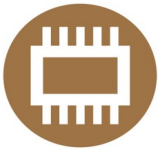

IND.2.1: Allgemeine ICS-Komponente

1 Beschreibung

1.1 Einleitung

Eine ICS-Komponente ist eine elektronische Komponente, die eine Maschine oder Anlage steuert oder regelt. Sie ist damit Bestandteil eines industriellen Steuerungssystems (engl. Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (engl. Operational Technology, OT). Diese Komponenten können Speicherprogrammierbare Steuerungen (SPS) (engl. Programmable Logic Controller, PLC), Sensoren, Aktoren, eine Maschine oder andere Teile eines ICS sein.

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.

ICS-Komponenten werden 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 Anwendungsprogramme in die Speicherprogrammierbaren Steuerungen lädt.

Die Rolle des Informationssicherheitsbeauftragten für den Bereich der industriellen Automatisierung wird je nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeichnung neben ICS-Informationssicherheitsbeauftragter (ICS-ISB) ist auch Industrial Security Officer.

1.2 Zielsetzung

Ziel dieses Bausteins ist die Absicherung aller Arten von ICS-Komponenten, unabhängig von Hersteller, Bauart, Einsatzzweck und -ort. Er kann für ein einzelnes Gerät oder ein aus mehreren Komponenten aufgebautes modulares Gerät verwendet werden.

1.3 Abgrenzung und Modellierung

Der Baustein IND.2.1 *Allgemeine ICS-Komponente* ist auf jede im Informationsverbund eingesetzte ICS-Komponente anzuwenden.

Die Anforderungen sind für eine allgemeine ICS-Komponente erarbeitet. Für spezifischere ICS-Komponenten, z. B. Sensoren und Aktoren oder Maschinen, sind zusätzliche Bausteine wie IND.2.3 *Sensoren und Aktoren* bzw. IND.2.4 *Maschine* verfügbar. Dort sind Anforderungen beschrieben, die über

die allgemeinen Anforderungen dieses Bausteins hinausgehen und zusätzlich umgesetzt werden müssen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* umgesetzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein IND.2.1 *Allgemeine ICS-Komponente* von besonderer Bedeutung:

2.1 Unsichere Systemkonfiguration

Die Standardkonfiguration von ICS-Komponenten ist häufig darauf ausgelegt, dass die Komponenten korrekt funktionieren und sich leicht in Betrieb nehmen lassen. Sicherheitsmechanismen spielen dabei oft eine untergeordnete Rolle. So sind in der Standardeinstellung häufig alle Dienste, Protokolle und Anschlüsse eingeschaltet und bleiben aktiv, auch wenn sie nicht benutzt werden. Ebenso bleiben voreingestellte Berechtigungen häufig unverändert.

Es ist für Angreifer leicht, diese ICS-Komponenten zu übernehmen und zu manipulieren. Ebenso ist es möglich, dass ein Angreifer die unsichere Systemkonfiguration ausnutzt, um die ICS-Komponente als Ausgangspunkt für weitere Angriffe zu nutzen. In der Folge können institutionskritische Informationen abfließen oder auch der gesamte Betrieb der Institution beeinträchtigt werden.

2.2 Unzureichendes Benutzer- und Berechtigungsmanagement

Einige ICS-Komponenten verfügen über ein eigenes Benutzer- und Berechtigungsmanagement. Ist dieses unzureichend konzipiert, kann es passieren, dass Mitarbeiter gemeinsam Benutzerkonten nutzen oder dass Berechtigungen von ausgeschiedenen Mitarbeitern oder Dienstleistern nicht gelöscht werden. Insgesamt können so unberechtigte Personen auf ICS-Komponenten zugreifen.

2.3 Unzureichende Protokollierung

Bei ICS-Komponenten beschränkt sich die Protokollierung häufig auf prozessrelevante Ereignisse. Für die Informationssicherheit relevante Daten werden oft nicht aufgezeichnet. Dadurch lassen sich Sicherheitsvorfälle nur schwer detektieren und hinterher nicht mehr rekonstruieren.

