Landesamt für Natur,
Umwelt und Verbraucherschutz
Nordrhein-Westfalen

Orientierungspapier

Darstellung der IT-Sicherheit im Sicherheitsbericht und in den Genehmigungsunterlagen zur Anlagensicherheit

Stand:

April 2021

Inhaltsverzeichnis

Seite

1. Einleitung 3

2. Netzwerkarchitektur / Zonenmodelle 5

3. Assetlisten 9

4. IT-Risikoanalyse / IT-Risikobeurteilung 11

5. Literaturquellen 15

Anhang: Abbildung Nr. 3: Beispiel für die Darstellung eines Netzwerkdiagramms in einer hohen Detailstufe

Die Entwurfserstellung erfolgte durch Stephan Gebhard (FB 74) unter Mitarbeit von Birgit Richter (FB 75). Die Endfassung enthält die Umsetzung der Rückmeldungen aus dem Arbeitsbereich Anlagensicherheit (Beschäftigte der Fachbereiche 74 und 75).

1. Einleitung

Die Entwicklungen der letzten Jahre haben dazu geführt, dass die IT[1] (Informationstechnologie) immer mehr Eingang in OT[2] (Operationstechnologie), deren Infrastrukturen, Funktionen und Prozesse, gefunden hat. Daher ist es nötig Anforderungen an die IT-Sicherheit von Industrieanlagen in der Anlagensicherheit zu berücksichtigen. Neben einem Verhindern von Eingriffen Unbefugter ist dies auch unter dem Gesichtspunkt der systematischen Fehlerfindung und Funktionsprüfung/-überwachung in modernen logikbasierten Systemen notwendig. Diesen Umständen tragen u.a. auch der umgestaltete KAS-51 (ehemals SFK-GS-38) /1/ der Kommission für Anlagensicherheit und die runderneuerte VDI/VDE 2180 /2/ Rechnung.

Bezugnehmend auf die Kernaspekte der IT-Sicherheit, also das Sicherstellen von Geheimhaltung, Integrität und Verfügbarkeit (von Daten bzw. Signalen), sind in Bezug auf die Anlagensicherheit nur die Belange der Integrität und Verfügbarkeit direkt sicherheitsrelevant (dessen unbeschadet ist es natürlich zumeist im starken Interesse der Betreiberin ebenfalls die Geheimhaltung zu gewährleisten).

Das primäre Ziel im Sinne der Störfall-Verordnung ist der Schutz der sicherheitsrelevanten Anlageteile (nachfolgend srA genannt) und der damit in Verbindung stehenden Subsysteme und ihre Darstellung im Sicherheitsbericht. Die IT-Sicherheit wird unter diesem Kontext betrachtet, das heißt vorrangig alle IT-Elemente, die die Integrität und Verfügbarkeit von srA beeinflussen können.

[1] Informationstechnik (IT) umfasst 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. [Übernommen aus dem BSI Glossar]

[2] Betriebstechnik (englisch: Operational Technology (OT)) ist Hard- und Software, die Änderung durch die direkte Überwachung und / oder Steuerung von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erfasst und bewirkt. [Übernommen aus dem BSI Glossar]

Dieses Papier definiert die zum gegenwärtigen Zeitpunkt notwendigen Minimalanforderungen an die Darstellung von IT-Aspekten im Sicherheitsbericht sowie in beizubringende Unterlagen im Rahmen von Genehmigungsverfahren.

In Hinblick auf die Art und Detailtiefe der Darstellung wurde sich hier an den Anforderungen zu anderen Inhalten im Sicherheitsbericht orientiert.

Der Detailierungsgrad muss geeignet sein, ein Nachvollziehen und eine Prüfung der Sicherheitsmaßnahmen und deren Schnittstellen zu ermöglichen. Je nach Größe einer Anlage kann es hilfreich sein, verschiedene Anlagenbereiche /Anlagenabschnitte in verschiedenen Detailierungsgraden darzustellen.

Die Mindestanforderungen an die Beschreibung von IT-Aspekten im Sicherheitsbericht beinhalten die Darstellung der:

a. Netzwerkarchitektur und Zonenmodelle,
b. Assetlisten,
c. IT-Risikoanalyse / IT-Risikobeurteilung.

In Analogie zu den klassischen Aspekten der Anlagensicherheit, entsprechen die IT-Aspekte

a. Netzwerkarchitektur / Zonenmodelle
   ⇒ Fließbildern des Verfahrensablaufes einer Anlage, je nach Detailtiefe: Block-, Verfahrens-, R&I - Fließbild),
b. Assetlisten
   ⇒ der Auflistung von sicherheitsrelevanten Anlagenteilen aufgrund ihres Stoffinhaltes sowie der besonderen Funktion (srA-Listen),
c. IT-Risikoanalyse / IT-Risikobeurteilung
   ⇒ der klassischen Gefahrenanalyse.

In den folgenden Kapiteln werden diese drei IT-Aspekte erläutert und Mindestanforderungen für die Darstellung genannt. Voraussetzung hierfür ist aber, dass die Betreiberin die aufgeführten Komponenten auch verwendet.

Die im Sicherheitsbericht dargestellten IT-Risikoanalysen, Netzwerkdiagramme und Assetlisten müssen in sich konsistent sein.

