Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: IND.2.7 Safety Instrumented Systems

1. Einleitung

Diese Umsetzungshinweise geben Hilfestellung bei der Erfüllung der spezifischen Sicherheitsanforderungen für Safety Instrumented Systems (SIS).

Ein SIS ist eine Einrichtung, die die Risiken, die von Maschinen und Industrieprozessen ausgehen und eine Gefahr für Mensch und Umwelt darstellen, auf ein tolerierbares Maß reduziert. Informationssicherheit hat den Schutz von Informationen als Ziel. Die weitgehende Vernetzung und der Einsatz von Standard-IT-Komponenten sind nur einige Gründe, warum auch SIS nicht ohne Informationssicherheit auskommen kann.

Grundsätzlich beziehen sich der Baustein sowie die vorliegenden Umsetzungshinweise auf alle Arten von SIS. Die Anforderungen des Bausteins gelten dabei unabhängig von den im Umsetzungshinweis genannten Maßnahmen. Lässt sich eine Maßnahme mit dem vorliegenden Gerätetyp nicht direkt umsetzen, ist eine alternative Maßnahme zur Erfüllung der Anforderung zu ermitteln und umzusetzen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins IND.2.7 *Safety Instrumented Systems* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein IND.2.7 Safety Instrumented Systems

IND.2.7.M1 Erfassung und Dokumentation (B)

Um geeignete Maßnahmen ableiten, Vorfälle bearbeiten und ein geeignetes Notfallmanagement einführen zu können, muss das SIS genau bekannt und dokumentiert sein. Hierzu sollten die folgenden Aspekte erfasst werden.

Erfassung und Dokumentation der Hardware- und Software-Komponenten

Der aktuelle und vollständige Ist-Zustand aller Komponenten muss dokumentiert werden. Dies ist notwendig, um zum SIS gehörige Komponenten zu definieren und es gegen die Umgebung bzw. Peripherie abzugrenzen.

Typische Hardware-Komponenten, die in einem SIS vorkommen, sind

- Sensoren,
- Auswertegeräte,
- Aktoren,
- Logiksystem (SSPS),
- I/O-Karten,
- Kommunikationsmodule,
- Drucker,
- Router,
- Switches,
- Firewalls,
- Programmiergeräte (Engineering Stations) sowie
- Konfigurationsgeräte (Handhelds).

Typische Software-Komponenten, die in einem SIS vorkommen, sind

- PC-Betriebssysteme,
- Firmware (bei Auswertegeräten, Sensoren, Aktoren, Firewalls, Netzkomponenten, SSPS),
- Engineering-Software (für SSPS),
- Konfigurationssoftware (für Sensoren/Aktoren, Netzkomponenten) sowie
- Hilfssoftware (PDF-Erzeuger, Office-Programme, Virenscanner, Whitelisting-Programm).

In der Dokumentation muss der Zweck jeder Komponente definiert werden. Unnötige oder zweckfremde Komponenten können so identifiziert und entfernt werden, um die Exposition gegenüber Gefährdungen zu senken.

Typ, Versionsnummer und Firmware-Version für die Hardware sowie Versionsnummer für die Software sollten dokumentiert sein. Die Übersicht erleichtert es, die Schwachstellen-Meldungen vom Hersteller oder CERT schnell gegenüber den eingesetzten Komponenten abzugleichen.

Um sicherzustellen, dass die Dokumentation der Komponenten aktuell und vollständig bleibt und Änderungen am SIS mit in die Dokumentation einfließen, muss die Dokumentation einmal jährlich überprüft werden.

Programme zur Software-Inventarisierung können die automatisierte Erfassung und den Abgleich mit einer Liste erlaubter Anwendungen unterstützen. Diese Programme setzen in der Regel das Installieren von

Zusatzsoftware voraus, was in einem Produktionsnetz nicht immer möglich ist. Oft ist eine manuelle Erfassung notwendig.

Erfassung und Dokumentation der relevanten Informationen

Informationen über das SIS sowie die Anlage und das Verfahren, die das SIS schützen soll, sind für den Erfolg einer Manipulation bzw. eines Angriffes mit ausschlaggebend. Die für den Betrieb relevanten Informationen müssen identifiziert, klassifiziert und dokumentiert werden. Beispiele hierfür sind Konfigurationsdateien sowie Parameter, Handbücher, Projektierungsdaten, Konstruktionsdateien und -Zeichnungen, sicherheitsbezogene Anwendungsprogramme usw.

