsatz zum Monitoring, um im Anforderungsfall die Sequence-of-Events nachvollziehen zu können. Diese ist für den „normalen“ Operator an PLT-B nicht zugänglich.

Remote-Zugriffe sind für PLT-B-Programmierstationen (IT4b) eher die Regel, um diese aus der Ferne zum Programmieren/Parametrieren zu nutzen. Remote-Zugriffe auf PLT-S-Programmierstationen (IT4a) für diesen Zweck sind nicht üblich.

Bei integrierten PLT-S/PLT-B-Logiksystemen (IT3c) definieren die sicherheitsgerichteten Funktionen den Schutzbedarf für die Programmierstation.

11.2.4.2 Gefährdungen

Die Programmierstation ist ein zentraler Angriffspunkt. Dies zeigen die bekanntgewordenen Angriffe Stuxnet und Triton.

- Manipulation über manipulierte Firmware
- Änderung der Darstellung der Panelfarben der Bedienstation (z. B. Alarm auch grün)
- Programme der Logiksysteme (IT3a, b, c) können manipuliert werden

11.2.5 IT5 - Bedienstation

11.2.5.1 Allgemein

Die PLT-S-Bedienstation (IT5a) wird verwendet, um sicherheitsrelevante Eingaben zu tätigen. Hierunter fallen z. B. produktionsabhängige Grenzwertschaltungen oder sicherheits-relevante Prozessparameter.

Eine weitere Nutzung kann darin bestehen sicherheitsrelevante Alarmer darzustellen oder sicherheitsrelevante Ereignisse zu quittieren, bzw. zurückzusetzen.

Typische Prozessbeobachtungen und Bedienungen sind hierüber im Normalfall nicht möglich.

11.2.5.2 Spezielle Anwendung IT5c

Verwendung der Funktionen von PLT-S-Bedienstation (IT5a) und PLT-B-Bedienstation (IT5b) auf einem Gerät. Dies sollte nur in Ausnahmen geschehen und bedarf einer besonderen Risikobetrachtung, z.B. in Hinsicht auf die Rückwirkungsfreiheit.

Die Verwendung von Funktionen gemäß PLT-S-Bedienstation (IT5a) und PLT-B-Bedienstation (IT5b) auf einem Gerät sollten grundsätzlich vermieden werden. Falls dies aus anderen Gründen nicht möglich ist, sind weitere Zusatzpunkte zu beachten. Wenn über Bedieneingaben sicherheitsrelevante Parameter verstellt werden sollen, ist es erforderlich die Handlung und die Daten zu verifizieren. Dies kann ggf. durch zusätzlichen Hardwareschalter oder weitere Überprüfungen geschehen. Grundsätzlich sollten diese Parameter als feste Auswahlen in dem PLT-S-Logiksystem (IT3a) hinterlegt sein und nicht frei durch den Operator eingegeben werden. Detaillierte Beschreibungen dazu finden sich auch in (4).

11.2.5.3 Gefährdungen für PLT-S-Bedienstation (IT5a) und PLT-S/PLT-B-Bedienstation (IT5c)

Anlagen werden üblicherweise "offen" betrieben, sind also meist nicht in abgeschlossenen Gebäuden aufgebaut. Zugang ist für jeden Mitarbeiter und häufig auch für jeden autorisierten Besucher des Werks möglich.

- Sicherheitsrelevante Grenz- und Prozesswerte können verändert werden. Dies ist bei unterschiedlicher Produktherstellung möglich/üblich. Beispielsweise wird die T3/T4 Umschaltung per Schlüsselschalter eingesetzt, um die Temperaturgrenzwerte an die verwendeten Stoffe hinsichtlich des Zündtemperaturgrenzwertes anzupassen
- Sicherheitsrelevante Alarmer können manipuliert werden.
- Sicherheitsfunktionen können deaktiviert werden:

Dies ist zum Beispiel nötig, wenn die Prozesseinheit mit kochendem Wasser gespült werden soll, aber die Prozesstemperatur maximal 80 Grad beträgt. Bei der Bedienstation ist zudem noch ein Rollen- und Lizenzkonzept zu berücksichtigen. Das System kann so konfiguriert und lizenziert sein, dass von der Bedienstation auch Engineering durchgeführt werden kann. In diesem Fall ist die Bedienstation ebenfalls als Programmierstation zu behandeln.

11.2.5.3.1 Gängige Absicherungsmaßnahmen

Es bedarf zwei Bedienstationen, um SIF zu deaktivieren. Gängig eher Schlüsselschalter. Diese Art von Maßnahme/Regelungen ergeben sich auch ohne den Cybersicherheitsaspekt allein aus der Betriebssicherheit.

11.2.6 IT6 - Konfigurationsgerät

Mit dem Konfigurationsgerät werden Sensoren (IT1a, IT1b, IT 1c) und Aktoren (IT2a, IT2b, IT2c) für den jeweiligen Einsatz konfiguriert (Status und Konfigurationswerte auslesen/einstellen).