2. Netzwerkarchitektur / Zonenmodelle

Es wird empfohlen dem Sicherheitsbericht folgendes beizufügen:

- Ein Netzwerkdiagramm mit niedriger Detailstufe (siehe z. B. Abb. 1 bzw. 2) Dies dient dazu insbesondere die Übergänge der OT zur IT darzustellen und einen Gesamtüberblick zu erhalten.
- als auch ein Netzwerkdiagramm mit hoher Detailstufe (siehe z. B. Abb. 3) Dies dient dazu die Verbindungen innerhalb der OT und insbesondere die Verbindungen innerhalb und zu den srA darzustellen.

Netzwerkdiagramme (auch als Netzwerkarchitekturen, Netzwerkpläne oder Netzwerkstrukturen bezeichnet) sind maßgeblich für die Verständlichkeit und Überprüfbarkeit der IT-Kommunikationsverbindungen / Kommunikationsinfrastruktur. Die beiden folgenden Abbildung Nr. 1 und Nr. 2 zeigen Darstellungen der Netzwerkarchitektur / Zonen, welche für einen groben Überblick geeignet sind.

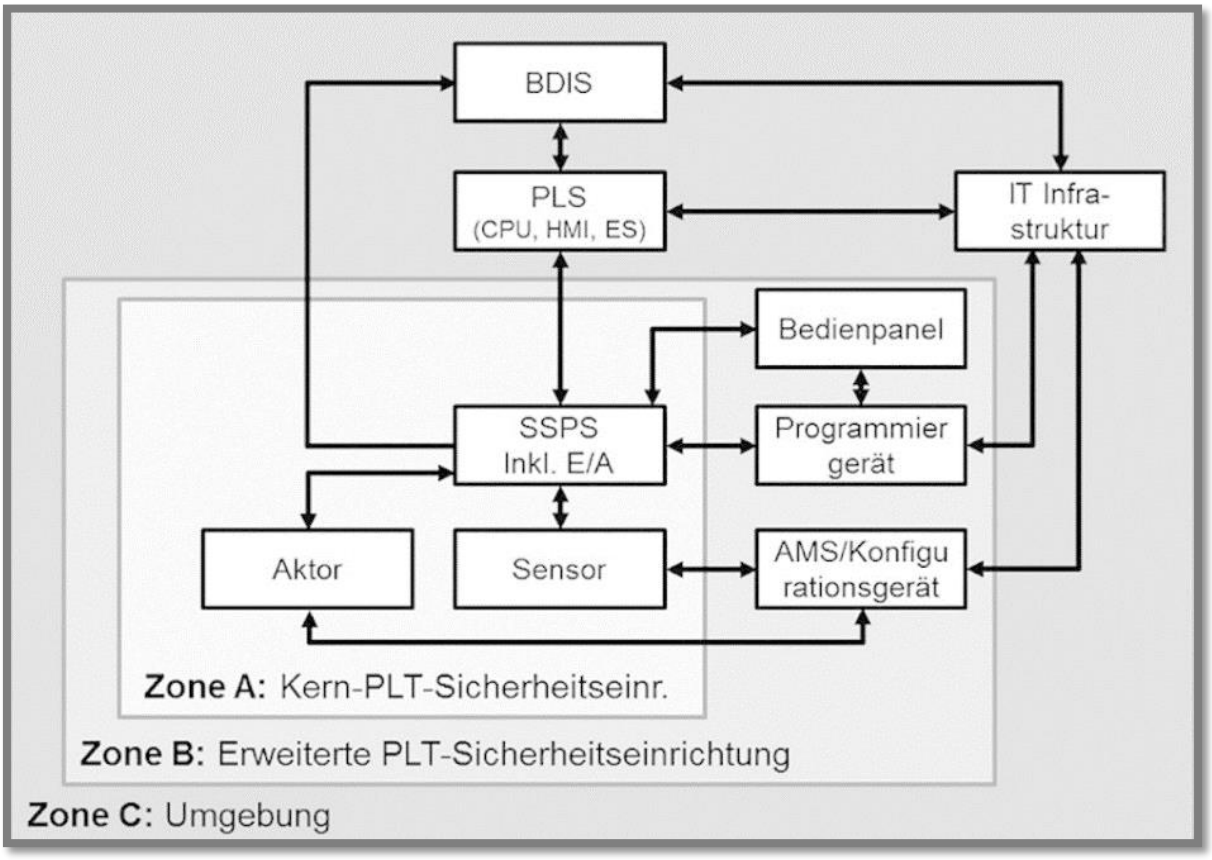


Abb. Nr. 1: Netzwerkarchitektur / Zonen nach dem Zonenmodell der NA 163 /3/

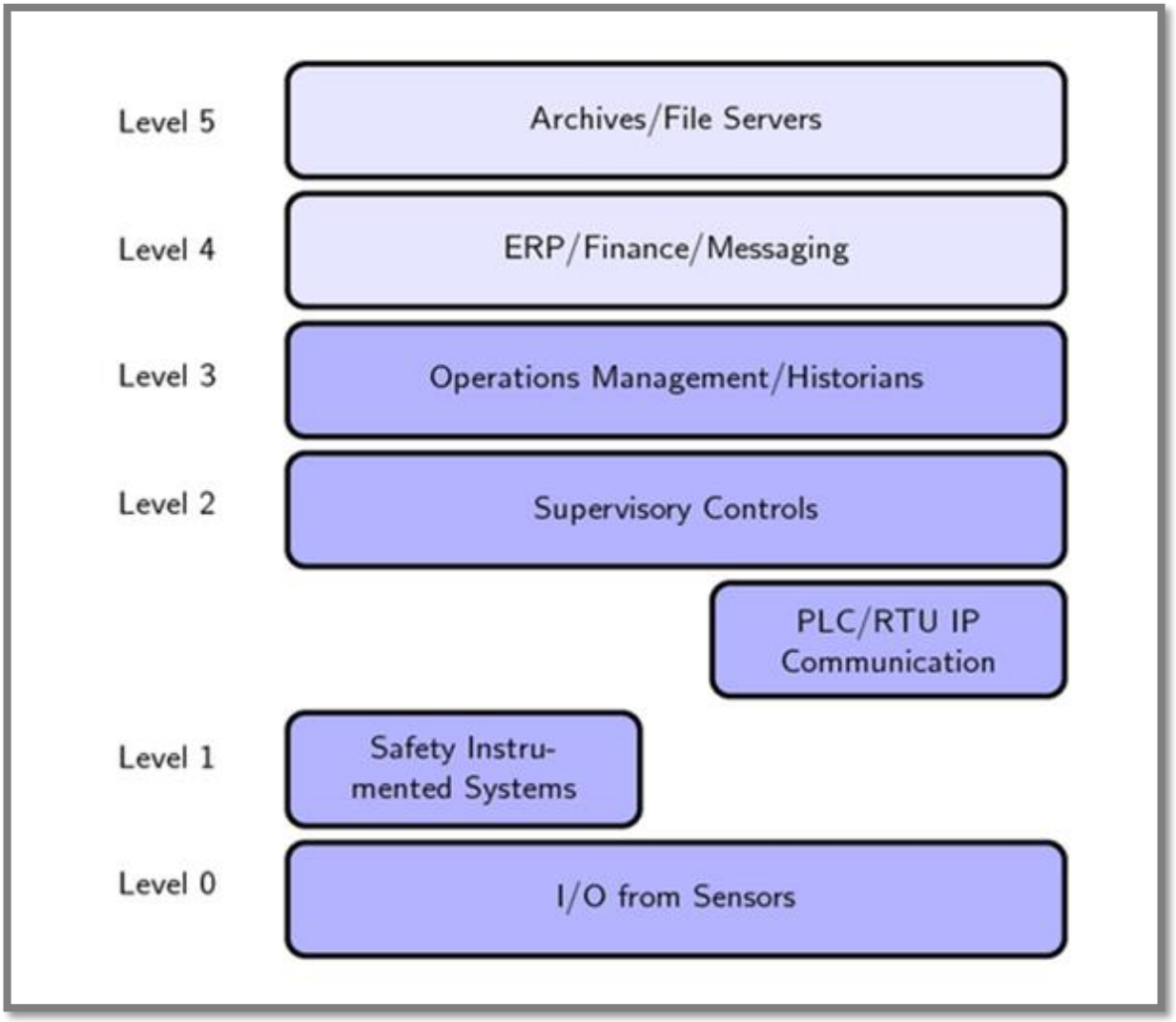


Abb. Nr. 2: Netzwerkarchitektur / Zonen nach dem Purdue Modell /4/

Abbildung 2 zeigt eine allgemeingültige Aufteilung eines Netzwerkes in einem Unternehmen. Level 0 – 3 finden sich ausschließlich in der OT. In Level 4 und 5 finden sich klassische IT-Systeme zur Auftragsverwaltung, Bürokommunikation und Arbeitsplatzrechner.

Der Schwerpunkt der Netzwerkarchitektur ist auf die Darstellung

- der Kommunikationsverbindungen innerhalb der OT Ebene (Level 0-3) und