Die folgenden Stufen für die Klassifizierung (siehe [BSI 200-2], Kapitel 5.1 Klassifikation von Informationen) sind z. B. möglich:

- Offen
- Intern
- Vertraulich
- Streng vertraulich

Je nach Geheimhaltungsstufe der Informationen müssen spezifische Regelungen zur Absicherung des Zugriffs sowie zur Authentisierung und Autorisierung berechtigter Personen erstellt werden. Des Weiteren sind Maßnahmen zu treffen, die die Vertraulichkeit dieser Informationen sicherstellen.

Erfassung und Dokumentation von Verbindungen

Der aktuelle und vollständige Ist-Zustand aller Daten- und Signalverbindungen muss dokumentiert werden. Art und Umfang der Verbindungen müssen auf das für die Funktion des SIS absolut notwendige Minimum beschränkt werden. Die genaue Kenntnis der zum SIS gehörigen Verbindungen ist notwendig, um Schwachstellen und mögliche Bedrohungen zu identifizieren und zu beurteilen.

Die Kommunikationspartner, zwischen denen eine Verbindung hergestellt wird, müssen dokumentiert werden. Die Kommunikationspartner sollen eindeutig identifizierbar sein und dem Änderungsmanagement, im Rahmen des Functional Safety Management (FSM), unterliegen. Zusätzlich sollen sie über eine positive Sicherheitsbeurteilung verfügen, d. h. für das SIS darf die Verbindung kein Sicherheitsrisiko darstellen.

Der Zweck jeder Verbindung muss dokumentiert werden. Verbindungen müssen ausschließlich dem Zweck dienen, für den sie eingerichtet wurden. Darüber hinausgehende Kommunikation darf nicht erfolgen. Im Folgenden sind Beispiele für zulässige Kommunikation aufgeführt:

- Signalverbindungen von Basic Process Control System (BPCS) zum Logiksystem:
    - Reset-Signal
    - Prozessstatussignale
    - Systemstatussignale
- Datenverbindungen zu folgenden Zwecken:
    - Programmierung des SSPS
    - Debugging des Anwenderprogramms
    - Forcen (Simulieren) von Variablen im Anwenderprogramm
    - Herunterladen von Antivirus-Aktualisierungen
    - Herunterladen von Patches und Updates aus vertrauenswürdigen Quellen
    - Herunterladen anderer freigegebener Daten von einer AV-Scan-Station beziehungsweise Wechseldatenträger-Schleuse

Um das Risiko für das SIS, das von Signal- und Datenverbindungen ausgeht, zu beurteilen und zweckfremde Verbindungen zu identifizieren, müssen die technischen Merkmale jeder Verbindung dokumentiert werden.

Typischerweise umfasst eine Dokumentation die folgenden Details, wobei je nach Art der Verbindung nicht alle Merkmale vorhanden sein müssen:

- Zeitliche Dauer der Verbindung:
  - permanent (z. B. Signalverbindungen)
  - temporär, regelmäßig wiederkehrend (z. B. Aktualisierung der Antivirussignaturen)
  - temporär, anlassbezogen (z. B. Übertragen einer neuen Version des Anwendungsprogramms in das Programmiergerät)
- Richtung des Datenaustausches (unidirektional / bidirektional)
- Art der Kommunikation (Daten bzw. Signale)
- Protokoll:
  - IP-basiert (MODBUS/TCP, OPC, NTP etc.)
  - andere OT-Protokolle (MODBUS seriell, Profibus, (wireless) HART etc.)
  - analoge bzw. digitale I/Os
- Bei IP-Verbindungen:
  - Quell- und Ziel-MAC-Adresse
  - Quell- und Ziel-IP-Adresse
  - Quell- und Ziel-Port-Adresse
- Sicherheitsparameter (Sicherheitseinstellungen, digitale Zertifikate, kryptografische Schlüssel etc.)
- Aufbaurichtung der Verbindung (aus dem SIS in die Umgebung sowie aus der Umgebung zum SIS)
- Inhalt der Kommunikation:
  - zulässige Dateigröße sowie Datenmenge
  - zulässiger Wertebereich
- Art der Sicherung der Authentizität der Kommunikationspartner (siehe IND.2.7.M9 *Absicherung der Daten- und Signalverbindungen*)

Erfassung und Dokumentation von Organisationsstrukturen

Personen, Organisationseinheiten und Prozesse, die mit dem SIS in Verbindung stehen, müssen erfasst und dokumentiert werden. Art und Umfang der mit dem SIS in Verbindung stehenden Organisationseinheiten und Personen müssen auf das für die Funktion des SIS absolut notwendige Minimum beschränkt werden.

