Bundesamt
für Sicherheit in der
Informationstechnik

IND.2.7 Safety Instrumented Systems

1. Beschreibung

1.1. Einleitung

Safety Instrumented Systems (SIS) bilden eine Untergruppe der Industrial Control Systems (ICS). SIS werden eingesetzt, um Gefahren für technische Anlagen, die Umwelt und Personen abzuwehren. Der prinzipielle Aufbau von SIS unterscheidet sich kaum von den konventionellen Automatisierungssystemen. Der wesentliche Unterschied liegt in den erhöhten Anforderungen an die Zuverlässigkeit, mit der die von einem SIS auszuführenden Sicherheitsfunktionen (SIF) vollzogen werden. Das Maß an Zuverlässigkeit wird mit Hilfe des vierstufigen Sicherheits-Integritätslevels (SIL) ausgedrückt, diese werden in der IEC 61508 definiert. SIL1 ist hierbei die geringste und SIL4 die höchste Anforderung an die Zuverlässigkeit. Abhängig von der SIL-Stufe gelten unterschiedliche Anforderungen an die zulässige Ausfallrate von Komponenten, die Hardware-Fehlertoleranz der Architektur, die Unabhängigkeit von Prüfenden sowie weitere sicherheitsrelevante Punkte. Der gesamte Lebenszyklus eines SIS ist organisatorisch in ein Functional Safety Management (FSM) eingebettet.

Dieser Baustein ist unabhängig von der jeweiligen SIL-Stufe eines SIS umzusetzen. Die Informationssicherheit ist in jeder Lebensphase zu berücksichtigen, von der Entwicklung der Komponenten bis hin zu deren Anwendung, Betrieb und Außerbetriebnahme. Dabei ist zu beachten, dass die Sicherstellung der Integrität der SIS die höchste Priorität hat.

Ein weiteres wesentliches Merkmal von SIS ist die Unabhängigkeit und die Trennung von umgebenden IT-Systemen und von der Betriebstechnik (Operational Technology, OT). Das bedeutet, dass die Verfügbarkeit und Integrität des SIS nicht von ihnen beeinflusst werden dürfen.

1.2. Zielsetzung

Das Ziel dieses Bausteins besteht darin, geeignete Anforderungen an SIS zu formulieren, die beim Aufbau eines Managementsystems für Informationssicherheit (ISMS) erfüllt werden müssen.

Der Begriff „SIS“ umfasst im Sinne dieses Bausteins die Komponenten Sensor, Aktor, die sicherheitsgerichtete speicherprogrammierbare Steuerung (SSPS), auch als Logiksystem bezeichnet, das Anwendungsprogramm sowie auch insbesondere die dazugehörigen Programmiergeräte (Engineering Station, Handhelds für die Sensor-/Aktor-Konfiguration) und Visualisierungseinrichtungen.

1.3. Abgrenzung und Modellierung

Der Baustein IND.2.7 *Safety Instrumented Systems* ist auf jede SIS-Komponente einmal anzuwenden.

Der vorliegende Baustein ergänzt die übergeordneten Bausteine IND.1 *Prozessleit- und Automatisierungstechnik* und IND.2.1 *Allgemeine ICS-Komponente* und setzt voraus, dass diese umgesetzt wurden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein IND.2.7 *Safety Instrumented Systems* von besonderer Bedeutung.

2.1. Manipulation des Logiksystems

Die Manipulation des Anwendungsprogramms auf dem Logiksystem, bei der die Integrität eines SIS verletzt werden kann, stellt das größte Risiko dar. Anders als bei „einfachen" OT-Komponenten, kann dies potenziell schwerste Auswirkungen auf die Sicherheit von Menschen, Umwelt und technischen Anlagen haben. Im Arbeitsblatt NA 163 des internationalen Verbands der Anwender von Automatisierungstechnik der Prozessindustrie NAMUR sind diesbezüglich folgende drei Kategorien zur Risikobeurteilung definiert:

