

# IND.1 Prozessleit- und Automatisierungstechnik

## 1. Beschreibung

### 1.1. Einleitung

Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.

In der Industrie, zu der unter anderem auch die Kritischen Infrastrukturen gehören, zählen dazu insbesondere industrielle Steuerungssysteme (Industrial Control Systems, ICS) und Automationslösungen, die dort Steuerungs- und Regelfunktionen aller Art übernehmen. Weitere Beispiele sind Laborgeräte, z. B. automatisierte Mikroskope oder Analysewerkzeuge, Logistiksysteme, wie Barcodescanner mit Kleinrechner, oder Gebäudeleittechnik.

Die in der Vergangenheit übliche physische Trennung der OT von anderen IT-Systemen und Datennetzen in Büroanwendungen ist heute aufgrund zunehmender Integrationsanforderungen nur in Ausnahmefällen bei erhöhtem Schutzbedarf anwendbar. Mehrstufige Produktionsschritte und deren übergreifende Steuerung sowie regulatorische Anforderungen machen es zunehmend notwendig, die OT auch über Organisationsgrenzen hinweg zu öffnen. Diese Entwicklung wird durch den Trend zur Optimierung von Fertigungsprozessen noch beschleunigt, vor allem im Rahmen der Industrie 4.0.

Da in der OT zunehmend auch IT-Komponenten aus der Office-IT eingesetzt werden, ist diese inzwischen ähnlich gefährdet. Gleichzeitig weist die OT gegenüber der klassischen IT aber wesentliche Unterschiede auf, die es erschweren, dort etablierte Sicherheitsverfahren anzuwenden. So kann es aufgrund von Vorgaben der herstellenden Unternehmen oder gesetzlichen Anforderungen Beschränkungen geben, die Veränderungen an Komponenten verhindern oder erschweren, wie zum Beispiel das Einspielen von Sicherheitsupdates oder nachträgliche Härtungsmaßnahmen. Die OT unterliegt zudem in der Regel deutlich längeren Lebenszyklen, auch über die Unterstützung der herstellenden Unternehmen hinaus, sodass Sicherheitsupdates nicht durchgängig verfügbar sind.

Ein wesentlicher Unterschied ergibt sich für die OT auch aus den oft hohen Verfügbarkeits- und Integritätsanforderungen. Denn im Vergleich dazu ist bei der Office-IT die Verfügbarkeit häufig von nachrangiger Bedeutung. Störungen von OT-Systemen können dagegen Gefährdungen von Leib, Leben und Umwelt nach sich ziehen und sind zumeist nicht durch einen Neustart zu beheben.

## 1.2. Zielsetzung

Ziel dieses Bausteins ist es, geeignete Anforderungen an die Informationssicherheit der OT aufzuzeigen. Er enthält komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen.

## 1.3. Abgrenzung und Modellierung

Der Baustein *IND.1 Prozessleit- und Automatisierungstechnik* ist auf jedes IT-System mit Prozessleit- und Automatisierungstechnik innerhalb des Informationsverbunds mindestens einmal anzuwenden.

Der Baustein ist übergreifend umzusetzen. Bestehen in den einzelnen Bereichen mit Prozessleit- und Automatisierungstechnik unterschiedliche Sicherheitsanforderungen an die Informationssicherheit, sollte der Baustein auf jedes IT-System getrennt angewandt werden.

Die Ausgestaltung der OT kann je nach Zweck, Branche, den eingesetzten IT-Systemen und der Technik sowie aufgrund des langen Einsatzzeitraums selbst bei vergleichbaren Anwendungsfällen stark variieren. Werden die Sicherheitsmaßnahmen auf Basis der Anforderungen aus diesem Baustein ausgewählt, sind diese Besonderheiten dabei zu berücksichtigen. Sie können wesentlichen Einfluss auf die Ausgestaltung des Sicherheitskonzepts nehmen. Auch der Risikoanalyse kann aus diesem Grund bereits bei der Erstellung eines Sicherheitskonzepts für den normalen Schutzbedarf eine hohe Bedeutung zukommen.