Typischerweise beteiligte Organisationseinheiten sind

- Betrieb, Betriebsleitung,
- Engineering,
- Wartung, Technik,
- IT-Betrieb,
- Arbeits-, Gesundheits- und Umweltschutz,
- CERT (Computer Emergency Response Team),
- Systemhersteller,
- Systemintegrator sowie
- Katastrophenschutz.

Zusätzlich müssen die vergebenen Benutzerkennungen und die zugewiesenen Rollen und Rechte dokumentiert und regelmäßig mit dem Ist-Zustand abgeglichen werden.

Die Verantwortlichkeiten und die konkreten Zuständigkeiten der Personen und Organisationen für folgende Prozesse müssen klar definiert und im Functional Safety Managementsystem beschrieben sein:

- Planung, Errichtung, Validierung des SIS,
- Bereitstellung der IT-Infrastruktur,
- Wiederkehrende Prüfung des SIS inklusive IT-Risikobeurteilung,
- Durchführung von technischen Änderungen (Planung, Validierung, Prüfung),
- Behebung von Fehlern / Sicherheitsschwachstellen in Komponenten des SIS,
- Erkennung von Sicherheitsereignissen sowie
- Steuerung der Behebung von Sicherheitsereignissen (Incident Response).

IND.2.7.M2 Zweckgebundene Nutzung der Hard- und Softwarekomponenten (B)

Nicht benötigte Verbindungen sowie Komponenten erhöhen die Exposition gegenüber Gefährdungen. Eine Beschränkung dieser auf das für die Sicherheitsfunktion (SIF) absolut notwendige Minimum stellt eine sehr wirksame Maßnahme dar.

IND.2.7.M3 Änderung des Anwendungsprogramms auf dem Logiksystem(B)

Die Änderung des Anwendungsprogramms auf dem Logiksystem (SSPS) stellt einen schwerwiegenden und riskanten Eingriff in das SIS dar. Eine ungewollte Übertragung eines neuen Anwenderprogramms muss verhindert werden.

Sind die Geräte mit einem Hardware- oder Softwareschutzmechanismus (beispielsweise Schlüsselschalter) ausgestattet, so ist dieser zu aktivieren, um einen unerlaubten Datentransfer zu erschweren. Sofern möglich sollte auch die Umgebung der Komponenten physisch geschützt werden, indem sie in einem abgeschlossenen Raum (alternativ Schaltraum oder Serverschrank) untergebracht werden, zu dem nur autorisierten Personen Zugang haben. Eine permanente Anbindung an das Programmiergerät sollte unterbunden sein. Je nach Schutzbedarf können weitere organisatorische Maßnahmen getroffen werden, z.B. Vier-Augen-Prinzip für jede Änderung.

IND.2.7.M4 Verankerung von Informationssicherheit im Functional Safety Management (S)

Das Functional Safety Management (FSM) ist das organisatorische Rahmenwerk für SIS und basiert je nach Ausprägung des SIS auf Regelwerken wie z. B. IEC 61508, IEC 61511, ISO 13849 oder IEC 62061. Es ist strukturell mit dem Informationssicherheitsmanagement gemäß der ISO/IEC 27000-Normenreihe vergleichbar.

Der Informationssicherheits-Managementprozess nach [BSI 200-2] sollte als fester Bestandteil in das Functional Safety Management integriert werden.

IND.2.7.M5 Notfallmanagement von SIS (S)

Aufgrund unterschiedlicher Anforderungen verfügen viele Institutionen bereits über ein Notfallmanagement, das bestimmte Szenarien abdeckt und Rollen sowie Prozesse festlegt. Mindestens folgende Szenarien müssen dort abgebildet werden:

1. Vorgehen bei kompromittiertem Kommunikationspartner des SIS (z. B. Verbindungsabbruch, Schadsoftware auf der Engineering Station)
2. Vorgehen bei kompromittiertem Sensor, Aktor oder Logiksystem

Die weiteren Schritte z. B. zur Eingrenzung des Vorfalls, Bereinigung der Ursachen und Wiederherstellung des validen Systemzustands müssen in einem Notfallplan geregelt werden. Der Plan sollte Handlungsabläufe und Zuständigkeiten für bestimmte Szenarios bereit halten.

Die Szenarien bzw. die festgelegten Prozesse sollten regelmäßig geübt werden.

IND.2.7.M6 Sichere Planung und Spezifikation des SIS (S)

Um die Risiken durch versehentliche oder absichtliche Handlungen zu reduzieren, sollten die Spezifikation und die Implementierung nur nach den dem Vier-Augen-Prinzip geändert werden.

IND.2.7.M7 Trennung und Unabhängigkeit des SIS von der Umgebung (S)

Ein OT-Netz sollte aus mehreren Netzsegmenten mit individuellen Schutzbedarfen bestehen. Der Datenverkehr zwischen den verschiedenen Segmenten und Ebenen (sowohl horizontale als auch vertikale Integration) sollte

- streng kontrolliert und überwacht werden (z. B. durch Security Monitoring) sowie
- auf das betrieblich unbedingt notwendige Maß reduziert werden (z. B. durch Firewalls).

Dies gilt auch für die Trennung des SIS von der Umgebung. Folgendes ist hierbei zwingend zu beachten:

- Die Integrität des SIS sollte weder durch den Abbruch von Verbindungen zu der Umgebung noch durch fehlenden Datenaustausch mit der Umgebung beeinflusst werden.
- Die Integrität der Sicherheitsfunktionen des SIS sollte nicht durch versehentliche oder vorsätzliche Übermittlung von falschen oder überflüssigen Daten oder Signalen aus der Umgebung beeinflusst werden.
- Für den Fall, dass die Integrität und Verfügbarkeit einer Daten- oder Signalverbindung von außerhalb zum SIS oder vom SIS aus nach außen nicht gewährleistet werden kann, sollte eine alternative Übermittlung von kritischen Daten (Ersatzwertstrategie) implementiert werden.
- Rückwirkungen, die von Änderungen oder Störungen in verbundenen Systemen verursacht werden, dürfen die Integrität des SIS nicht beeinträchtigen.

Die Zonen-Einteilung der PLT-Sicherheitseinrichtung gemäß NAMUR NA 163 zeigt eine exemplarische Aufteilung in drei Netzsegmente (Zonen) (siehe unten 3.1 *Wissenswertes*, Abbildung 2). Eine andere Netzarchitektur ist zulässig, wenn folgende Kriterien beachtet werden:

- Der Verbindungsaufbau sollte immer aus dem Netzsegment mit dem höheren Schutzbedarf (SIS in Zone A) in das Netzsegment mit dem niedrigeren Schutzbedarf (Zone B) initiiert werden.
- Eine direkte Verbindung von Zone A in die Umgebung ist nicht zulässig.
- Die Übergänge zwischen den Segmenten werden kontrolliert, überwacht und protokolliert.
- Die Netztrennung darf nicht umgangen werden.
- Weiterführende Informationen zur Absicherungen von Kommunikationsverbindungen sind in IND.2.7.M9 *Absicherung der Daten- und Signalverbindungen* enthalten.

IND.2.7.M8 Sichere Übertragung von Engineering-Daten auf SIS (S)

Sollten Daten aus dem Internet, z. B. direkt vom Hersteller, heruntergeladen werden, so ist auf die Authentizität und die Integrität zu achten. Für eine verschlüsselte Verbindung und die Überprüfung der Authentizität sorgen SSL/TLS-Zertifikate, die von einer Certificate Authority herausgegeben und signiert werden. Die Integrität der zu übertragenden Daten kann dann mithilfe eines Hashwertes geprüft werden. Voraussetzung ist die Kenntnis über den Hashwert des Originals.

Die Programmiergeräte sollten nicht permanent mit dem SIS über das Netz verbunden werden. Eine temporäre Verbindung sollte nur dann aufgebaut werden, wenn eine Änderung nötig ist (siehe auch IND.2.7.M9 *Absicherung der Daten- und Signalverbindungen*).

Wird das Anwendungsprogramm für das Logiksystem auf einen Wechseldatenträger (beispielsweise auf eine Speicherkarte) geschrieben, so sollten zuvor Maßnahmen für einen sicheren und restriktiven Umgang mit mobilen Speichergeräten ergriffen worden sein. Dazu gehören z. B. folgende Maßnahmen:

- Eine Richtlinie zum Umgang mit Wechseldatenträgern ist erstellt und dem Personal bekannt.
- Die Nutzung fremder Geräte ist untersagt und wird durch technische Maßnahmen, z. B. USB Device Manager, verhindert.
- Die private Nutzung dienstlicher Geräte ist untersagt.
- Das Booten von Wechseldatenträgern ist deaktiviert.
- Die Auto-Play-Funktion ist abgeschaltet, sofern das Betriebssystem diese Funktion unterstützt.
- Wechseldatenträger werden beim Anschluss an ein System automatisch auf Schadprogramme überprüft.
- Es existiert eine Wechseldatenträgerschleuse, um fremde Geräte zu überprüfen bzw. um die Inhalte auf firmeneigene Wechseldatenträger zu übertragen, und das Personal ist mit der Handhabung vertraut.