2.4 Manipulation und Sabotage einer ICS-Komponente

Die vielfältigen Schnittstellen von ICS-Komponenten führen zu einem erhöhten Manipulationsrisiko für IT-Systeme, die Software und übertragene Informationen. Je nach Motivation und Kenntnissen des Angreifers kann sich das lokal, aber auch standortübergreifend auswirken. Zudem können Status- und Alarmmeldungen oder sonstige Messwerte unterdrückt oder verändert werden.

Manipulierte Messwerte können Fehlentscheidungen von ICS-Komponenten bzw. des Bedienpersonals nach sich ziehen. Manipulierte Systeme können dazu genutzt werden, um andere Systeme oder Standorte anzugreifen oder um eine laufende Manipulation zu vertuschen.

2.5 Einsatz unsicherer Protokolle

Die im Umfeld industrieller Steuerungsanlagen eingesetzten Protokolle bieten teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Technische Informationen wie Mess- und Steuerwerte werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen. Ein Angreifer mit Zugang zum Übertragungsmedium kann dann die Inhalte der Kommunikation auslesen und verändern oder Steuerbefehle einschleusen. So kann er Handlungen provozieren bzw. den Betrieb direkt beeinflussen. Ein Angriff auf Protokollebene ist auch dann möglich, wenn die ICS-Komponente ansonsten sicher konfiguriert ist und selbst keine Schwachstellen aufweist.

2.6 Denial-of-Service-(DoS)-Angriffe

Ein Angreifer kann den Betrieb von ICS-Komponenten durch DoS-Angriffe beeinträchtigen. Bei Prozessen, die unter Echtzeitbedingungen ablaufen, kann bereits eine kürzere Störung zu Informations- oder Kontrollverlusten führen.

2.7 Schadprogramme

Die Bedrohung durch Schadprogramme verschärft sich auch für industrielle Steuerungsanlagen immer mehr. Infektionsmöglichkeiten ergeben sich durch Schnittstellen zur Office-IT (vertikale Integration) und zur Außenwelt. Aber auch mobile Endgeräte wie Service-Notebooks oder Wechseldatenträger, die bei der Programmierung und Wartung von ICS-Komponenten eingesetzt werden, stellen eine Gefahr dar. Denn durch Letztere können Schadprogramme auch in isolierte Umgebungen eingebracht werden.

2.8 Ausspionieren von Informationen

ICS-Komponenten enthalten häufig detaillierte Informationen über den geregelten oder überwachten Prozess bzw. Vorgang. Auch aus sonstigen übertragenen Werten wie Mess- oder Steuerungsdaten lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter.

Angreifer könnten hier im Rahmen von Industriespionage an Geschäftsgeheimnisse gelangen, z. B. an Rezepte, Verfahren oder anderes geistiges Eigentum. Auch können sie Informationen über die Funktionsweise einer ICS-Komponente und ihre Sicherheitsmechanismen gewinnen, die sie für weitere Angriffe benutzen können.

2.9 Manipulierte Firmware

Bei ICS-Komponenten lässt sich neben dem Anwendungsprogramm auch das Betriebssystem (Firmware) verändern. Dadurch kann manipulierte Software in das System gelangen. Die internen Speicher könnten durch ein kompromittiertes Programmiergerät über eine lokale Datenschnittstelle (z. B. USB) oder über eine andere bestehende Netzverbindung von einem Angreifer verändert werden. Ebenso könnte ein Software-Update auf dem Weg vom Hersteller zum Betreiber manipuliert worden sein. Schließlich könnte eine ICS-Komponente mit bereits kompromittierter Firmware beim Betreiber eintreffen, etwa bei manipulierter Lieferkette (engl. *supply chain*) oder einem Einkauf aus unsicheren Quellen. Ein Angreifer erhält dadurch die Möglichkeit, Prozesse und Abläufe zu verändern bzw. zu verfälschen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.1 *Allgemeine ICS-Komponente* 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	Mitarbeiter, Planer, Wartungspersonal, OT-Betrieb (Operational Technology, OT)