Das Betriebspersonal sollte in Bezug auf relevante Bedrohungen und Gefährdungen geschult und sensibilisiert werden. Hierfür ist der Baustein *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit* umzusetzen.

Zusätzlich zu diesem Baustein ist die umgebende Infrastruktur der OT, also Standorte, Anlagen, Gebäude oder Räume, durch möglichst spezifische Bausteine zu modellieren, um die Schutzwirkung dieses Bausteins zu ergänzen.

Für eine geeignete Protokollierung im Bereich der Prozessleit- und Steuerungstechnik ist der Baustein *OPS.1.1.5 Protokollierung* umzusetzen.

ICS-Systeme sollten grundsätzlich mit berücksichtigt werden, wenn der Baustein *ORP.4 Identitäts- und Berechtigungsmanagement* umgesetzt wird.

## 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.1 Prozessleit- und Automatisierungstechnik* von besonderer Bedeutung.

### 2.1. Beeinträchtigung durch schädliche Umgebungseinflüsse

ICS-Komponenten sind in industriellen Umgebungen häufig besonderen Bedingungen ausgesetzt, die den sicheren Betrieb beeinträchtigen können. Dazu zählen extreme Wärme, Kälte, Feuchtigkeit, Staub, Vibration oder auch ätzend oder korrodierend wirkende Umgebungen. Häufig treten auch mehrere Faktoren gleichzeitig auf. Durch solche schädlichen Einflüsse können ICS-Komponenten schneller verschleifen und früher ausfallen.

### 2.2. Ungeeignete Einbindung der OT in die Sicherheitsorganisation

Durch unterschiedliche Rahmenbedingungen, Kenntnisse und Vorgehensweisen in den Bereichen Office-IT und OT können bei übergreifenden Sicherheitsvorgaben Probleme bei der Umsetzung

auftreten. Sicherheitsvorgaben aus dem Bereich der Office-IT können einerseits aufgrund technischer oder prozessualer Besonderheiten bei ICS-Systemen nicht umsetzbar sein. Andererseits könnte es sein, dass ICS-spezifische Informationssicherheits- und Safety-Aspekte, also Aspekte der funktionalen Sicherheit, den oder der Informationssicherheitsbeauftragten der Office-IT nicht bekannt sind. So können Reibungsverluste in der Kommunikation und der Umsetzung entstehen. Außerdem könnten Risiken nicht erkannt oder unzureichend behandelt werden.

### **2.3. Ungeeignete Einbindung der OT in betriebliche Abläufe**

Auch wenn sich OT und IT zunehmend annähern, gibt es Besonderheiten, die das Übertragen etablierter betrieblicher Abläufe erschweren. Betriebliche Eingriffe im Rahmen des Change- und Incident-Managements zur sicheren Konfiguration, Störungsbehebung oder zum Einspielen von Sicherheitsupdates können etwa eine erneute behördliche Freigabe oder den Verlust des Supports nach sich ziehen. Nicht autorisierte Änderungen können die Funktion einer Komponente beeinflussen und damit potenziell auch Auswirkungen auf deren Safety-Funktion haben.

Die OT dient der Überwachung, Steuerung und Automatisierung von technischen Abläufen. Störungen dieser Systeme können zu Produktionsausfällen, technischen oder personellen Schäden und Umweltschäden führen. Diese potenziellen Auswirkungen müssen bei betrieblichen Eingriffen berücksichtigt werden.