- deren Anbindung (Schnittstellen) an andere Ebenen der IT / Netzwerke / Zugänge sowohl innerhalb wie außerhalb der Verantwortung der Betreiberin (Übergange von Level 0 - 3 zu Level 4 & 5)

zu legen.

Aktualität und Vollständigkeit sind zu gewährleisten, temporäre Lösungen, Ausweichverbindungen etc. sind darzustellen.

Die Abbildung Nr. 3 im Anhang zeigt die Darstellung eines Netzwerkdiagramms in einer hohen Detailstufe und ist ein Beispiel für die Umsetzung der im folgenden genannten Mindestanforderungen.

<u>Mindestanforderungen (ausgehend von den srA):</u>

- Darstellung und Bezeichnung der sicherheitstechnisch relevanten Sensoren (inklusive PLT-BS), Aktoren und Logiksysteme. Dies schließt hybride Bauteile[3] und vollintegrierte Systeme[4] mit ein.
- Darstellung und Bezeichnung von beteiligten Bauteilen wie z.B. Routern, Switchen, DMZ Systemen (Firewalls) etc.
- Darstellung und Bezeichnung der verwendeten Übertragungsstrukturen (Busstrukturen, Funknetze etc.).
- Darstellung und Bezeichnung der Schnittstellen zu anderen Komponenten bzw. Subsystemen (Computern, Bauteilen, Netzwerken, HMI's etc.)
- Darstellung und Bezeichnung von sämtlichen Zugangswegen zu oben genannten Systemen (einschließlich Zugänge, welche Level „überspringen" oder „durchstechen")
- Darstellung sämtlicher auf der Assetliste verzeichneten Elemente, welche im Bezug zur Anlagensicherheit stehen (inklusive situativer oder temporärer Anbindungen).

