IND.2.2: Speicherprogrammierbare Steuerung (SPS)

1 Beschreibung

1.1 Einleitung

Eine Speicherprogrammierbare Steuerung (SPS, engl. Programmable Logic Controller, PLC) ist eine ICS-Komponente. Sie übernimmt Steuerungs- und Regelaufgaben in der Betriebstechnik (engl. Operational Technology, OT). Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind heute fließend, so kann z. B. auch ein Fernwirkgerät (engl. Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen oder ein Programmable Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs zu vereinen. Jedoch ist die SPS immer noch das klassische Automatisierungsgerät, sodass in diesem Baustein die Begriffe SPS, RTU und PAC synonym verwendet werden.

Eine SPS verfügt über digitale Ein- und Ausgänge, ein Echtzeitbetriebssystem (Firmware) sowie weitere Schnittstellen für Ethernet oder Feldbusse. Die Verbindung zu Sensoren und Aktoren erfolgt über die analogen oder digitalen Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit Prozessleitsystemen erfolgt meist über die Ethernet-Schnittstelle und IP-basierte Netze.

Die möglichen Realisierungen sind vielfältig, eine Speicherprogrammierbare Steuerung kann als Baugruppe, Einzelgerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden. Am häufigsten anzutreffen sind modulare Speicherprogrammierbare Steuerungen, die aus verschiedenen funktionalen Steckmodulen zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualisieren, Alarmieren und Protokollieren durch die SPS übernommen.

Aufgrund der im OT-Umfeld typischen hohen Verfügbarkeitsanforderungen und der oft extremen Umgebungsbedingungen wie Hitze oder Kälte, Staub, Vibration oder Korrosion wurden ICS-Komponenten schon immer als robuste Geräte mit hoher Zuverlässigkeit und langer Lebensdauer konstruiert.

Eine SPS wird normalerweise über Spezialsoftware des jeweiligen Herstellers konfiguriert bzw. programmiert. Das wird entweder über sogenannte Programmiergeräte, z. B. als Anwendung unter Windows oder Linux, oder über eine Engineering-Station durchgeführt, welche die Daten über ein Netz verteilt.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, alle Arten von Speicherprogrammierbaren Steuerungen abzusichern, unabhängig von Hersteller, Bauart, Einsatzzweck und -ort. Der Baustein kann für eine einzelne SPS oder eine zusammenhängende als SPS eingesetzte Baugruppe angewendet werden.

1.3 Abgrenzung und Modellierung

Der Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* ist auf jede SPS-Komponente bzw. jede Gruppe davon einmal anzuwenden.

Der vorliegende Systembaustein soll alle Arten von Speicherprogrammierbaren Steuerungen absichern, hierzu gehört eine SPS und auch Geräte, die gleiche oder ähnliche Funktionen integrieren. Er ergänzt den Baustein IND.2.1 *Allgemeine ICS-Komponente*. Bei der Anwendung ist dieser Baustein daher auch zu berücksichtigen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Betriebs- und Steuerungstechnik* umgesetzt werden. Ebenso wird der Bereich funktionale Sicherheit (Safety) nicht behandelt.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* von besonderer Bedeutung:

2.1 Unvollständige Dokumentation

Speicherprogrammierbare Steuerungen sind oft unvollständig dokumentiert, sodass nicht alle Produktfunktionen bekannt sind. Besonders lückenhaft sind häufig die Angaben über die verwendeten Dienste, Protokolle und Kommunikationsports sowie zur Berechtigungsverwaltung. Das erschwert jedoch die Gefährdungsanalyse, da Schnittstellen, Funktionen sowie sicherheitsrelevante Mechanismen übersehen werden. Dadurch können potenzielle Gefährdungen nicht berücksichtigt werden. Zudem kann nicht oder nur eingeschränkt auf neue Schwachstellen reagiert werden, wenn diese nicht erfasst sind.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* aufgeführt. Grundsätzlich ist der ICS-Informationssicherheitsbeauftragte (ICS-ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Grundsätzlich zuständig	ICS-Informationssicherheitsbeauftragter
Weitere Zuständigkeiten	ICS-Administrator

3.1 Basis-Anforderungen

Für den Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* sind keine Basis-Anforderungen definiert.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)*. Sie SOLLTEN grundsätzlich umgesetzt werden.

IND.2.2.A1 Erweiterte Systemdokumentation für Speicherprogrammierbare Steuerungen [ICS-Administrator] (S)
Steuerungsprogramme und Konfigurationen SOLLTEN immer archiviert werden, wenn sie verändert werden. Ändert sich die Konfiguration oder werden Komponenten ausgetauscht, SOLLTE dies vollständig dokumentiert werden.

IND.2.2.A2 Benutzerkontenkontrolle und restriktive Rechtevergabe [ICS-Administrator] (S)
Zugriffsrechte auf Funktionen und Schnittstellen einer SPS SOLLTEN restriktiv vergeben werden. Bestehende Benutzerkonten SOLLTEN regelmäßig daraufhin überprüft werden, ob sie noch erforderlich sind. Es SOLLTE zudem geprüft werden, ob die zugewiesenen Berechtigungen noch korrekt sind. Wenn sich an den Zuständigkeiten der Mitarbeiter etwas ändert, SOLLTEN die Berechtigungen umgehend angepasst werden.

IND.2.2.A3 Zeitsynchronisation [ICS-Administrator] (S)
Für die Systemzeit SOLLTE eine zentrale automatisierte Zeitsynchronisation eingerichtet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Für den Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4 Weiterführende Informationen

4.1 Wissenswertes

Zum Baustein IND.2.2 *Speicherprogrammierbare Steuerung* liegen keine weiteren Informationen vor.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.41 Sabotage

Elementare Gefährdungen Anforderungen	CIA	G 0.14	G 0.15	G 0.19	G 0.21	G 0.22	G 0.23	G 0.30	G 0.41
IND.2.2.A1					X	X	X		X
IND.2.2.A2		X	X	X	X	X	X	X	X
IND.2.2.A3					X	X			