IND.2.7.M9 Absicherung der Daten- und Signalverbindungen (S)

Daten- und Signalverbindungen im betrachteten System, vor allem aber solche aus der Umgebung, bergen ein Gefährdungspotential. Die Verbindungen sollten daher abgesichert werden (siehe 3.1. *Wissenswertes*, Abbildung 2: *Zonen-Einteilung PLT-Sicherheitseinrichtung gemäß NAMUR NA 163*).

Starke physische Sicherung

Alle Daten- und Signalverbindungen eines SIS sollten physisch stark gesichert werden. Als physisch stark gesicherte Verbindungen gelten:

- dedizierte Safety-Netze, die inklusive sämtlicher Netzkomponenten vollständig unter Kontrolle des Betreibers sind,
- Point-to-Point-Verbindungen sowie
- Netze, die bereits über Sicherheitsmaßnahmen verfügen und bei denen sowohl das Kommunikationsmedium als auch die Verbindungen auf Manipulation überwacht werden.

Kommunikation zwischen ... und ...	Analoge oder digitale I/Os, ohne HART		Protokollbasierte Punkt-zu-Punkt-Verbindung (IP, HART, Modbus, Profibus, ...)		Netzwerk bzw. Bus (>2 Teilnehmer)	
	Phys. stark gesichert	Phys. nicht gesichert	Phys. stark gesichert	Phys. nicht gesichert	Phys. stark gesichert	Phys. nicht gesichert
(A oder B) < – > (A oder B)	1 2 3 4 5 6 O	1 2 3 4 5 6 X	1 2 3 4 5 6 O O N O	1 2 3 4 5 6 X O O O	1 2 3 4 5 6 O O N O	1 2 3 4 5 6 X X X O
(A oder B) < – > Umgebung	1 2 3 4 5 6 O X - - - -	1 2 3 4 5 6 O X - - - -	1 2 3 4 5 6 X X O O O O	1 2 3 4 5 6 X X X X O O	1 2 3 4 5 6 X X O O X O	1 2 3 4 5 6 X X X X X X

Abbildung 1: Absicherung von Kommunikationsverbindungen ([NA 163])

X: empfohlen | O: optional | N: nicht erforderlich | – : nicht anwendbar

Weitere Sicherung für *unidirektionale* Daten- und Signalflüsse

Die Unidirektionalität des Datenflusses vom SIS nach außen (d. h. Rückwirkung nicht möglich) sollte sichergestellt werden. Dies ist z. B. durch den Einsatz von Datendioden umsetzbar.

Weitere Sicherung für *bidirektionalen* Daten- und Signalaustausch

Zur Sicherung von *bidirektionalem* Daten- und Signalaustausch sollten entsprechend der Komplexität der Verbindung und der vorhandenen physischen Absicherung die folgenden Maßnahmen 1 bis 6 umgesetzt werden:

- **Maßnahme 1**: Für alle Zonen, die mit der SIS-Zone kommunizieren sollen, müssen deren Betreiber im Vorfeld die Informationssicherheit in Form einer Sicherheits- bzw. Risikobeurteilung nachweisen.
- **Maßnahme 2**: Übertragene Daten und Signale sollen auf Plausibilität (wie durch IEC 61511 gefordert) geprüft werden. Verletzungen der Plausibilität sollten gemeldet bzw. alarmiert werden.
- **Maßnahme 3**: Jeder Kommunikationspartner, der von außen mit der SIS-Zone kommunizieren möchte, muss sich vor dem Datenaustausch erfolgreich authentifizieren. Die übertragenen Daten bzw. Werte sollten verschlüsselt werden. Mit dieser Maßnahme soll sichergestellt werden, dass nur autorisierte Komponenten mit dem SIS kommunizieren.
- **Maßnahme 4**: Die Verbindung muss von innen nach außen (d. h. von Zone A über B, siehe 3.1 *Wissenswertes*, Abbildung 2) in die Umgebung aufgebaut werden. Damit soll sichergestellt werden, dass Versuche, sich von außen auf das SIS zu verbinden, abgewiesen werden.
- **Maßnahme 5**: Die Verbindung muss z. B. durch eine Firewall so gesteuert werden, dass lediglich der Datenverkehr von explizit zugelassenen Ports, IP- und/oder MAC-Adressen möglich ist.
- **Maßnahme 6**: Die Nutzdaten und Signale, die über die Verbindung ausgetauscht werden, müssen inspiziert und auf Anomalien überwacht werden (Deep Packet Inspection, Intrusion Detection).

