



IND.2.3 Sensoren und Aktoren

1. Beschreibung

1.1. Einleitung

Sensoren sind als elektronische Komponente mit Mikroprozessor und Software ausgeführte Messumformer, die eine physikalische Größe in einen elektrischen Ausgabewert wandeln. Dieser wird als normiertes Einheitssignal (häufig 4 bis 20mA, 0 bis 10V) an einer seriellen Schnittstelle oder als digitale Informationen, die über einen Feldbus oder Ethernet-Protokolle übertragen werden, bereitgestellt. Messumformer stellen neben den Messwerten häufig noch Schnittstellen bereit, über die eine Diagnose und Parametrierung erfolgt. So kann ein Sensor neben einem elektronischen Ausgabewert auch noch über weitere Schnittstellen verfügen, z. B. WLAN-, Bluetooth- oder Wireless-HART-Schnittstellen für Parametrierung und Diagnose.

Auf dem Markt gibt es viele unterschiedliche Sensoren, z. B. um physikalische Größen zu messen. Je nach Aufgabe variieren der Funktionsumfang und die Leistungsfähigkeit eines Sensors stark. Die Bandbreite umfasst einerseits Sensoren, die lediglich Messwerte liefern und nicht konfiguriert werden müssen. Es gibt aber auch solche, die eine Kalibrierung, Konfiguration oder Vorverarbeitung von Daten bis hin zur vollständigen Signalverarbeitung ermöglichen (intelligente Sensoren, smart sensors).

1.2. Zielsetzung

Ziel dieses Bausteins ist es, alle Arten von Sensoren abzusichern, unabhängig von herstellenden Unternehmen, Bauart, Einsatzzweck und -ort. Er kann für einen einzelnen Sensor oder eine zusammenhängende Sensor-Baugruppe angewendet werden.

1.3. Abgrenzung und Modellierung

Der Baustein IND.2.3 *Sensoren und Aktoren* ist auf Sensoren und Aktoren einmal anzuwenden.

Der vorliegende Baustein ist anzuwenden, um Sensoren abzusichern. Er ergänzt den übergeordneten Baustein IND.2.1 *Allgemeine ICS-Komponente* und setzt diesen voraus.

Einfache Sensoren ohne Konfigurationsschnittstellen oder komplexere Verarbeitungslogik werden durch den Baustein nicht erfasst. Denn bei diesen beschränken sich die möglichen Schutzmaßnahmen lediglich darauf, den Zugang zum Sensor abzusichern und zu überwachen, ob er aktiv ist.

Auch behandelt der Baustein nicht den Schutz komplexer drahtloser Sensornetze. Er beschreibt lediglich, wie sich einzelne Sensoren absichern lassen. Weiterhin werden keine

Sicherheitsanforderungen für Prozessleit- und Automatisierungstechnik beschrieben. Dafür muss der Baustein IND.1 *Prozessleit- und Automatisierungstechnik* umgesetzt werden.

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.2.3 *Sensoren und Aktoren* von besonderer Bedeutung.

2.1. Unzureichende Sicherheitsanforderungen bei der Beschaffung

Sensoren für ICS-Komponenten in industriellen Umgebungen sind häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Beispiele hierfür sind extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Atmosphären. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Umgebungseinflüsse können die Sensoren von ICS-Komponenten schneller verschleifen und früher ausfallen oder fehlerhafte Werte messen.

Aus mangelndem Bewusstsein für die Risiken und aus Kostengründen wird bei der Beschaffung und Installation häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in Sensoren mitunter schwerwiegende Schwachstellen enthalten sein, die sich später nur sehr aufwändig beheben lassen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.3 *Sensoren und Aktoren* 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	ICS-Informationssicherheitsbeauftragte
Weitere Zuständigkeiten	Wartungspersonal, OT-Betrieb (Operational Technology, OT)

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.2.3.A1 Installation von Sensoren (B) [OT-Betrieb (Operational Technology, OT), Wartungspersonal]

Sensoren MÜSSEN in geeigneter Weise installiert werden. Sensoren MÜSSEN ausreichend robust sein. Sie MÜSSEN zuverlässig unter den vorhandenen Umgebungsbedingungen wie großer Wärme, Kälte, Staub, Vibration oder Korrosion messen können.

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.2.3.A2 Kalibrierung von Sensoren (S) [Wartungspersonal]

Wenn notwendig, SOLLTEN Sensoren regelmäßig kalibriert werden. Die Kalibrierungen SOLLTEN geeignet dokumentiert werden. Der Zugang zur Kalibrierung eines Sensors MUSS geschützt sein.

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.2.3.A3 Drahtlose Kommunikation (H)

Drahtlose Verwaltungsschnittstellen wie Bluetooth, WLAN oder NFC SOLLTEN NICHT benutzt werden. Alle nicht benutzten Kommunikationsschnittstellen SOLLTEN deaktiviert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Zum Baustein *IND.2.3 Sensoren und Aktoren* liegen keine weiteren Informationen vor.