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein IND.2.1 *Allgemeine ICS-Komponente* vorrangig erfüllt werden:

IND.2.1.A1 Einschränkung des Zugriffs auf Konfigurations- und Wartungsschnittstellen [OT-Betrieb (Operational Technology, OT)] (B)

Standardmäßig eingerichtete bzw. vom Hersteller gesetzte Passwörter MÜSSEN gewechselt werden (siehe ORP.4 *Identitäts- und Berechtigungsmanagement)*. Der Wechsel MUSS dokumentiert werden. Die Passwörter MÜSSEN sicher hinterlegt werden.

Es MUSS sichergestellt werden, dass nur berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von ICS-Komponenten zugreifen können. Die Konfiguration von ICS-Komponenten DARF NUR nach einer Freigabe durch den Verantwortlichen oder nach einer Authentisierung geändert werden.

IND.2.1.A2 Nutzung sicherer Übertragungs-Protokolle für die Konfiguration und Wartung [Wartungspersonal, OT-Betrieb (Operational Technology, OT)] (B)

Für die Konfiguration und Wartung von ICS-Komponenten MÜSSEN sichere Protokolle eingesetzt werden. Die Informationen MÜSSEN geschützt übertragen werden.

IND.2.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.2.1.A4 Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen [Wartungspersonal, OT-Betrieb (Operational Technology, OT)] (B)

Alle nicht genutzten Dienste, Funktionen und Schnittstellen der ICS-Komponenten MÜSSEN deaktiviert oder deinstalliert werden.

IND.2.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

IND.2.1.A6 Netzsegmentierung [OT-Betrieb (Operational Technology, OT), Planer] (B)

ICS-Komponenten MÜSSEN von der Office-IT getrennt werden. Hängen ICS-Komponenten von anderen Diensten im Netz ab, SOLLTE das ausreichend dokumentiert werden. ICS-Komponenten SOLLTEN so wenig wie möglich mit anderen ICS-Komponenten kommunizieren.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein IND.2.1 *Allgemeine ICS-Komponente*. Sie SOLLTEN grundsätzlich erfüllt werden.

IND.2.1.A7 Erstellung von Datensicherungen [OT-Betrieb (Operational Technology, OT)] (S)

Vor jeder Systemänderung an einer ICS-Komponente MÜSSEN Backups erstellt werden.

IND.2.1.A8 Schutz vor Schadsoftware [OT-Betrieb (Operational Technology, OT)] (S)

ICS-Komponenten SOLLTEN durch geeignete Mechanismen vor Schadprogrammen geschützt werden (siehe OPS.1.1.4 *Schutz vor Schadprogrammen*). Wird dafür ein Virenschutzprogramm benutzt, SOLLTEN das Programm und die Virensignaturen nach der Freigabe durch den Hersteller immer auf dem aktuellen Stand sein.

Wenn die Ressourcen auf der ICS-Komponente nicht ausreichend sind oder die Echtzeitanforderung durch den Einsatz von Virenschutzprogrammen gefährdet werden könnte, SOLLTEN alternative Maßnahmen ergriffen werden, etwa die Abschottung der ICS-Komponente oder des Produktionsnetzes.

IND.2.1.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

IND.2.1.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

IND.2.1.A11 Wartung der ICS-Komponenten [Mitarbeiter, OT-Betrieb (Operational Technology, OT), Wartungspersonal] (S)
Bei der Wartung einer ICS-Komponente SOLLTEN immer die aktuellen und freigegebenen Sicherheitsupdates eingespielt werden. Updates für das Betriebssystem SOLLTEN erst nach Freigabe durch den Hersteller einer ICS-Komponente installiert werden. Alternativ SOLLTE die Aktualisierung in einer Testumgebung erprobt werden, bevor diese in einer produktiven ICS-Komponente eingesetzt wird. Für kritische Sicherheitsupdates SOLLTE kurzfristig eine Wartung durchgeführt werden.