11.2.6.1 Verwendung in Modellarchitekturen

Mobiles oder stationäres Konfigurationsgerät, wobei die temporäre Verbindung eine Maßnahme darstellt. Durch diese ergibt sich bei der Gefährdungsbetrachtung kein Unterschied.

Auf dem Konfigurationsgerät laufen alle notwendigen Programme zum Programmieren des Zielgerätes.

11.2.6.2 Gefährdungen

- Ansteuerung über Leitsystem (Aufspielen von Schadcode)
- Missbrauch/Entwendung des Gerätes zur Konfiguration von Feldgeräten
- Nutzung sowohl als Universalgerät (auch Programmierstation) als auch über mehrere Standorte
- Manipulation der Konfigurationsfunktion: Fehlerhafte Programme auf die Systeme (Sensor, Aktor) unbewusst aufspielen
- Malware auf dem Gerät mit Übertragung auf andere Geräte (Malwareschleuder)
- Manipulation von Feldgerät der andere Konfigurationsgeräte infiziert (bei Bestandsgeräten aufgrund der geringen Leistungsfähigkeit noch unwahrscheinlich.)

11.2.7 IT7 –Servicegeräte

11.2.7.1 Allgemein

Das Servicegeräte, oft ein Laptop oder Smartphone, dient der Konfiguration des ICS. Im Gegensatz zum Konfigurationsgerät (IT6) und Programmierstationen (IT4a, IT4b, IT4c) ist diese Komponente grundsätzlich nicht fest im OT-Netzwerk eingebunden. Daher kann sie in verschiedenen ICS oder sogar in verschiedenen Standorten genutzt werden.

Zudem ergibt sich häufig die Notwendigkeit, Ersatzgeräte wegen alter Betriebssysteme und Software vorzuhalten. Da die Verfügbarkeit gegeben sein muss, ist es oft nicht zweckmäßig alte Laptop im Schrank aufzubewahren, die bei Bedarf nicht mehr funktionierten, weil Hardwareteile durch Alterung und Nichtbenutzung defekt sind (z. B. Akkus). Um die Verfügbarkeit von alten Geräten sicherzustellen, bieten sich Virtuelle Maschinen an, da das Image gesichert werden kann und sich schnell auf neue Hardware überspielen lässt.

11.2.7.2 Gefährdungen

Auch wenn die Geräte mobil sind und grundsätzlich überall angeschlossen werden können, sind nicht alle Komponenten automatisch gefährdet. Dies liegt an dem Umstand, dass sich die Endgeräte hinsichtlich ihrer Applikationen, Übertragungstechnik und Protokollsprache unterscheiden können.

Je nach Verwendung kommt es zu den gleichen Gefährdungen wie für Konfigurationsgerät und Programmierstation. Daher heben die folgenden Gefährdungen vorwiegend zusätzlich den mobilen Charakter hervor:

- Durch Portabilität ist ein Überspringen von Netzwerksegmenten möglich. Gerade wenn das Gerät einer Person gehört (Owner), nutzt diese es für alle Geräte.
- Unterschiedliche Nutzer eines Gerätes (Schwachstelle: Unachtsamer Nutzer)
- Zugriff mit erhöhten Rechten.
- Es ist eventuell nicht bekannt, wann und wie das Gerät vorher verwendet wurde.
- Trend zur kontaktlosen Kommunikation und die Verwendung von Multifunktionsgeräten (Smartphone).
- Es liegt keine Netzwerkverbindung vor. Das heißt eine Kompromittierung des Gerätes erfolgt vermutlich über den Hersteller (Firmware und bei extern die IT) oder durch das zu parametrierende Endgerät
- Mit Servicegeräten werden auch kleinere elektrische Komponenten parametrieren (z. B. Grenzwertgeber)

11.2.7.3 Gängige Absicherungsmaßnahmen

Eine Lösung könnte sein, dass dedizierte Geräte je Anlagen oder Zonen eingesetzt werden. Dies kann jedoch zu hohem organisatorischen Aufwand oder Unübersichtlichkeit führen, wenn ein Standard mehrere Anlagenabschnitte oder gar Betreiber hat.

Letztendlich lässt sich die Gefährdung nur dadurch beherrschen, dass die Geräte auf aktuellem Softwarestand sind. Zur Sicherstellung der Verfügbarkeit (gerade von Altgeräten), ist die Bündelung mehrere PG als virtuelle Maschine auf einem Host zu prüfen. Bei externen Technikern hilft nur Gerät prüfen und ggf. auf Schadsoftware zu scannen, um diese zu identifizieren. Vor einer Kompromittierung Firmware schützt dies nicht. Dies liegt in der Verantwortung des Herstellers, der seine eigene Cybersicherheit gewährleistet.