- Unter Kategorie 1 werden Manipulationen zusammengefasst, welche die Sicherheitsfunktion (SIF) auslösen, ohne dass der Anforderungsfall eingetreten ist. Die Auswirkungen sind im Sinne der funktionalen Sicherheit nicht gefährlich, da das SIS den sicheren Zustand herbeigerufen hat. Die Manipulationen führen allerdings zu einer Betriebsunterbrechung. Ursache dafür können beispielsweise Schadsoftware oder menschliche Fehlhandlungen sein.
- Kategorie 2 beschreibt einen Fall, bei dem die Sicherheitsfunktion deaktiviert ist und dadurch kein Schutz mehr geboten ist. Ein inakzeptables Ergebnis wird erst erreicht, wenn der Anforderungsfall eingetreten ist. Die Auswirkungen werden als gefährlich eingestuft, da das SIS seine primäre Aufgabe nicht erfüllen kann. Angriffsszenarien werden als komplex eingestuft, da die Manipulation des Logiksystems allein nicht ausreicht, um einen Schaden zu verursachen.
- Die dritte Kategorie behandelt das gravierendste Szenario, indem eine oder mehrere Sicherheitsfunktionen deaktiviert werden und der Anforderungsfall vorsätzlich herbeigeführt wird. Auch hier werden die Auswirkungen als gefährlich und die Angriffsszenarien als sehr komplex eingestuft. Denn um den Anforderungsfall herbeiführen zu können, müssen Angreifende neben Kenntnissen über die Manipulation des SIS auch über fundierte Kenntnisse zu den physikalischen Prozessen verfügen.

Im Dezember 2017 wurde erstmals über eine Schadsoftware berichtet, die gezielt SIS manipuliert hat. Der Weg des Angriffs führte über die Engineering Station, auf der sich die spezielle Software für die Programmierung und Parametrierung befand. Die dort installierte Malware suchte von dort aus gezielt nach verbundenen Logiksystemen eines bestimmten herstellenden Unternehmens und lud darauf ausführbaren Code, der das Anwendungsprogramm (die Logik) manipulierte. Aufgrund eines Fehlers in diesem Code schlug die Gültigkeitsüberprüfung fehl. Daraufhin löste die Sicherheitsfunktion aus und fuhr die angegriffene Anlage in einen sicheren Zustand herunter. Der Angriff war zwar nicht erfolgreich, hätte aber sowohl aufgrund seiner Auswirkung als auch seiner Komplexität der Kategorie 2 oder 3 zugeordnet werden können.

2.2. Unzureichende Überwachungs- und Detektionsverfahren

Eine wesentliche Funktion von Automatisierungssystemen liegt darin, Betriebszustände des zu automatisierenden Prozesses zu überwachen. So werden für gewöhnlich den Prozess betreffende Warnungen (z. B. bei überschrittenen Füllständen) und technische Parameter (z. B. Temperatur, Ventilstellung) berücksichtigt. Im Gegensatz dazu wird die unterstützende IT-Infrastruktur oft nicht überwacht.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse nicht oder nur unzureichend überwacht, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.7 *Safety Instrumented Systems* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeit	Rolle
Grundsätzlich zuständig	OT-Leitung
Weitere Zuständigkeiten	Planende, ICS-Informationssicherheitsbeauftragte, Wartungspersonal

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

IND.2.7.A1 Erfassung und Dokumentation (B) [Planende, Wartungspersonal]

Alle zum SIS gehörenden Hardware- und Softwarekomponenten, relevante Informationen, Verbindungen sowie Rollen und Zuständigkeiten MÜSSEN gesondert erfasst und dokumentiert werden.

IND.2.7.A2 Zweckgebundene Nutzung der Hard- und Softwarekomponenten (B) [Wartungspersonal]

Die Hard- und Softwarekomponenten, die zum SIS gehören oder im Zusammenhang mit diesem genutzt werden, DÜRFEN NICHT zweckentfremdet werde.