[3] Hybride Bauteile (auch gemeinsam genutzte Bauteile genannt) sind nicht exklusiv SPS bzw. SSPS zugeordnet, sondern sind in beide Loops eingebettet. Z.B. Sensoren mit hohem SIL-Level welche Betriebseinrichtungen und in sicherheitsgerichteten Loops verwendet werden.

[4] Vollintegrierte Systeme sind z.B. Logiksysteme die sowohl die Aufgaben der Betriebseinrichtungen als auch der sicherheitsgerichteten Steuerungen orchestrieren. Es handelt sich dabei zumeist um ein in sich geschlossenes Hardwarebauteil. Die Priorisierte Signalweiterleitung und Bearbeitung von sicherheitsgerichteten Aufgaben erfolgt dabei durch interne Prozesse (zum Teil mittels eigenen Logiksubsystemen). Bei Kompromittierung der SPS droht hier somit auch Betroffenheit der SSPS weswegen es nötig sein kann SPS Loops auf dem Niveau der SSPS abzusichern.

Art der Darstellung:

Ausgehend von der fehlenden normativ geregelten Art der Darstellung haben sich diverse Darstellungsformen (insbesondere was die Symbolik betrifft) etabliert. Üblich sind z.B. Darstellungen mit Symbolbibliotheken (z. B. von Cisco-, AWS- oder Azure). Legenden mit Benennung/Erläuterung der verwendeten Symbole in den Netzwerkdiagrammen sind beizufügen. Es ist auf eine allgemeine verständliche Darstellungsweise zu achten.

3. Assetlisten

Assetlisten enthalten Objekte (Hard-, Software und Daten) die Betreiberinnen für sich als schützenswert definiert haben. Das Spektrum reicht hierbei normalerweise von Patenten bis hin zu sicherheitsgerichteten Steuerungen. Assetlisten sind neben Netzwerkdiagrammen die zweite unabdingbare Informationsquelle. Inhalt und Darstellung sind recht variabel, neben dem Asset-Namen und seinem Eigentümer / Prozess werden oftmals weitere Informationen, wie zum Beispiel Asset-Kategorie, Standort, damit in Verbindung stehende Elemente, Versionsnummern / Inventarnummern, darauf ggf. laufende Software, Versionsnummern der Software etc. hinterlegt.

Für die Anlagensicherheit ist zumeist nur ein kleiner Teil der Assetliste von Bedeutung. Es ist aber darauf zu achten, dass zusammen mit dem Netzwerkdiagramm und R & I Kennzeichnungen eine kompatible und nachvollziehbare (in sich schlüssige) Darstellung entsteht.

Assetname	**Prozess**	**Schnittstellen**
Aktor 1(R&I Kennzeichnung)	Kühlkreislauf Prozess X	Bussystem XZ,
Bussystem XY	Kühlkreisläufe der Prozesse X und Überlaufschutz Tank Y	Sensor 1, Sensor 2, Sensor 3, Aktor 1, Logiksystem X
Logiksystem X	Kühlkreislauf Prozess X (Nutzung durch SPS + SSPS; vollintegriert)	Bussystem XY, Fernwartungszugang XZ,…
Sensor 1 (R&I Kennzeichnung)	Kühlreislauf Prozess X (Nutzung durch SPS und SSPS)	Bussystem XY, Sensor 2 für innerbetriebliche Funktionsprüfung
Sensor 2(R&I Kennzeichnung)	Kühlkreislauf Prozess X	Bussystem XY, Sensor 1 für innerbetriebliche Funktionsprüfung
Sensor 3 (R&I Kennzeichnung)	Überlaufschutz Tank Y	Bussystem XY, …..
Fernwartungszugang XZ	Logiksystem XZ	Logiksystem X, …..
Programmiergerät (Laptop)	Variabel	Variabel (Instandhaltungsschnittstelle)

Abb. Nr. 4: Beispiel: für einen abstrahierten Auszug einer Assetliste

Mindestanforderungen:

- Auszug der Assetliste mit allen sicherheitstechnisch relevanten Bauteilen (also Sensoren, Aktoren, Logiksysteme und Programmiergeräte (z.B. Laptops), inklusive PLT-BS), mit Zuordnung zu den Messstellen (R&I Kennzeichnung) zum jeweiligen Verfahrensprozess bzw. vom SSPS mitverwendeten Systemen.
- Darstellung der Systeme die einen direkten Einfluss/Zugriff auf oben genannten Bauteilen haben oder sonst von Relevanz für die Sicherheit sind bzw. sein können (Schnittstellen).
- Zuordnung der einzelnen Assets zu einem / mehreren Prozessen (Logikloops etc.)
- Kennzeichnung hybrider oder vollintegrierte Bauteile (also Bauteile die SPS + SPSP Funktionen in einem beinhalten)

4. IT-Risikoanalyse / IT-Risikobeurteilung

Die VDI/VDE 2180 „Funktionale Sicherheit in der Prozessindustrie“ schreibt eine IT-Risikobeurteilung generell vor: „Um das Gefährdungspotenzial einzuschätzen und geeignete Gegenmaßnahmen festzulegen, muss eine IT-Risikobeurteilung durchgeführt werden.“ (/2/, Blatt 1, Kapitel 8.1).