Für die **Maßnahmen 3 und 4** sind folgende Realisierungsvarianten denkbar:

- Es könnte eine zertifikatsbasierte Authentisierung und Verschlüsselung genutzt werden, wenn die Kommunikationspartner dies nativ unterstützen.
- Es könnten Software-VPNs eingesetzt werden, mit deren Hilfe verschlüsselte Tunnel zwischen den Kommunikationspartnern vom SIS in die Umgebung aufgebaut werden. Dies ist aber nur möglich, sofern die Kommunikationspartner dies unterstützen.
- Falls die Kommunikationspartner Zertifikate oder VPN nicht direkt unterstützen, könnten (transparente) VPN-Gateways eingesetzt werden. VPN-Gateways sind dedizierte Hardware-Komponenten, die verschlüsselte VPN-Tunnel herstellen und sich gegenseitig authentisieren.

IND.2.7.M10 Anzeige und Alarmierung von simulierten oder gebrückten Variablen (S)

Werden Variablen auf einem Bedienpanel oder im Basic Process Control System angezeigt, sollte aus der Anzeige eindeutig hervorgehen, ob es sich bei der Variable um den tatsächlichen oder um einen simulierten Wert handelt.

Die Simulation und Brückung von Variablen sollte in Alarmlisten und Logdateien protokolliert werden.

IND.2.7.M11 Umgang mit integrierten Systemen (S)

Für den Umgang mit integrierten Systemen sind folgende Lösungsansätze denkbar:

- **Lösung 1**: Die Komponente sollte als Ganzes in das Managementsystem der Funktionalen Sicherheit eingebettet werden, d. h. sie wird validiert und unterliegt, auch für den "betrieblichen" Teil, dem Änderungsmanagement.
- **Lösung 2**: Der Nachweis sollte erbracht werden, dass innerhalb der gemeinsam genutzten Komponente eine, unter IT-Sicherheitsaspekten hinreichende Trennung und Unabhängigkeit zwischen dem "sicheren" Teil und dem "betrieblichen" Teil vorliegt. Voraussetzung ist hier, dass der Nachweis der Konformität zu IEC 61508 oder IEC 61511 vorliegt.
- **Lösung 3**: Es sollte schriftlich dokumentiert werden, dass sich durch die gemeinsame Nutzung keine nicht tolerierbaren Informationssicherheitsrisiken für das SIS ergeben.

Im Falle von Lösung 2 oder 3 sind die Anforderungen des Bausteins IND 2.7 *Safety Instrumented Systems* und die vorliegenden Umsetzungshinweise lediglich für den Teil der Komponente zu implementieren, der für die Funktionale Sicherheit verwendet wird.

IND.2.7.M12 Sicherstellen der Integrität und Authentizität von Anwendungsprogrammen und Konfigurationsdaten (H)

Sofern Komponenten wie das Logiksystem (SSPS) sowie Feldgeräte (Sensoren, Aktoren) Sicherheitsmaßnahmen unterstützen, die die Authentizität und die Integrität der Daten (Firmware, Anwendungsprogramm, Konfiguration) gewährleisten, so sind diese zu aktivieren und sicher zu konfigurieren. Hierzu zählen beispielsweise das Booten von signierter Firmware, Umgang mit signierten oder verschlüsselten Daten usw.

Für Geräte, die aufgrund ihres Alters oder Designs diese Sicherheitsfunktionalitäten nicht zur Verfügung stellen, müssen seitens des Betreibers andere Maßnahmen ergriffen werden, um die Authentizität und die Integrität dieser Daten sicherzustellen.

Firmware sowie Firmware-Updates müssen durch den Hersteller signiert werden. Hierfür sind nur kryptografische Verfahren zu nutzen, die öffentlich und nach dem Stand der Technik als sicher eingestuft sind. Die technische Richtlinie des BSI zu TLS [BSI 02102-2] ermöglicht eine langfristige Orientierung bei der Wahl jeweils geeigneter kryptografischer Verfahren.

Werden Daten heruntergeladen, so ist die Authentizität der Quelle sicherzustellen und die Integrität der Daten zu prüfen (siehe IND.2.7.M8 *Sichere Übertragung von Engineering-Daten auf SIS*).

Für das Einbringen von Daten durch Dritte, z. B. Wartungspersonal, müssen sowohl organisatorische als auch technische Maßnahmen ergriffen werden, wie beispielsweise:

- Vier-Augen-Prinzip,
- Freigabe durch den Betreiber,
- Datenträgerschleuse sowie
- Verbot fremde Systeme einzubringen und zu nutzen (wirksame Verhinderung durch technische Maßnahmen).