11.2.8 IT8 – Betriebsdateninformationssystem

11.2.8.1 Allgemein

Das Betriebsdateninformationssystem (BDIS IT8) speichert Prozesswerte. Prozesswerte sind typischerweise einfache physikalische Größen von Sensoren wie Temperatur, Druck als Zeitreihen, durchaus aber auch Stellwerte (Ventil auf/zu). Mit diesen Daten lassen sich auf den zugehörigen Clients live und historisch Trenddarstellungen abbilden. Weiterhin können diese Daten zu einem Vergleich der aktuellen Zustände mit historischen Anlagenzuständen benutzt werden. So können z. B. Analysen zum Zweck der Fehleranalyse und Optimierung des Prozesses und der Anlage durchgeführt und Entwicklungen wie eine Leckage frühzeitig erkannt sowie Key-Performance-Indicators beobachtet werden.

Ein BDIS (IT8) besteht meist aus einer Client-Server-Anwendung bei der der Server die Zustandsdaten in einer Datenbank verwaltet. Der Client läuft auf zugehörigen Bedienstationen, oft auch als Anwendungen auf Büro-Rechnern, und ruft die historischen Anlagendaten vom Server ab.

In der Regel werden die Prozessdatenarchive über das Unternehmensnetzwerk für höhere Ebenen nutzbar gemacht, da diese teils auch für unternehmerische Tätigkeiten (z. B. Abrechnung) genutzt werden (können).

11.2.8.2 Realisierungsvarianten der Datenübertragung:

Das PLT-S-Logiksystem (IT3a) überträgt die Daten zum PLT-B-Logiksystem (IT3c). Das BDIS (IT8) holt sich die Daten über das PLT-B-Logiksystem (IT3b). Der Nachteil dieser Variante ist, dass ein höherer Aufwand, höhere Last innerhalb der PLT-B und evtl. ein Verlust des zeitlichen Bezugs der Signale auftritt. Ein Vorteil ist der Wegfall einer zusätzlichen Kommunikationsverbindung vom BDIS (IT8) zum PLT-S-Logiksystem (IT3a).

11.2.8.3 Gefährdungen

- Missbrauch für DoS-Angriff auf PLT-S-Logiksystem
- Ausleitung von Informationen. Rückschlüsse auf Sicherheitsparameter und -Funktionen möglich
- direkter Zugriff auf IT3c aus der OT-Infrastruktur
- Die historischen Daten werden zur Ableitung von Sollwerten genutzt. Bei einer Manipulation könnten damit diese Sollwerte verändert werden ohne direkten Zugriff auf entsprechende Geräte erlangen zu müssen.
- Replay-Attacke: Nutzung der Daten zum Vortäuschen eines validen Prozesses.

11.2.8.4 Gängige Absicherungsmaßnahmen

Mindestens Zeitstempel/Zähler (gegen Replay-Attacken), Verschlüsselung der Übertragung (eher selten), Identifizierung/Authentifizierung der Quellen, Segmentierung der Netzwerke

11.2.8.5 Daten

Aus den Daten können Prozessabläufe rekonstruiert und eventuell Schwellenwerte herausgefunden werden. Kritische Informationen für das PLT-S werden nicht erfasst.

11.2.9 IT9b Sprungserver

11.2.9.1 Allgemein

Er dient dazu, eine oder mehrere Verbindungen von entfernten Stationen zu ermöglichen. Er kann zentrale IT-Anwendungen bereitstellen. Er kann innerhalb von ICS Netzwerken oder zur Herstellung von Verbindungen von der IT-Infrastruktur in das ICS genutzt werden. Dafür wird pro Verbindung eine separate Session auf dem Server gestartet. Mittels dieser Session hat der Client die Möglichkeit, die gleiche Ansicht und Funktion zu erlangen, wie sie bei einer Bedienstation ist.

11.2.9.2 Verwendung in Modellarchitektur

Der Terminalserver kann auch als Jump Server dienen.

11.2.9.3 Gefährdungen

- je nach Zielkomponenten und Umgehung von Verbindungsbeschränkungen
- Gängige Absicherungsmaßnahmen
- Verwendung von mehreren Netzwerkkarten zwecks Zugangsbeschränkung und Netzsegmentierung

11.2.10 IT9d Datensicherung

11.2.10.1 Allgemein

Der Backup-Server ist zentraler Bestandteil des Backupmanagements. Dessen Aufgabe ist es allgemein, eine Datensicherung (inkl. Programme, Konfiguration, ggf. Betriebssystem) als sogenanntes Backup abzulegen und langfristig zu speichern. Im Falle des Ausfalls eines Systems kann ein Ersatz-System mit dem letzten Update neu aufgesetzt werden. Bei dem Backup-Server handelt sich um eine Softwarekomponente für Server oder einen eigenständigen Server. Zugang zu dieser Funktionalität ist Herstellerabhängig und erfolgt meist über das Netzwerk auf Speichersysteme mit Festplatten und oft von dort auf Magnetbänder.