Gemäß KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ /1/ ist eine IT-Risikobeurteilung nur dann nötig, wenn von einer besonderen Gefährdung (durch den Betriebsbereich) im Sinne des Leitfadens auszugehen ist. Dies ist bei den meisten Betriebsbereichen der oberen Klasse primär zu unterstellen, es ist jedoch immer eine Einzelfallenscheidung so dass auch Ausnahmen möglich sind.

Eine systematische Gefahrenabschätzung für IT / OT ist ohne IT-Risikobeurteilung nur schwerlich realisierbar, daher ist in Analogie zur klassischen Gefahrenanalyse eine IT-Risikobeurteilung durchzuführen und zumindest deren zugrunde gelegte Methode und die Ergebnisse, einschließlich der daraus resultierenden Maßnahmen, im Sicherheitsbericht darzulegen. Die Definition der IT-Risikobeurteilung (gemäß KAS-51) lautet:

„Die IT-Risikobeurteilung

• erfasst Schwachstellen aus Sicht der IT-Sicherheit für alle im Betriebsbereich eingesetzten Assets.
• erfasst IT-Gefährdungen aus Sicht der IT-Sicherheit. IT-Gefährdungen sind IT-Bedrohungen, die von extern oder intern über Schwachstellen auf Komponenten und Systeme einwirken können.
• identifiziert die möglichen Auswirkungen der IT-Gefährdungen auf die Integrität und Verfügbarkeit der sicherheitstechnischen Funktionen (nach DIN EN 61511 /5/) (Auswirkungsanalyse) und
• bewertet diese anhand der Wahrscheinlichkeit des Ausnutzens der IT-Schwachstelle.“

Die offizielle Beschreibung einer IT-Schwachstelle gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI) /6/ lautet: „Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.“

Ein Beispiel um die Begrifflichkeiten zu verdeutlichen:
Eine SSPS kann über einen USB-Port konfiguriert werden. Der USB-Port ist frei zugänglich. Hierbei handelt es sich um eine Schwachstelle, weil es sich um einen ungeschützten Zugang handelt. Eine Bedrohung ist in diesem Fall, dass eine unberechtigte Person den USB-Port missbraucht und die SSPS umkonfiguriert. Aus der Schwachstelle und der Bedrohung resultiert die Gefährdung einer unberechtigten Änderung der Konfiguration der SSPS. Aus der Gefährdung resultiert in dem Beispiel das Risiko, dass durch die manipulierte Konfiguration ein sicherheitsrelevanter Grenzwert verändert wird, der zu einem Störfall führen kann.

Nr.	Erläuterung	Explanation	Ergebnis	Result	Abweichung	Empfohlen / Freiwillig	Priority
8.3.2	Rollen, Rechte und Passwörter wurden definiert bzw. Standardpasswörter wurden geändert.	Roles, rights and passwords have been defined or default passwords have been changed.					#
8.3.2			1)Allgemeines Rollenkonzept ist noch nicht erstellt. 2)Standardpasswörter sind nicht verändert. Konzepterstellung zur Absicherung der Safety Komponenten. Sicherheit muss in Zusammenhang mit dem Zutrittsschutz / Zugangsschutz gesehen werden.	1) General role concept has not yet been created. 2) Default passwords are not changed. Concept creation to secure the safety components. Security must be seen in connection with access protection/ access protection.	ja	empfohlen	1

Abb. Nr. 5: Beispielhafter Auszug einer IT-Risikobeurteilung nach NA 163

Da die bisherigen Ansätze der klassischen Gefahrenanalyse für einen Einbezug der IT / OT Thematik oftmals nur bedingt geeignet sind, ist es ratsam diese separat in einer IT-Risikobeurteilung durchzuführen (beschränkt auf die Aspekte der Integrität und Verfügbarkeit).

Ein Hintergrund für diese Trennung ist insbesondere die unterschiedliche Betrachtungsweise der klassischen Gefahrenanalyse und der IT-Risikobeurteilung.

In der klassischen Gefahrenanalyse wird ein Fehler in einem sicherheitsrelevanten Anlageteil bzw. eines sicherheitsrelevanten Anlagenteils auf Grund einer Funktion unterstellt. Dagegen können Cyberangriffe z. B. zum Ausfall oder Manipulation der gesamten Steuerungs- und Sicherheitsfunktionen der Prozessleittechnik führen, das heißt, hier werden mehrere Fehler gleichzeitig hervorgerufen.

Resultierend aus den IT-Gefährdungen der IT-Risikobeurteilung müssen Maßnahmen abgeleitet und umgesetzt werden, die eine ausreichende Sicherheit im Rahmen der praktischen Vernunft im Sinne der Störfall-Verordnung darstellen. Diese Gestattung der fachlichen Schnittstelle zwischen OT und IT ermöglicht es, im Rahmen der klassischen Gefahrenanalyse weiterhin nur einen Fehler zu unterstellen.