IND.2.1.A12 ENTFALLEN (S)
Diese Anforderung ist entfallen.

IND.2.1.A13 Geeignete Inbetriebnahme von ICS-Komponenten [OT-Betrieb (Operational Technology, OT)] (S)
Bevor ICS-Komponenten in Betrieb genommen werden, SOLLTEN sie dem aktuellen, intern freigegebenen Firmware-, Software- und Patch-Stand entsprechen.

Neue ICS-Komponenten SOLLTEN in die bestehenden Betriebs-, Überwachungs- und Informationssicherheitsmanagement-Prozesse eingebunden werden.

IND.2.1.A14 ENTFALLEN (S)
Diese Anforderung ist entfallen.

IND.2.1.A15 ENTFALLEN (S)
Diese Anforderung ist entfallen.

IND.2.1.A16 Schutz externer Schnittstellen [OT-Betrieb (Operational Technology, OT)] (S)
Von außen erreichbare Schnittstellen SOLLTEN vor Missbrauch geschützt werden.

IND.2.1.A17 Nutzung sicherer Protokolle für die Übertragung von Mess- und Steuerdaten [OT-Betrieb (Operational Technology, OT)] (S)
Mess- oder Steuerdaten SOLLTEN bei der Übertragung vor unberechtigten Zugriffen oder Veränderungen geschützt werden. Bei Anwendungen mit Echtzeitanforderungen SOLLTE geprüft werden, ob dies umsetzbar ist. Werden Mess- oder Steuerdaten über öffentliche Netze übertragen, SOLLTEN sie angemessen geschützt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein IND.2.1 *Allgemeine ICS-Komponente* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

IND.2.1.A18 Kommunikation im Störfall [OT-Betrieb (Operational Technology, OT), Mitarbeiter] (H)
Es SOLLTE alternative und unabhängige Kommunikationsmöglichkeiten geben, die bei einem Störfall benutzt werden können, um handlungsfähig zu bleiben.

IND.2.1.A19 Security-Tests [OT-Betrieb (Operational Technology, OT)] (H)
Mithilfe von regelmäßigen Security-Tests SOLLTE geprüft werden, ob die technischen Sicherheitsmaßnahmen noch effektiv umgesetzt sind. Die Security-Tests SOLLTEN nicht im laufenden

Anlagenbetrieb erfolgen. Die Tests SOLLTEN auf die Wartungszeiten geplant werden. Die Ergebnisse SOLLTEN dokumentiert werden. Erkannte Risiken SOLLTEN bewertet und behandelt werden.

IND.2.1.A20 Vertrauenswürdiger Code [OT-Betrieb (Operational Technology, OT)] (H)
Firmware-Updates oder neue Steuerungsprogramme SOLLTEN NUR eingespielt werden, wenn vorher ihre Integrität überprüft wurde. Sie SOLLTEN nur aus vertrauenswürdigen Quellen stammen.

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 Maßnahmen für die IT-Sicherheit in ICS für Hersteller und Integratoren von ICS.

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.

In der NIST Special Publication 800-82 - „Guide to Industrial Control Systems (ICS) Security“ ist beschrieben, wie IT-Sicherheit für Industrial Control Systems umgesetzt werden kann.

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.2.1 *Allgemeine ICS-Komponente* von Bedeutung.

G 0.2	Ungünstige klimatische Bedingungen
G 0.4	Verschmutzung, Staub, Korrosion
G 0.8	Ausfall oder Störung der Stromversorgung
G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.10	Ausfall oder Störung von Versorgungsnetzen
G 0.12	Elektromagnetische Störstrahlung
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 0.25	Ausfall von Geräten oder Systemen
G 0.28	Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.41 Sabotage

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen