Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: IND.2.2 Speicherprogrammierbare Steuerung (SPS)

1. Einleitung

Diese Umsetzungshinweise geben Hilfestellung bei der Umsetzung der spezifischen Sicherheitsanforderungen für Speicherprogrammierbare Steuerungen und vergleichbare Automatisierungsgeräte, die Teil einer ICS-Anlage bzw. der Operational Technology (OT) sind. Eine SPS ist eine elektronische Komponente zur Steuerung oder Regelung und ist Teil einer Maschine oder Anlage.

SPSen gibt es in diversen Bauformen (Baugruppe, Slot-SPS, Soft-SPS, Busklemme). Je nach Branche gibt es ähnliche Geräte mit vergleichbaren Funktionen, jedoch anderen Bezeichnungen.

Grundsätzlich beziehen sich der Baustein sowie die vorliegenden Umsetzungshinweise auf SPSen aller Bauarten. Dabei ist jedoch zu beachten, dass sich nicht jede Maßnahme mit jedem Gerätetyp wortwörtlich umsetzen lässt. Es ist bezüglich der Begrifflichkeiten immer diejenige Interpretation zu wählen, die der Absicht der Anforderung am nächsten kommt. Dies betrifft insbesondere emulierte Soft-SPSen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* aufgeführt.

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

2.1. Maßnahmen zum Baustein IND.2.2 Speicherprogrammierbare Steuerung (SPS)

IND.2.2.M1 Erweiterte Systemdokumentation für speicherprogrammierbare Steuerungen (S)

Eine vollständige Systemdokumentation ist für den sicheren Betrieb einer ICS-Umgebung zwingend erforderlich. Die Dokumentation schafft die gebotene Transparenz über die eingesetzten Geräte, deren Spezifika und deren Integration. Sie bildet die Grundlage für das Schwachstellen-Management und den sicheren Betrieb. Nur eine aktuelle Dokumentation kann dabei ihren Zweck erfüllen.

Die Systemdokumentation der Geräte wird zum integralen Bestandteil der Gesamtdokumentation der ICS-Struktur. Sie umfasst die systemspezifischen Gegebenheiten. Der Systembetrieb der Automatisierungsgeräte erfolgt eingebettet in die etablierten Betriebsprozesse zur geregelten Durchführung von Änderungen, zur Bearbeitung von Störungen oder zum Schwachstellen-Management der ICS-Umgebung und sollte diese Aspekte nur insofern betrachten, wie Besonderheiten beim Betrieb der Automatisierungsgeräte zu berücksichtigen sind.

Die Systemdokumentation der Geräte umfasst typischerweise nachfolgende Informationen:

- Funktion / Zweck des Geräts
- Informationen zu den eingesetzten Komponenten
    - Hardware-Komponenten und deren Typ und Hersteller
    - Laufzeit des Hersteller-Supports
    - bestehende Wartungsverträge
    - Versionsangaben zur eingesetzten Hard- und Software (auch Firmware)
- Installation und Wiederherstellung (z. B. mit Hilfe von Ersatzgeräten)
- System- und Sicherheitskonfiguration
    - aktivierte Dienste / Protokolle
    - Geräteschnittstellen
    - Protokollierungseinstellungen
    - Sicherheitsfunktionen wie Firewall bzw. Access Control Lists, VPN, Integritätsschutz
- Benutzer- und Rechtemodell
- eingesetzte Protokolle und Kommunikationsmatrix
- Informationen zum Betrieb der Geräte
    - Testmöglichkeiten bei Änderungen
    - betriebliche Überwachung (Monitoring)
    - Fernzugriff
    - Sicherung
    - Regeltätigkeiten / Wartungspläne
- Verweise / Hinweise zur Ablage von technischen Benutzerkonten und Notfalladministrationsbenutzern

Die Systemdokumentation kann durch Referenzierung einer Konfigurationssicherung unterstützt werden. Die vom Herstellerstandard abweichenden Einstellungen und Anpassungen an die Infrastruktur sollten daraus nachvollziehbar begründet hervorgehen.

Der Zugriff auf die Systemdokumentation sollte auf berechtigte Personen beschränkt und für diese auch im Störungsfall leicht möglich sein. Hierzu kann neben der digitalen Ablage in einem Netzlaufwerk sowohl eine geschützte Ablage auf hochverfügbaren Systemen (z. B. Steuerungssystem) als auch eine papiergebundene Fassung hilfreich sein.

IND.2.2.M2 ENTFALLEN

Die zugehörige Anforderung ist entfallen.

IND.2.2.M3 Zeitsynchronisation (S)

Eine synchronisierte Systemzeit ist neben funktionalen Gesichtspunkten wie etwa der korrekten zeitlichen Einordnung von Messdaten eine wichtige Voraussetzung für die Korrelation von protokollierten Systemereignissen. Das OT-System sollte daher auch aus diesem Grund über eine anlagenweit synchronisierte Systemzeit verfügen (siehe auch IND.1.NET.1.2.M8 *Zeit-Synchronisation* sowie IND.1.M10 *Monitoring, Protokollierung und Detektion*).

Die Systemzeit kann hierbei aus einem eigenen Zeitempfänger oder aus einer zentralen Zeitquelle bezogen werden. Wird eine offizielle Systemzeit benötigt, sollte die Zeit über einen DCF77-Empfänger aus amtlicher Quelle bezogen werden, alternativ per GPS.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

Für den Umsetzungshinweis UH_IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* sind keine Quellenverweise vorhanden.