Mit Blick auf die OT sind die aus der klassischen Gefahrenanalyse resultierenden Sicherheitsfunktionen Ausgangspunkt für die im Sicherheitsbericht darzustellenden Teile der IT-Risikobeurteilung, ergänzt um die damit in Zusammenhang stehenden Subsysteme / Schnittstellen (dies schließt auch Hybride oder vollintegrierte Bauteile mit ein). Temporäre oder alternative Schnittstellen sind zu betrachten.

Mindestanforderungen:

- Art und Umfang der IT-Risikobeurteilung sollen der Anlage Rechnung tragen, so können beispielswiese für kleinere Anlagen checklistenartige Verfahren wie das der NA 163 /3/ angewendet werden.
- Die für die IT-Risikobeurteilung verwendete Systematik bzw. zugrunde gelegten Regelwerke (Typische Vertreter sind z. B.: IEC 62443 /4/, DIN ISO 2700X /7/, NA 163 /3/ i. V. m VDI/VDE 2180 /2/ und VDI/VDE 2182 /8/) sind durch die Betreiberin zu beschreiben. Bei Verwendung einzelner auf dem Markt erhältlicher Produkte zur Erstellung einer IT-Risikobeurteilung ist deren Systematik und Aufbau zu beschreiben, sowie deren Vergleichbarkeit zu oben genannten Systematiken darzulegen. Die Erfüllung ggf. vorhandener Eingangsvoraussetzungen ist nachzuweisen (z.B. bei Verwendung der Checkliste nach NA 163 /3/).
- Die zugrunde gelegten Methoden und deren Ergebnisse der IT-Risikobeurteilung sind im Sicherheitsbericht darzulegen (in Analogie zur klassischen Gefahrenanalyse)
- Die im Sicherheitsbericht hinterlegten IT-Risikoanalysen, Netzwerkdiagramme und Assetlisten müssen in sich konsistent sein.

5. Literaturquellen

/1/ KAS-51 „Leitfaden Maßnahmen gegen Eingriffe Unbefugter“ (14. November 2019), kostenfrei als Download erhältlich (http://www.kas-bmu.de/ -> Publikationen)

Die Kommission für Anlagensicherheit (KAS) ist eine nach § 51a Bundes-Immissionsschutzgesetz beim Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit gebildete Kommission (vormals Störfallkommission (SFK)).

/2/ VDI/VDE 2180 „Funktionale Sicherheit in der Prozessindustrie“,

Blatt 1 Einführung, Begriffe, Konzeption, April 2019
Blatt 2 Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen, September 2019
Blatt 3 Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (PFD), September 2019
Blatt 4 Mechanische Komponenten in PLT-Sicherheitseinrichtungen, Januar 2021

/3/ NAMUR-Arbeitsblatt NA 163 IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen, Ausgabe: 2017-12-15

/4/ IEC 62443 Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme

ist mit 14 Teile geplant, mit Stand März 2021 sind neun davon veröffentlicht. Die vierzehn Teile können den folgenden vier Bereichen zugeordnet werden:

1. Bereich Allgemeine Grundlagen, Modelle und Konzepte
2. Bereich Politiken und Prozesse
3. Bereich Sicherheitsanforderungen - Industriellen Steuerungs- und Leittechniken
4. Bereich Sicherheitsanforderungen - Industrielle Komponenten

/5/ DIN EN 61511: Funktionale Sicherheit - PLT-Sicherheitseinrichtungen für die Prozessindustrie, Teil 1 bis 3, Stand 02.2019

/6/ Bundesamt für Sicherheit in der Informationstechnik (BSI)
(https://www.bsi.bund.de/DE/Home/home_node.html)

IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit

(wird jährlich im Februar aktualisiert. Stand März 2021: Edition 2021, kostenfrei als Download erhältlich (BSI - IT-Grundschutz-Kompendium (bund.de))