11.2.10.2 Gefährdungen

- Schwache Absicherung wegen geringerer Relevanz/Prüfregularien? (leichte Passwörter, einfacher Zutritt)
- Manipulation (mit Ziel Sabotage)
- Informationsbeschaffung (IP Leakage, Programminhalte eines Logiksystems)
- Verzögerung der Wiederherstellung
- Backdoors ins Backup einpflegen

11.2.10.3 Gängige Absicherungsmaßnahmen

- Die gespeicherten Images brauchen Prüfsummen, die getrennt gespeichert werden, so dass Manipulationen der Datensicherungen auffallen und das Zurückspielen blockiert wird.
- Datensicherungen sollten fernab der Quelle gespeichert werden, um im Falle eines Brandes nicht mit der Quelle abhandeln zu kommen. Da cybersicherheitsrelevante Informationen und Intellectual Property

mitgespeichert werden und als Vorkehrung gegen Manipulation und Sabotage sollte die Lagerung zugangsbeschränkt sein.

- Zeitgemäße Verschlüsselung der Daten.

11.2.11 IT9f Updateservice

11.2.11.1 Allgemein

Der Updateservice ist ein zentraler Bestandteil des Patch- und Änderungsmanagement. Dessen Aufgabe ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.“ (1 S. OPS.1.1.3) Bei dem Updateservice handelt sich um eine Softwarekomponente für Server, über die sich Updates für Betriebssysteme und Anti-Viren-Software entkoppelt vom regulären Update-Service der Hersteller bereitstellen und installieren lassen.

Administratoren können selbst festlegen, welche Rechner mit welchen Updates zu einem bestimmten Zeitpunkt versorgt werden sollen. Es bieten sich umfangreiche Steuerungs- und Administrationsmöglichkeiten.

11.2.11.2 Gefährdungen

- Nicht alle Patche sind zugelassen, Freigabe für nicht patchfähige Komponenten
- Veraltete Signaturen werden verwendet.
- Schadcode bleibt unerkannt.

11.2.11.3 Gängige Absicherungsmaßnahmen

- Datenschleuse: Alle externen Daten gehen über diese Instanz zur Integritätsprüfung
- Integritätsprüfung der Patches

11.2.12 IT9g Verzeichnisdienst

11.2.12.1 Allgemein

Ein Verzeichnisdienst ist ein Server zur zentralen Authentifizierung von Computern und Benutzern in einem Rechnernetz. Es sind auch redundante Verzeichnisdienste einsetzbar, um im Fehlerfall nutzbar zu bleiben

Im Verzeichnisdienst kann festgelegt werden, welche Benutzer sich anmelden dürfen, zu welchen Benutzergruppen sie gehören und wie die Passwort-Regeln umgesetzt werden. Änderungen können für alle Computer oder Benutzer gelten, oder nur für Teilgruppen.

11.2.12.2 Verwendung in Modellarchitektur

Der Verzeichnisdienst ist entweder in der IT-Infrastruktur oder als separater Verzeichnisdienst mit eigener Domäne in der OT-Infrastruktur angeordnet.

11.2.12.3 Gefährdungen

- Veralteten Softwareversionen
- einfache Administrator Passworte
- schlechte/falsche Konfigurationen
- Datenbank (credentials) herunterladen und offline knacken.
- Domain-Adminrechte (worst case) Rechte geben

- Zusätzliche Konten anlegen

11.2.12.4 Protokolle

Transmission Control Protocol/Internet Protocol (TCP/IP) ist eine Gruppe von Netzwerkprotokollen. Die Identifizierung der am Netzwerk teilnehmenden Rechner, geschieht über IP-Adressen. Server Message Block (SMB) ist ein Netzprotokoll für Datei-, Druck- und andere Serverdienste in Rechnernetzen. Weiterhin kommt LDAP zum Einsatz.

11.2.12.5 Daten

Auf dem Verzeichnisdienst sind beispielsweise Rechnernamen, Benutzer und Berechtigungen der Benutzer gespeichert.

11.2.13 Weitere Dienste IT9h

Dieser Abschnitt beschreibt Beispiele für „Weitere Dienste“. Diese werden aber nicht explizit durchnummeriert.

11.2.13.1 IT9h DNS-Server

11.2.13.1.1 Allgemein

Ein DNS-Server führt die Namensauflösung im "domain name system" (DNS) aus und ist kein eigenes Gerät, sondern ein Systemdienst. Die Auflösung wechselt angefragte Namen eines Zielsystems in IP-Adressen um. Die Datengrundlage erstellt der Server selbst, sofern dieser der Verwalter der Zone ist oder übernimmt sie von einem hierarchisch übergeordneten System.