IND.2.7.A3 Änderung des Anwendungsprogramms auf dem Logiksystem (B) [Wartungspersonal]

Bereits vorhandene Schutzmechanismen am Logiksystem MÜSSEN aktiviert sein. Wenn dies nicht möglich ist, MÜSSEN alternative Maßnahmen ergriffen werden. Anwendungsprogramme auf den Logiksystemen DÜRFEN NUR von autorisierten Personen geändert oder zur Übertragung freigegeben werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

IND.2.7.A4 Verankerung von Informationssicherheit im Functional Safety Management (S) [ICS-Informationssicherheitsbeauftragte]

Alle Prozesse und Zuständigkeiten bezüglich der Informationssicherheit von SIS SOLLTEN klar definiert sein. Im Functional Safety Management SOLLTEN diese beschrieben und namentlich genannt sein.

IND.2.7.A5 Notfallmanagement von SIS (S) [ICS-Informationssicherheitsbeauftragte]

Die Behandlung von Sicherheitsvorfällen SOLLTE in einem Vorfallreaktionsplan festgehalten werden. Dieser SOLLTE die Rollen und Zuständigkeiten festhalten und die zu ergreifenden Maßnahmen enthalten.

IND.2.7.A6 Sichere Planung und Spezifikation des SIS (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]

Versehentliche oder unautorisierte Änderungen an der Spezifikation, Implementierung und an den Engineering-Daten SOLLTEN verhindert werden.

IND.2.7.A7 Trennung und Unabhängigkeit des SIS von der Umgebung (S) [Planende, Wartungspersonal]

Das SIS SOLLTE rückwirkungsfrei von seiner Umgebung betrieben werden, um seine Sicherheitsfunktionen gewährleisten zu können. Prozesse, die potenziell Auswirkungen auf das SIS haben, SOLLTEN dem Änderungsmanagementprozess des Functional Safety Management unterstellt werden.

IND.2.7.A8 Sichere Übertragung von Engineering Daten auf SIS (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]

Die Integrität der Engineering-Daten SOLLTE während der Übertragung auf SIS sichergestellt werden.

IND.2.7.A9 Absicherung der Daten- und Signalverbindungen (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]

Sofern keine Rückwirkungsfreiheit von Daten- und Signalverbindungen (Unidirektionalität) nachgewiesen werden kann, SOLLTEN diese Verbindungen geeignet abgesichert werden.

IND.2.7.A10 Anzeige und Alarmierung von simulierten oder gebrückten Variablen (S) [Planende]

Variablen der SIS, die durch Ersatzwerte besetzt (simuliert) oder von außen gebrückt werden, SOLLTEN in geeigneter Weise überwacht werden. Die Werte SOLLTEN den Benutzenden fortlaufend angezeigt werden. Grenzwerte SOLLTEN definiert werden. Wenn diese Grenzwerte erreicht werden, SOLLTEN die zuständigen Personen in geeigneter Weise alarmiert werden.

IND.2.7.A11 Umgang mit integrierten Systemen (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]

Für integrierte Systeme SOLLTE eine passende Strategie entwickelt werden, die den Umgang mit Komponenten regelt, welche die funktionale Sicherheit (Safety) betreffen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

IND.2.7.A12 Sicherstellen der Integrität und Authentizität von Anwendungsprogrammen und Konfigurationsdaten (H) [Planende]

Es SOLLTE darauf geachtet werden, dass die herstellenden Unternehmen geeignete Mechanismen entwickeln und integrieren, die die Integrität und Authentizität von Konfigurationsdaten und Anwendungsprogrammen auf dem Logiksystem oder auf den damit verbundenen Sensoren und Aktoren gewährleisten. Jegliche Software, die als Download angeboten wird, SOLLTE vor Manipulation geschützt werden. Verletzungen der Integrität SOLLTEN automatisch erkannt und gemeldet werden.

4. Weiterführende Informationen

4.1. Wissenswertes

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.

Die internationalen Normen

- 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)

stellen weitere Hilfsmittel zur Einrichtung von IT-Sicherheit in Safety Instrumented Systems zur Verfügung.

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

- Blatt 2.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber - Presswerk“ sowie
- Blatt 3.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber - LDPE-Anlage“

bietet ein Vorgehensmodell und Anwendungsbeispiele für Informationssicherheit im ICS-Umfeld.