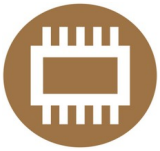

IND.2: ICS-Komponenten

IND.2.4: Maschine

1 Beschreibung

1.1 Einleitung

Eine Maschine ist eine technische Vorrichtung, die automatisierte Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Werkstücke auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System gesteuert, das die entsprechenden Arbeitsanweisungen und -schritte vorgibt. Solche Maschinen werden auch als Automaten bezeichnet.

Meistens werden Maschinen von Maschinenbauern konstruiert und mit bestimmten vordefinierten Funktionen ausgestattet. Der Betreiber der Maschine kann allerdings auch die Parameter bestimmen, nach denen sie arbeiten soll. So lassen sich beispielsweise Formen, die gefräst werden sollen, oder Kalibrierungen für bestimmte Materialien einstellen. Damit der Betreiber die Parameter verändern kann, verfügen Maschinen über verschiedene Schnittstellen, z. B. für Wechseldatenträger, spezialisierte Programmiergeräte oder Netzzugriffe.

Häufig werden von Maschinenbauern auch Fernwartungsdienstleistungen angeboten, um frühzeitigen Verschleiß zu erkennen oder in Problemsituationen schnell reagieren zu können.

1.2 Zielsetzung

Dieser Baustein beschreibt, wie elektronisch gesteuerte, halb- oder vollautomatische Maschinen (z. B. CNC-Maschinen) unabhängig von Hersteller, Bauart, speziellem Einsatzzweck und -ort abgesichert werden können.

1.3 Abgrenzung und Modellierung

Der Baustein IND.2.4 *Maschine* ist auf jede Maschine einmal anzuwenden.

Der vorliegende Baustein ergänzt den übergeordneten Baustein IND.2.1 *Allgemeine ICS-Komponente* und setzt voraus, dass dieser umgesetzt wurde. Darüber hinaus werden nur Anforderungen für Maschinen definiert, auf deren interne Strukturen eine Institution nicht zugreifen kann.

Auch werden keine Sicherheitsanforderungen für Prozessleit- und Automatisierungstechnik beschrieben. Dafür muss der Baustein IND.1 *Prozessleit- und Steuerungstechnik* umgesetzt werden. Ebenso wird der Bereich der funktionalen Sicherheit nicht behandelt. Näheres dazu findet sich im Baustein IND.2.7 *Safety Instrumented Systems*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein IND.2.4 *Maschine* von

besonderer Bedeutung:

2.1 Ausfall oder Störung durch ungenügende Wartung

Werden Maschinen nicht regelmäßig gewartet, können sie frühzeitig nicht mehr korrekt funktionieren oder ganz ausfallen. Durch Fehlfunktionen können z. B. Mitarbeiter gefährdet werden oder die Produktion könnte erheblich beeinträchtigt werden.

2.2 Gezielte Manipulationen

Sind die Schnittstellen einer Maschine ungenügend geschützt, können Angreifer die Maschine manipulieren, z. B. über lokale Programmiergeräte oder Netzdienste. Dadurch können Werkstücke beschädigt werden oder ganze Produktreihen fehlerhaft sein. Die Angreifer können aber auch die Maschine selbst beschädigen, sodass auch dadurch ein wirtschaftlicher Verlust entsteht.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.4 *Maschine* 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.

Zuständigkeit	**Rolle**
Grundsätzlich zuständig	ICS-Informationssicherheitsbeauftragter
Weitere Zuständigkeiten	OT-Betrieb (Operational Technology, OT)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein IND.2.4 *Maschine* vorrangig erfüllt werden:

IND.2.4.A1 Fernwartung durch Maschinen- und Anlagenbauer [OT-Betrieb (Operational Technology, OT)] (B)

Für die Fernwartung einer Maschine MUSS es eine zentrale Richtlinie geben. Darin MUSS geregelt werden, wie die jeweiligen Fernwartungslösungen einzusetzen sind. Die Richtlinie MUSS auch festlegen, wie Kommunikationsverbindungen geschützt werden sollen. Hierüber hinaus MUSS sie auch beschreiben, welche Aktivitäten während der Fernwartung überwacht werden sollen.

Außerdem SOLLTE NICHT möglich sein, dass über die Fernwartung einer Maschine auf andere IT-Systeme oder Maschinen der Institution zugegriffen werden kann.

Mit einem Dienstleister MUSS vereinbart werden, wie er die in der Maschine gespeicherten Informationen verwerten darf.

IND.2.4.A2 Betrieb nach Ende der Gewährleistung [OT-Betrieb (Operational Technology, OT)] (B)

Es MUSS ein Prozess etabliert werden, der gewährleistet, dass die Maschine auch über den Gewährleistungszeitraum hinaus sicher weiterbetrieben werden kann. Hierzu MÜSSEN mit dem Lieferanten weitere Unterstützungsleistungen vertraglich vereinbart werden.

3.2 Standard-Anforderungen

Für den Baustein IND.2.4 *Maschine* sind keine Standard-Anforderungen definiert.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Für den Baustein IND.2.4 *Maschine* sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4 Weiterführende Informationen

4.1 Wissenswertes

Zum Baustein IND.2.4 *Maschine* liegen keine weiterführenden 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.2.4 *Maschine* von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.39 Schadprogramme