Die Systeme, mit denen das SIS programmiert und parametriert wird, dürfen ausschließlich für diesen Zweck verwendet und nicht ans Netz angeschlossen werden. Diese sind verschlossen aufzubewahren. Des Weiteren müssen diese Systeme trotz erhöhten Aufwands sicher administriert und betrieben werden (z. B. Härtung, aktueller Stand von Betriebssystem und Software, Whitelisting, Antiviren-Schutz usw.)

Zwischen der SIS-Zone B und der Umgebung außerhalb des SIS sollte eine Demilitarisierte Zone (DMZ) hinzugefügt werden (siehe Abbildung 2: *Zonen-Einteilung PLT-Sicherheitseinrichtung gemäß NAMUR NA 163*). Die DMZ stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie die SIS-Zonen A und B. Sie wird aus zwei physisch getrennten Firewalls sowie einem Application Level Gateway aufgebaut. Proxy-Dienste mit Filterfähigkeiten bis hin zum Layer 7 sollten den Datenverkehr steuern und kontrollieren.

Die Protokolldaten müssen regelmäßig ausgewertet und Ereignisse untersucht werden.

Es sollten Systeme zur Erkennung von sicherheitsrelevanten Ereignissen (z. B. Anomalieerkennung, IDS) eingesetzt werden.

3. Weiterführende Informationen

3.1. Wissenswertes

Das Arbeitsblatt NA 163 *IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen* des internationalen Verbands NAMUR [NA 163] unterteilt das betrachtete System in drei Bereiche, die beim Erstellen des Bausteins und den vorliegenden Umsetzungshinweisen als Referenz dienten.