/7/ DIN ISO/IEC 27000 ff. Informationstechnik – IT-Sicherheitsverfahren –

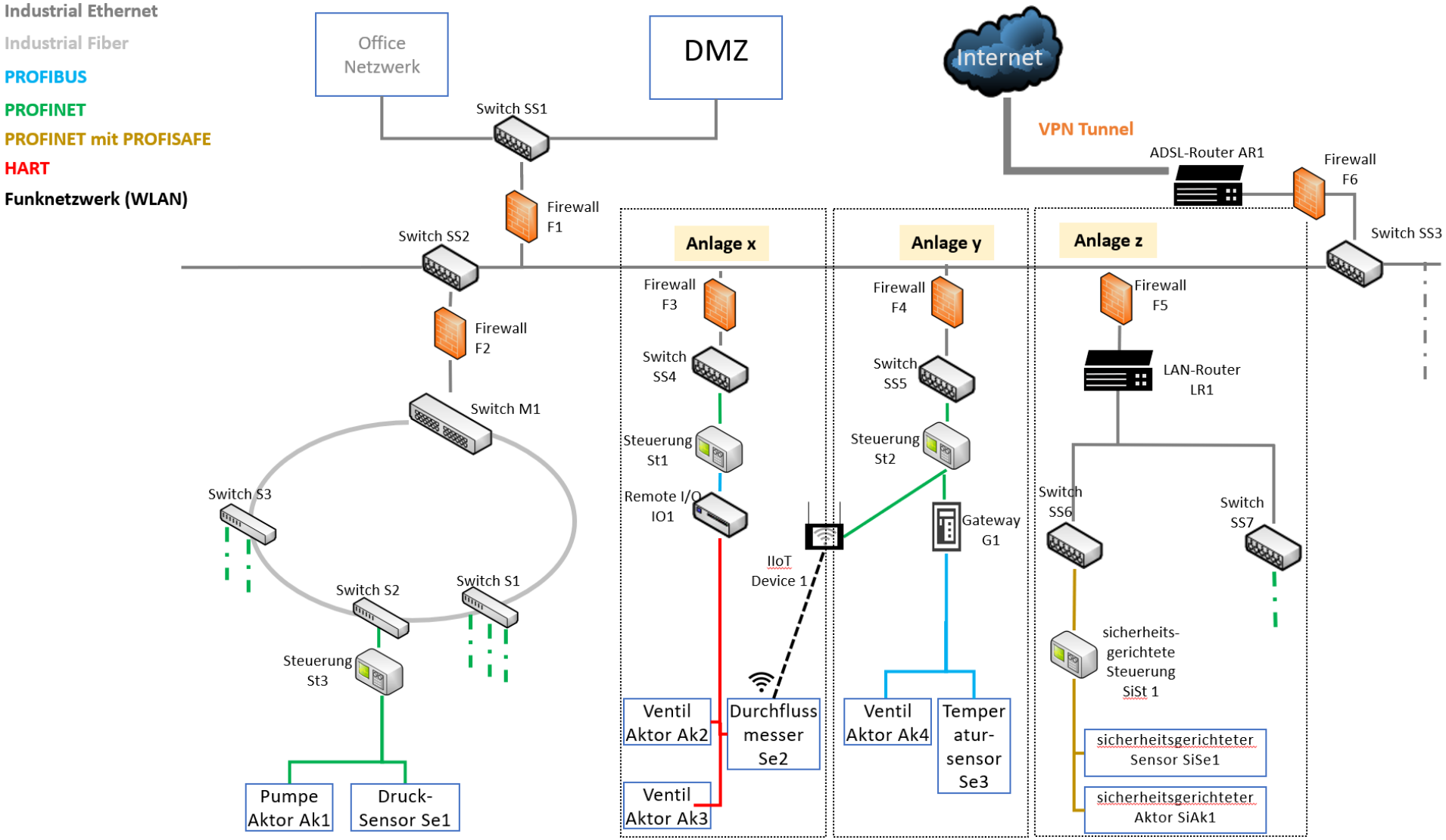
27000: Informationssicherheits-Managementsysteme - Überblick und Terminologie
27001: Informationssicherheits-Managementsysteme – Anforderungen
27002: Leitfaden für Informationssicherheits-Maßnahmen
27003: Informationssicherheits-Managementsysteme – Leitfaden
27005: Informationssicherheit- Risikomanagement
27006: Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten
27007: Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen

Sowie weitere 15 fachspezifische Subnormen.

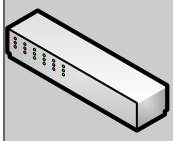
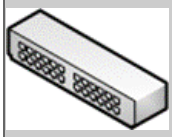
/8/ VDI 2182 „Informationssicherheit in der industriellen Automatisierung“:

Blatt 1 Allgemeines Vorgehensmodell
Blatt 2.1 Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller Speicherprogrammierbare Steuerung (SPS)
Blatt 3.1 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Hersteller Prozessleitsystem einer LDPE-Anlage
Blatt 3.2 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Integratoren LDPE-Reaktor
Blatt 3.3 Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber LDPE-Anlage
Blatt 4 Empfehlungen zur Umsetzung von Security-Eigenschaften für Komponenten, Systeme und Anlagen

Abbildung Nr. 3: Beispiel für die Darstellung eines Netzwerkdiagramms in einer hohen Detailstufe



Legende

Sym-bol	Bezeich-nung	Erläuterung
	**Switch**	Ein Switch ist ein Kopplungselement, das mehrere Rechner / Bauteile in einem Netzwerk miteinander verbindet. Die einzelnen Ein-/Ausgänge, eines Switches können unabhängig voneinander Daten empfangen und senden.
	**Sicherheitsgerichteter Switch / Industrial Switch**	Ein Switch der auf das industrielle Umfeld ausgerichtet ist. Im Vergleich zum normalen Switch sind diese Geräte deutlich robuster und resistenten gegenüber äußeren Umwelteinwirkungen. Oftmals sind bereits Security Applikationen integriert.
	**Managed Switch**	Ein Managed Switch, erlaubt es das Netzwerk zu überwachen, zu konfigurieren und auf einzelne Prozesse / Einstellungen gezielt einzuwirken z .B bestimmte Bauteile / Verbindungen zu priorisieren oder virtuelle Subnetze einzurichten und zu verwalten.
	**Firewall**	Eine Firewall dient dazu, den Zugriff auf / in einem Netzwerk zu regulieren bzw. beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln bzw. Parameter, ob bestimmte Netzwerkpakete durchgelassen oder verworfen werden.
	**Steuerung**	Steuerungen beeinflussen des Verhaltens von damit verbundenen Bauteilen /technischen Systemen in Abhängigkeit von den eingestellten Zielwerten.

