Bundesamt
für Sicherheit in der
Informationstechnik

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 (englisch Industrial Control System, ICS) oder allgemeiner einer Betriebstechnik (englisch Operational Technology, OT). Diese Komponenten können Speicherprogrammierbare Steuerungen (SPS) (englisch 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 herstellenden Unternehmens 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 oder der Informationssicherheitsbeauftragten für den Bereich der industriellen Automatisierung wird je nach Art und Ausrichtung der Institution anders genannt. Eine weitere Bezeichnung neben ICS-Informationssicherheitsbeauftragte (ICS-ISB) ist auch Industrial Security Officer.

1.2. Zielsetzung

Ziel dieses Bausteins ist die Absicherung aller Arten von ICS-Komponenten, unabhängig von herstellenden Unternehmen, 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

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.2.1 *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 Angreifende leicht, diese ICS-Komponenten zu übernehmen und zu manipulieren. Ebenso ist es möglich, dass bei einem Angriff die unsichere Systemkonfiguration ausgenutzt wird, 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 Benutzenden- und Berechtigungsmanagement

Einige ICS-Komponenten verfügen über ein eigenes Benutzenden- und Berechtigungsmanagement. Ist dieses unzureichend konzipiert, kann es passieren, dass Mitarbeitende gemeinsam Konten nutzen oder dass Berechtigungen von ausgeschiedenen Mitarbeitenden oder Dienstleistenden 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 der

Angreifenden 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. Dritte mit Zugang zum Übertragungsmedium können dann die Inhalte der Kommunikation auslesen und verändern oder Steuerbefehle einschleusen. So können Handlungen provoziert bzw. der Betrieb direkt beeinflusst werden. 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

Angreifende können 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.

Dritte 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 Angreifenden verändert werden. Ebenso könnte ein Software-Update auf dem Weg vom herstellenden Unternehmen zum Betreibenden manipuliert worden sein. Schließlich könnte eine ICS-Komponente mit bereits kompromittierter Firmware beim Betreibenden eintreffen, etwa bei manipulierter Lieferkette (englisch

supply chain) oder einem Einkauf aus unsicheren Quellen. Angreifende erhalten 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. 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	Mitarbeitende, Planende, 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.2.1.A1 Einschränkung des Zugriffs auf Konfigurations- und Wartungsschnittstellen (B) [OT-Betrieb (Operational Technology, OT)]

Standardmäßig eingerichtete bzw. vom herstellenden Unternehmen 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 Mitarbeitende auf Konfigurations- und Wartungsschnittstellen von ICS-Komponenten zugreifen können. Die Konfiguration von ICS-Komponenten DARF NUR nach einer Freigabe durch die verantwortliche Person oder nach einer Authentisierung geändert werden.

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

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 (B) [Wartungspersonal, OT-Betrieb (Operational Technology, OT)]

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 (B) [OT-Betrieb (Operational Technology, OT), Planende]

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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

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

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

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

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 das herstellende Unternehmen 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 (S) [Mitarbeitende, OT-Betrieb (Operational Technology, OT), Wartungspersonal]

Bei der Wartung einer ICS-Komponente SOLLTEN immer die aktuellen und freigegebenen Sicherheitsupdates eingespielt werden. Updates für das Betriebssystem SOLLTEN erst nach Freigabe durch das herstellende Unternehmen 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 (S) [OT-Betrieb (Operational Technology, OT)]

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 (S) [OT-Betrieb (Operational Technology, OT)]

Von außen erreichbare Schnittstellen SOLLTEN vor Missbrauch geschützt werden.

IND.2.1.A17 Nutzung sicherer Protokolle für die Übertragung von Mess- und Steuerdaten (S) [OT-Betrieb (Operational Technology, OT)]

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 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.2.1.A18 Kommunikation im Störfall (H) [OT-Betrieb (Operational Technology, OT), Mitarbeitende]

Es SOLLTE alternative und unabhängige Kommunikationsmöglichkeiten geben, die bei einem Störfall benutzt werden können, um handlungsfähig zu bleiben.

IND.2.1.A19 Security-Tests (H) [OT-Betrieb (Operational Technology, OT)]

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 (H) [OT-Betrieb (Operational Technology, OT)]

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 herstellende Unternehmen 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.