11.2.13.1.2 Verwendung in der Modellarchitektur

In Prozess-Leitsystemen wird vielfach auf die Verwendung von Namen für Netzwerkknoten verzichtet. Zum einen kostet die Namensauflösung Zeit. Zum anderen sind Cyber-Angriffe auf DNS bekannt. Nicht zuletzt macht die Verwendung der Namensauflösung die Prozesssteuerung von einem weiteren System, eben dem DNS-Server abhängig. Stattdessen kommen statische IP-Adressen zum Einsatz. Ad-hoc-Kommunikation mit Systemen, die nicht a priori bekannt waren, ist eher unüblich.

DNS kommt bei Active Directory zum Einsatz. Zudem kann es im Feld verwendet werden, wenn entsprechende Zugriffe auf Weboberflächen bspw. ein Logiksystem über den Domainnamen und nicht der IP-Adresse erfolgt.

Der Server wird meist von Automatisierungstechnikern aufgesetzt und gewartet.

11.2.13.1.3 Gefährdungen

DNS-Spoofing (der Angreifer beantwortet DNS-Abfragen anstelle des DNS-Servers und mit Fake-Adressen):

- Im Fall eines Logiksystems
 - Änderungen an der Software werden nicht durchgeführt. Dies gilt nur, wenn die Verbindung über das Netzwerk stattfindet.
 - Credentials werden abgegriffen
- Backup-Server:
 - Es wird kein Backup mehr angelegt
 - Das Backup wird an Dritte übertragen.

Hinweis: Es bleibt anzumerken, dass für Spoofing-Attacken, der Angreifer bereits tief im System vorgedrungen ist. Der DNS-Server ist dann ein unübliches Ziel.

- DOS-Attacken auf DNS-Server (Ausfall des Servers)
 - solange die DNS-Daten im Cache der kommunizierenden Komponenten vorgehalten werden, hat ein Ausfall des DNS Servers keine unmittelbare Auswirkung
 - mittelbare Auswirkung hat das DNS Spoofing nur bei neuer Etablierung von Kommunikationsanfragen

11.2.13.1.4 Daten

Es werden Daten im Zone-Cache gespeichert, die für die Integrität oder Funktionsfähigkeit der PLT-S wesentlich sind.

11.2.13.2 IT9.5 Netzwerküberwachung, Monitoring, IDS

Informationen für Einstieg und Vertiefung zu den Themen Netzwerküberwachung, Monitoring und Intrusion Detection Systems finden sich unter anderem in folgenden Dokumenten:

- Baustein DER.1 Detektion von sicherheitsrelevanten Ereignissen
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium Einzel PDFs 2023/05 DER Detektion und Reaktion/DER 1 Detektion von sicherheitsrelevanten Ereignissen Edition 2023.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_1_Detektion_von_sicherheitsrelevanten_Ereignissen_Edition_2023.pdf)
- Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen
https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/PDCA/PDCA_node.html
- Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html>
- Leitfaden zur Einführung von Intrusion Detection Systems
https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/IDS02/index_hm.html

11.2.13.3 QR-/Barcodescanner

Über einen Scanner werden Daten erfasst und für die weitere Verwendung vorgesehen. Die Informationen gelangen über einen Rechner an das Leitsystem und gehen direkt in die Rezepte ein. Bei einer Manipulation könnte die Reihenfolge der Zutaten vertauscht werden.

11.2.13.4 Print-Server

Es ist durchaus üblich, dass Informationen über das BDIS in die IT-Infrastruktur weitergeleitet werden. Dies gilt auch für Druckanfragen. Der Drucker ist Teil der IT-Infrastruktur, da das Leitsystem eventuell keinen lokalen Drucker hat. Damit besteht eine Verbindung in die IT-Infrastruktur.

11.2.13.5 Gebäudesteuerung

Eine Manipulation oder Störung kann die Auswirkung A1 haben. Über die der Gebäudeautomation zugeordneten Systeme kann der Betrieb gestört werden, bspw. Lichtsteuerung, Klimatisierung oder ggf. Produkte zerstört werden.

11.2.13.6 Zeitsynchronisation

Wird die Systemzeit der Netzmanagement-Komponenten unzureichend synchronisiert, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame

Basis aufweisen. So kann auf Ereignisse nicht angemessen reagiert werden. Probleme können zudem nicht beseitigt werden. Dadurch können beispielsweise Sicherheitsvorfälle und Datenabflüsse unerkannt bleiben.

11.2.14 IT10 – IT-Infrastruktur

Die IT-Infrastruktur umfasst Netzwerke, Server und Arbeitsplatzrechner. Eine Betrachtung dieser Komponenten findet nicht statt.

11.2.15 Netzwerkkomponenten

Die physische Netzwerkstruktur und die dort eingesetzten Komponenten werden in diesem Dokument nicht betrachtet. Der Grund dafür ist, dass sich der Aufbau des Netzwerks stark von den Gegebenheiten in der Anlage und dem Hersteller unterscheidet. Beim Absichern der Anlage müssen diese Komponenten mitbetrachtet und vor Zugriffen geschützt werden.

Dies gilt insbesondere, wenn an die Netzwerksegmente durch PLT-S und PLT-B gemeinsam genutzt werden oder ein Zonenübergang möglich ist.