	**ADSL-Router**	Router sind Netzwerkgeräte, die Netzwerkpakete zwischen mehreren Netzwerken weiterleiten können. Asymmetric Digital Subscriber Line (ADSL) bezeichnet eine gebräuchliche Anschlusstechnik von Breitbandanschlüssen. Umgangssprachlich sind damit oft Router für den Anschluss ans Internet gemeint
	**LAN-Router**	Local Area Network (LAN) Router dienen dazu lokale Netzwerke miteianderer zu verbinden. Das lokal ist dabei nicht mit räumlicher Nähe gleichzusetzen.
	**Remote I/O**	Remote-I/O-Systeme übertragen binäre und analoge Sensor- /Aktordaten, über eine Busschnittstelle an ein Leitsystem. Sie sind speziell für den Einsatz unter schwierigen umgebungsbedungen ausgelegt z.B. Ex-Atmosphäre.
	**IIoT Device**	Beim Industrial Internet of Things (IIoT) handelt es sich um die Adaption des IoT für das industrielle Umfeld. Ziel ist hierbei mittels Vernetzung und allumfänglicher Kommunikation aller Bauteile untereinander die betriebliche Effektivität zu erhöhen. IIoT wird oftmals als Vorbedingung für eine Industrie 4.0 gesehen.
	**Gateway**	Gateways sind Komponenten (Hard- und/oder Software), welche zwischen zwei Systemen eine Verbindung herstellten. Neben einer reinen Weiterleitung werden diese Daten zumeist verändert. Z.B. um sie zu anderen Netzwerken oder kompatibel zu machen.

Erläuterung zu Bussystemen / Verbindungstypen

HART- Protokoll (auch Hart-Verdrahtung genannt)

HART ist die Abkürzung für Highway Addressable Remote Transducer . Das HART-Protokoll basiert auf einer Überlagerung eines 4/20-mA Standardsignals mit einem digitalen Signal mittels Frequenzumtastung so das 2 simultane Kommunikationswege entstehen. Das 4/20-mA Signal überträgt den Messwert, während die digitale Komponente Systemparameter bzw. zusätzliche Informationen enthalten kann. Es handelt sich um ein klassisches Master-/Slave-Protokoll, was bedeutet das ein Slave (Feldgerät) nur dann Informationen liefert, wenn diese vom Master (Steuerung) angefordert werden. Pro Slave sind 2 Master möglich.

PROFIBUS

PROFIBUS gehört zu den digitalen Feldbussen (nicht auf Ethernet Basis). PROFIBUS wurde als digitale Alternative zum HART Protokoll entwickelt. Es ermöglicht eine bidirektionale Kommunikation zwischen mehreren Master und Slave Einheiten. Es ist zwischen PA Variante (Process automation) und DP (Dezentrale Perepherie) zu unterscheiden. Vereinfacht ausgedrückt ist DP das schnellere und PA das robustere System.
Auszug aus dem Wiki zum primären Einsatzzweck (Kombinationen sind möglich):

- DP -> Kommunikation von Sensoren und Aktoren durch eine zentrale Steuerung in der Fertigungstechnik.
- PA -> Kommunikation zwischen Mess- und Prozessgeräten, Aktoren und Prozessleitsystem bzw. SPS/DCS in der Prozess- und Verfahrenstechnik eingesetzt

Industrial Ethernet

Industrial Ethernet ist der „Core“ Standard auf dem die meisten modernen Industrienetzwerke basieren. Es handelt sich dabei um eine Weiterentwicklung des klassischen (LAN) Ethernets und ist grundsätzlich vergleichbar mit dem im Office Bereich üblichen Ethernetnetzwerken.

Industrial Fiber

Industrial Fiber ist bezogen auf Aufbau und Funktion grundsätzlich vergleichbar mit Industrial Ethernet, arbeitet im Gegensatz zu diesem aber ausschließlich mit Glasfaserverbindungen, was die Geschwindigkeit der Datenübertragung stark erhöht und somit große Strecken mit geringer Latenz überbrücken kann.

PROFINET

PROFINET steht für Process Field Network und basiert auf der Ethernet Technologie (aufbauend auf dem Industrial-Ethernet-Standard). PPOFINET nutzt TCP/IP- und IT-Standards, ist Echtzeitfähig und modular konfigurierbar. Es ermöglicht die nahtlose Integration von Feldbussen und Protokollen, ist aber im engeren Sinne kein Feldbus für sich selbst gesehen (wird aber im Sprachgebrauch so verwendet).

PROFINET mit PROFISAFE

PROFISAFE ist ein zusätzliches Protokoll was auf einem PROFINET System läuft. PROFISAFE definiert die Kommunikation mit sicherheitsgerichteten Geräten, so dass eine Zuverlässigkeit bis SIL 3 (im loop) gewährleistet werden kann, indem es eine zusätzliche virtuelle Datentransferschicht hinzufügt auf der dann zusätzliche Daten transportiert werden.

Funknetzwerk

In Funknetzwerken werden Informationen mittels elektromagnetischer Wellen übertragen werden (basierend auf der jeweiligen Funktechnik). Typische Vertreter sind z. B. Bluetooth, WLAN oder Wimax, welche alle über spezielle Vor- und Nachteile verfügen.

Allen gemein ist das Funknetzwerke zumeist räumlich nicht präzise eingestellt werden können und somit tendenziell auch für Personen außerhalb des Betriebsbereichs erreichbar sind. Darüber hinaus sind Funkverbindungen anfällig für Störungen (z. B. durch andere Anlagen, Maschinen oder Störsendern).