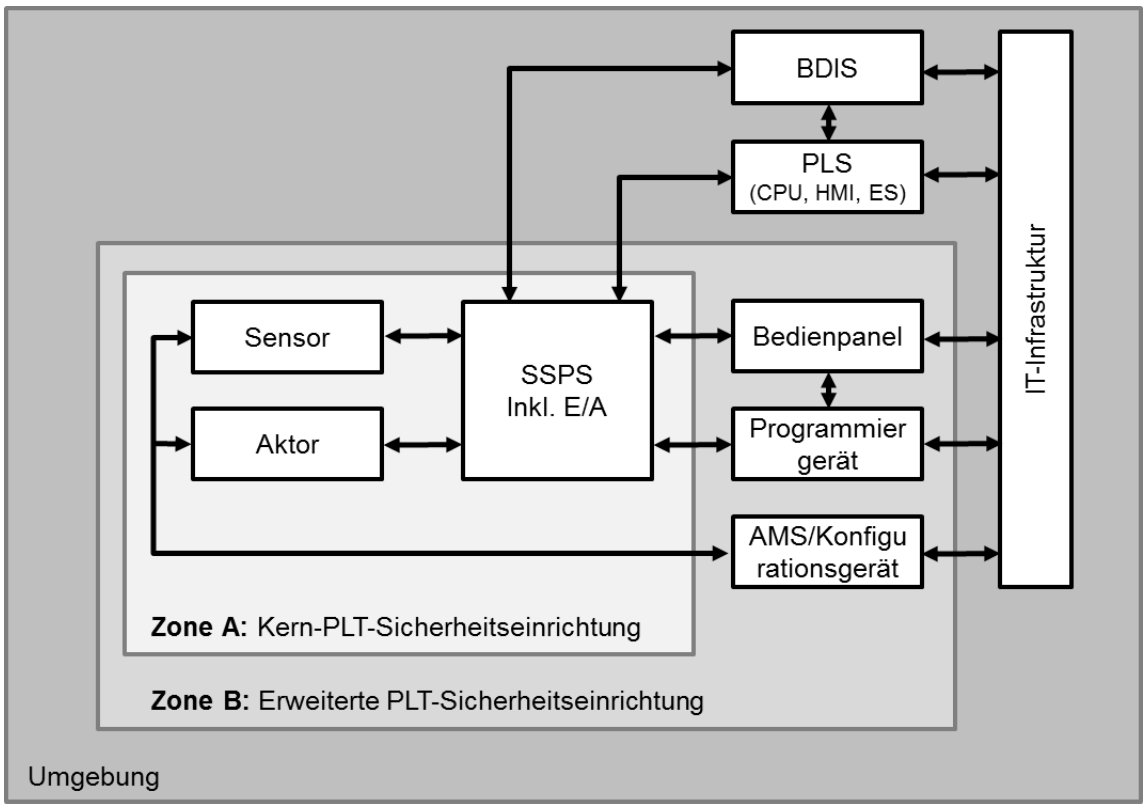

Abbildung 2: Zonen-Einteilung PLT-Sicherheitseinrichtung gemäß NAMUR NA 163

Bereich 1: Die **Kern-PLT-Sicherheitseinrichtung (Zone A)** umfasst die Sicherheitseinrichtung gemäß Definition in IEC 61508-1 mit dem Logiksystem, den Ein- und Ausgabebaugruppen inkl. Remote-I/O sowie den Aktoren und Sensoren. Verbindungen und unter Umständen vorhandene Netzkomponenten (Kabel, Switches, etc.), die der Verbindung zwischen Geräten innerhalb der Zone A dienen, werden gleichfalls dieser Zone zugeordnet.
Im Zweifel gilt: Wenn die Hard- bzw. Softwarekomponente notwendig ist, um die Sicherheitsfunktion (Safety Instrumented Function, SIF) auszuführen, zählt diese zu Zone A.

Bereich 2: Komponenten, die für die Ausführung der Sicherheitsfunktion nicht notwendig sind, jedoch das Verhalten der Kern-Sicherheitseinrichtung beeinflussen können, werden der **erweiterten Sicherheitseinrichtung (Zone B)** zugeordnet. Typische Beispiele sind: Bedien-Eingabe-Panels (HMIs), Visualisierungsstationen, das Programmiergerät (Engineering Station) für die Sicherheitseinrichtung und das Asset Management System (AMS) sowie Vorrichtungen zur Sensor- und Aktor-Konfiguration.

Bereich 3: In der **Umgebung** befinden sich Komponenten und Systeme, die weder direkt noch indirekt der Sicherheitseinrichtung zuzuordnen sind, aber in Verbindung mit der Sicherheitsfunktion stehen können (z. B. Reset-Anforderungen oder Visualisierung Sicherheitsfunktion-Zustand, etc.).

Weiterführende Informationen

Mit dem *ICS-Security-Kompendium* gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Hilfestellungen für den Test der Komponenten und bietet Maßnahmen für die IT-Sicherheit in ICS für Hersteller und Integratoren von ICS.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27019 *Information technology – Security techniques - Information security controls for the energy utility industry* Vorgaben für die Absicherung von Energieversorgern.

Der Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) und Österreichs E-Wirtschaft bietet mit dem Dokument *Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme* eine Hilfestellung zum sicheren Betrieb von Steuerungs- und Telekommunikationssystemen.

Folgende **internationale Normen** stellen weitere Hilfsmittel zur Einrichtung von IT-Sicherheit in Safety Instrumented Systems (SIS) zur Verfügung:

- IEC 61508-1:2010 *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Part 1: *General requirements*: International Electrotechnical Commission (IEC)
- IEC 61511-1:2016 *Functional safety - Safety instrumented systems for the process industry sector:* International Electrotechnical Commission (IEC)
- IEC 62443-2-1:2010 *Industrial communication networks - Network and system security*, Part 2-1: *Establishing an industrial automation and control system security program*: International Electrotechnical Commission (IEC)
- IEC 62443-2-4:2015 *Security for industrial automation and control systems*, Part 2-4: *Security program requirements for IACS service providers*: International Electrotechnical Commission (IEC)
- IEC 62443-4-1: ENTWURF *Security for industrial automation and control systems - Technical security requirements for IACS components*: Part 4-1: *Secure product development life-cycle requirements*: International Electrotechnical Commission (IEC)
- IEC 62443-4-2:ENTWURF *Technical security requirements for IACS components*: Part 4-2: *Technical security requirements for IACS components*: International Electrotechnical Commission (IEC)

Der Internationale Verband der Anwender von Automatisierungstechnik der Prozessindustrie NAMUR hat zur Risikobeurteilung das Dokument *IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen* veröffentlicht.

Im *Guide to Industrial Control Systems (ICS) Security*: NIST Special Publication 800-81 wird beschrieben, wie IT-Sicherheit im ICS-Umfeld eingeführt werden kann.

Zur Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) wurde die Richtlinie VDI/VDE 2180 veröffentlicht.

Die Richtlinie VDI/VDE 2182 bietet ein Vorgehensmodell und Anwendungsbeispiele für Informationssicherheit im ICS-Umfeld mit folgenden Blättern:

- Blatt 2.3 *Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber – Presswerk*
- Blatt 3.3 *Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber – LDPE-Anlage*

3.2. Quellenverweise

[BSI 200-2] BSI-Standard 200-2 *IT-Grundschutz-Methodik*: Bundesamt für Sicherheit in der Informationstechnik, Oktober 2017

[BSI 02102-2] BSI TR-02102-2 *Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)*, Version: 2020-1

[NA 163] NA 163 *IT-Risikobeaurteilung von PLT-Sicherheitseinrichtungen*, NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e. V.), Dezember 2017