11.2.15.1 N1-Switch

Die Switches verbinden Systeme miteinander, die über die gleiche Art kommunizieren und können als Verteiler gesehen werden. Im Umfeld industrieller Steuerungsanlagen sind diese auf die besonderen Einsatzumgebungen (z. B. hohe oder wechselhafte Temperaturen, Feuchtigkeit, Vibration) ausgelegt.

Für den Switch im OT-Umfeld sind im Wesentlichen die Schutzziele Verfügbarkeit und Integrität von Bedeutung. Im OT-Umfeld kann, in Abhängigkeit der übertragenen Informationen, auch das Schutzziel Vertraulichkeit relevant sein.

11.2.15.2 N2-Firewall

Eine Firewall ist ein Sicherungssystem, das ein Netzwerk von einem anderen Netzwerk trennt und durch den Einsatz von Regeln die Kommunikation steuert und unter Umständen blockiert. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente.

Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absenderadresse und/oder Zieladresse, und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise unterbindet die Firewall unerlaubte Netzwerkzugriffe.

Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer Personal Firewall (auch Desktop Firewall) und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall genannt). In Abgrenzung zur Personal Firewall arbeitet die Software einer externen Firewall nicht auf dem zu schützenden System selbst, sondern auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet und dank der Firewall-Software gleichzeitig den Netzwerkverkehr zwischen den Netzen kontrolliert und beschränkt.

11.2.15.3 N3 Gateway

Ein Gateway hat die Eigenschaft, dass es die als Protokollumsetzer fungiert, das die Kommunikation zwischen verschiedenen Systemen ermöglichen kann, die unterschiedliche Kommunikationsarten (z. B. Modbus <-> TCP) verwenden. Das tritt i.d.R. bei der Kommunikation zwischen Systemen unterschiedlicher Ebenen ein. Ein Gateway kann demnach als Übersetzer gesehen werden.

Typische Gateway-Komponenten sind

- Prozessankopplung,
- OPC-Server (genutzt als OPC Gateway),

- HART-Gateway und
- Firewall.

Das HART-Gateway dient als Kommunikationsschnittstelle zwischen Komponenten der Einheiten- bzw. Stationsebene und der Feldebene. Es dient im Wesentlichen dem Verwalten, Konfigurieren und Parametrisieren von angeschlossenen Geräten.

Beim Gateway sind im OT-Umfeld vor allem die Schutzziele Verfügbarkeit und Integrität relevant. Es ist anzumerken, dass die Architektur von OT meist so ausgelegt ist, dass ein Ausfall des Gateways nicht zu einem Ausfall des Prozesses bzw. der Prozesssteuerung, sondern (nur) zu einer Loss-of-View in der Steuerungsebene oder zentralen Leitebene führt. Das Schutzziel Vertraulichkeit ist für Gateways in der Regel nicht besonders relevant.

11.3 Anhang C Mapping

Tabelle 17 Mapping von KAS-51, ISO/IEC 27001:2018 und IT-Grundschutz

Aspekte der Informationssicherheit	KAS-51	ISO/IEC 27001:2018	IT-Grundschutz-Kompodium 2022
Festlegung von Verantwortlichkeiten	4.1	5	ISMS.1 Sicherheitsmanagement
Zugangs- und Zutrittsmanagement und -überwachung	4.2	A.5.15	INF.1 Allgemeines Gebäude
Zugriffsmanagement und Prozesssteuerung	4.3	A.8.3	ORP.4 Identitäts- und Berechtigungsmanagement
Manipulationserkennung und -schutz	4.4	A.6.8	DER.1 Detektion von sicherheitsrelevanten Ereignissen
Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	4.5	A.5.19	OPS.2.1 Outsourcing für Kundschaft OPS.3.1 Outsourcing für Dienstleistungsunternehmen ORP.2.A4 Festlegung von Regelungen für den Einsatz von Fremdpersonal
Sensibilisierung/Schulung eigener Arbeitskräfte	4.6	A.6.3	ORP.3 Sensibilisierung und Schulung
Reaktion auf neue Schwachstellen und IT-Bedrohungen	4.7	A.6.8	DER.2.1 Behandlung von Sicherheitsvorfällen
Entscheidung über das Vorliegen einer besonderen Gefährdung	5	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Bedrohungsanalyse	6.1	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Gefahrenanalyse	6.2	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS

Aspekte der Informationssicherheit	KAS-51	ISO/IEC 27001:2018	IT-Grundschutz-Kompendium 2022
IT-Risikoanalyse	6.3	8	BSI Standard 200-3 Risikoanalyse auf der Basis von IT-GS
Schutz vor physischen Eingriffen Unbefugter (Außentäter)	7.1.1	A.7	Bausteine der Schicht "Infrastruktur" z.B. INF.1 Allgemeines Gebäude
Schutz vor unbefugten Eingriffen durch Innentäter	7.1.2	A.5.15 A.5.16 A.5.17 A.5.18	ORP.4 Identitäts- und Berechtigungsmanagement
Einführung in Sicherheitsmanagement	7.2.1	A.5	ISMS.1 Sicherheitsmanagement
Schutz vor cyber-physischen Angriffen	7.2.2	A.8.20 A.8.21 A.8.22	NET.1.1 Netzarchitektur und -design
Schutz vor Drohnenangriffen	7.2.3	A.7.1	Bausteine der Schicht "Infrastruktur" z.B. INF.1 Allgemeines Gebäude
Sicherheitsmanagement	A1	A.5.1 A.5.2 A.5.3 A.5.5 A.5.6 A.5.8 A.5.9	ISMS.1 Sicherheitsmanagement
Hinweise auf Drohungen auf Betriebsbereiche nach 12. BImSchV	A3	n/a	-

11.4 Anhang D Glossar

Begriff	Erläuterung
Aktoren	Geräte, die mittels normierter Signale den physikalischen Prozess beeinflussen können. Aktoren können u.a. Pumpen, Verdichter oder Regelventile sein.
Betriebsdateninformationssystem (BDIS)	Betriebsdateninformationssystem sammelt und integriert Informationen über einen Produktionsprozess aus verschiedenen Quellen. Quelle: Wikipedia, PIMS
Bus-System	System zur Übertragung von Daten zwischen mindestens zwei Teilnehmern über ein gemeinsames Medium; in der Prozessautomationstechnik eingesetztes Kommunikationssystem.
Chemieanlage	Verfahrenstechnische Produktionsanlagen zur Herstellung chemischer Produkte.

Begriff	Erläuterung
Feld	Bereich der Anlage, in dem sich das verfahrenstechnische Equipment (u. a. Behälter, Rohrleitungen und Feldgeräte) befindet. Dies kann ein Gebäude oder auch den Außenbereich umfassen.
Funktionale Sicherheit Safety	Teil der Gesamtsicherheit, der sich auf die Fähigkeit eines Systems bezieht, eine bestimmte Funktion sicher auszuführen. Im Rahmen des Grundschutzprofils soll hierunter die Absicherung von Prozessen durch Prozessleittechnik verstanden werden.
Firewall	System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. (5)
Geltungsbereich	Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. (1)
HART-Protokoll	Das HART-Protokoll (Highway Addressable Remote Transducer) dient dem normierten Übertragen von Daten der Sensoren und Aktoren.
Bedienstation	Schnittstelle, die zum Bedienen, zum Beobachten und bei Bedarf zum Eingriff in den Prozess eingesetzt wird.
Gemeinsam genutzte Komponente	Unter gemeinsam genutzten Komponenten im Sinne der Cybersicherheit werden Geräte verstanden, mit deren Hilfe sowohl Sicherheitsfunktionen als auch Betriebsfunktionen ausgeführt, konfiguriert oder programmiert werden. Ein Sensor kann beispielsweise sowohl für die Betriebs- als auch die Sicherheitsfunktion Daten bereitstellen.
Industrial Control System (ICS)	Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse. Sie bestehen in der Regel aus einem redundanten Produktionsnetzwerk, Sensoren, Aktoren, Steuerungen und Rechnern mit unterschiedlichen Aufgaben. Sie dienen der Steuerung von Anlagen.
Informationsverbund	Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen (1).
Institution	Oberbegriff für Unternehmen, Behörden und sonstige öffentliche oder private Organisationen (1).

Begriff	Erläuterung
Informationssicherheitsmanagement-system (ISMS)	Die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind (1).
Informationstechnik (IT)	Alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen (1).
integrierte Komponente	Dies bezeichnet die Zusammenführung von mehreren Funktionen in einer Komponente.
Komponente	Eine Komponente ist in der Softwarearchitektur eine eigenständig einsetzbare Einheit mit Schnittstellen nach außen, die mit anderen Komponenten verbunden werden kann. Sie ist sowohl fachlich als auch technisch unabhängig und besitzt eine gewisse Größe (im Sinne eines wirtschaftlichen Wertes) (1).
Leitstand	Räumlichkeit oder Bedienstation, von der aus die Chemieanlage überwacht und bedient wird.
Logiksystem	Ein Logiksystem kann aus einer nicht programmierbaren Logik z.B. einem Relais oder einer programmierbaren Steuerung bestehen. Die Software ist ggf. ein Teil des Logiksystems. Im Text wird unterschieden zwischen sicherheitsgerichteten Logiksystemen (kurz: PLT-S-Logiksystem) und nicht sicherheitsgerichteten Logiksystemen (kurz: PLT-B-Logiksystem).
Manufacturing Execution System (MES)	Software, die in der Betriebsleitebene der Automatisierungspyramide eingesetzt wird. Sie dient u.a. der Produktionsplanung, Ressourcenplanung und Wartung.
Modellierung	Bei der Vorgehensweise nach IT-Grundschrift wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschrift-Kompendium nachgebildet. Hierzu enthält Kapitel 2.2 der IT-Grundschrift-Kompendium für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind (1).
Operational Technology (OT); Betriebstechnik	Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert

Begriff	Erläuterung
PAAG-Verfahren	<p>In Deutschland verbreitete Methode zur systematischen Gefahrenanalyse für Prozessanlagen, abgeleitet aus der international etablierten HAZOP (HAZard and OPerability) Systematik</p> <p>Akronym für die Verfahrensschritte:</p> <ul style="list-style-type: none"> • Prognose, • Auffinden der Ursachen, • Abschätzen der Auswirkungen und • Gegenmaßnahmen.
PLS	<p>Meist für größere verfahrenstechnische Anlagen eingesetzt. Es bildet üblicherweise ein Gesamtsystem, das folgende Mechanismen beinhaltet:</p> <ul style="list-style-type: none"> • Prozessnahe Komponenten zur Steuerung von Aktoren und Aufnahme von Messwerten, • Alarmsystem, • Anlagenvisualisierung, • Kurvenaufzeichnung von analogen Messwerten, • Verwaltung der Nutzenden, • Möglichkeiten des Engineerings sowie • eine zentrale Datenhaltung.
Prozessleittechnik (PLT) Process Control Technology (PCT)	Mittel und Verfahren, die dem Steuern, Regeln und Absichern verfahrenstechnischer Anlagen dienen
PLT-Sicherheitseinrichtung (PLT-S) Englisch: Safety Instrumented System (SIS)	Realisierung einer Sicherheitsfunktion (SIF) durch Prozessleittechnik entsprechend IEC 61511.
PLT-Betriebseinrichtung (PLT-B) Englisch: Business Process control system (BPCS)	Realisierung einer Betriebsfunktion durch Prozessleittechnik
PLT Betriebseinrichtung mit Sicherheitsfunktion (PLT-BS)	Realisierung einer Sicherheitsfunktion durch Prozessleittechnik entsprechend VDI/VDE 2180 mit einem Risikoreduzierungsfaktor von maximal 10, z. B. unter Nutzung des Prozessleitsystems
Remote-I/O	Ein Remote-I/O-Modul verbindet in der Regel mehrere binäre oder analoge Sensoren und Aktoren mit einem weiter entfernten beziehungsweise räumlich getrennten Leitsystem oder Steuerung.
Restrisiken	Risiko, das übrigbleibt, welches nicht durch Maßnahmen abgedeckt werden kann
Schaltraum	Ein Schaltraum ist eine Räumlichkeit, in der elektrische Geräte stehen, die für den Betrieb einer Chemieanlage erforderlich sind.
Sensoren	<p>Sensoren sind Geräte, die zur Aufnahme von physikalischen Größen dienen. Sie wandeln diese in normierte Signale um. Sensoren können u.a. Druckmessungen, Füllstandmessungen oder Durchflussmessungen sein.</p>

Begriff	Erläuterung
Speicherprogrammierbare Steuerung (SPS)	Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird. Sie ist ein Beispiel für PLT-B-Logiksysteme.
Sicherheitsgerichtete speicherprogrammierbare Steuerung (SSPS)	Sicherheitsgerichtete-SPS gewährleisten das geforderte Maß an Sicherheit und Verfügbarkeit für den Einsatz in sicherheitskritischen Systemen. Sie ist ein Beispiel für ein PLT-S-Logiksystem.
Störfall	Ereignis, das unmittelbar oder später zu einer ernsten Gefahr (für Menschen oder die Umwelt) oder zu erheblichen Sachschäden führt. Die entsprechenden Schwellen und Begriffe gehen aus der 12. BImSchV hervor. Ein solches Ereignis kann z. B. von einer Chemieanlage mit bestimmten großen Mengen gefährlicher Stoffe herrühren.
Zielobjekt	Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus den IT-Grundschutz-Katalogen zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

Literaturverzeichnis

1. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutzkompendium. [Online] 2023. [Zitat vom: 10. 01 2024.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.
2. **National Institute of Standards and Technology.** SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security. [Online] 2023. [Zitat vom: 10. 01 2025.] <https://csrc.nist.gov/pubs/sp/800/82/r3/final>.
3. —. SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. [Online] 2018. [Zitat vom: 10. 01 2025.] <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.
4. **NAMUR.** NE 154 "Funktionale Sicherheit in Batch-Prozessen". 2023.
5. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutz-Kompendium NET 3.2 Firewall. [Online] 2023. [Zitat vom: 10. 01 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.html.
6. —. ICS-Security-Kompendium. [Online] 2024. [Zitat vom: 10. 01 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html.
7. —. IT-Grundschutz-Kompendium IND.1 Prozessleit- und Automatisierungstechnik. [Online] 2023. [Zitat vom: 10. 01 2025.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2023.pdf.