### **2.4. Unzureichender Zugangsschutz**

Industrielle Steuerungsanlagen werden immer seltener vollständig autark von der Außenwelt betrieben. Moderne Fertigungs- und Erzeugungsprozesse erfordern einen Informationsaustausch mit vor- und nachgelagerten Produktionsschritten und sind häufig an die zentralen Produktionsplanungs- und Steuerungssysteme einer Institution angebunden. Um elektronisch Informationen auszutauschen, müssen die Produktionsanlagen außerdem mit Drittnetzen, wie der Office-IT oder den Netzen von Partnern, Partnerinnen und Dienstleistenden, verbunden sein. Interaktive Zugriffe von Büro- oder Mobilarbeitsplätzen und der betrieblich bedingte elektronische Datenaustausch, etwa zur Bereitstellung von Software und Updates, bedeuten eine weitere Vernetzung mit der Außenwelt. Auch die Einrichtung von Fernzugängen für eine Rufbereitschaft oder für Dienstleistende können den Zugriff von außen ermöglichen.

Werden die erforderlichen Kommunikationskanäle zu weit gefasst oder unzureichend gesichert, können Dritte diese Zugangswege ausnutzen, um auf diese zuzugreifen und um diese zu kompromittieren. Industrielle Steuerungsanlagen können einerseits von zielgerichteten Schadsoftware-Angriffen betroffen sein. Andererseits können sie auch von Schadprogrammen kompromittiert werden, die eigentlich auf die Manipulation der Office-IT abzielen. Durch eine fehlende Segmentierung oder Kontrolle des Datenverkehrs kann Schadsoftware auf die Systeme gelangen.

Aber auch der Einsatz von Virenschutz-Software kann ein Risiko für die OT darstellen. Etwa dann, wenn keine Freigabe des herstellenden Unternehmens für die Umgebung vorliegt oder Fehlerkennungen und aktive Systemeingriffe den Betrieb gefährden. Ein vergleichbares Störungspotenzial kann sich auch aus dem Betrieb netzbasierter Intrusion Prevention Systeme (IPS) ergeben, weil dabei Verbindungen unterbrochen werden können.

### **2.5. Unsicherer Projektierungsprozess/Anwendungsentwicklungsprozess**

Anpassungen und Weiterentwicklungen von IT-Systemen, Anwendungen und Steuerungsprogrammen können einen kritischen Eingriff in die Steuerungsanlage darstellen. Störungen können dabei aus funktionalen Fehlern bei unzureichenden Test- und Validierungsschritten, fehlerhaften oder manipulierten Projektierungsdaten oder Schwachstellen in

der Software entstehen. Etwa dann, wenn wichtige Sicherheitsfunktionen wie Ein- und Ausgabe- oder Berechtigungsprüfungen unzureichend umgesetzt werden.

Weitere Gefahren können sich aus unsicheren Entwicklungsumgebungen, der ungeeigneten Ablage von Programmcode, Dokumentations- oder Projektdaten sowie aus den Datentransferschnittstellen ergeben.

## **2.6. Unsicheres Administrationskonzept und Fernadministration**

Die Administration industrieller Steuerungssysteme erfolgt in bestimmten Fällen über Netzzugriffe. Dabei werden unterschiedliche öffentliche und private Netze wie z. B. Telefonnetze, Funknetze, Mobilfunknetze und zunehmend das Internet genutzt. Sind diese Zugänge unzureichend geplant, unsicher konfiguriert oder werden diese nicht überwacht, können Dritte unter Umständen unbefugt auf einzelne OT-Komponenten oder die Infrastruktur zugreifen. So können sie etwa die Sicherheitsmechanismen am Perimeter umgehen.

## **2.7. Unzureichende Überwachungs- und Detektionsverfahren**

Eine wesentliche Funktion industrieller Steuerungssysteme ist es, den Betrieb eines automatisierten Prozesses zu überwachen. So wird etwa bei unterschrittenen Füllständen oder abweichenden Temperaturen oder Ventilstellungen eine entsprechende Warnung ausgegeben. Die unterstützende IT-Infrastruktur wird dagegen häufig nicht ausreichend überwacht.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse solcher Betriebsumgebungen nicht oder nur unzureichend kontrolliert, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden. Darüber hinaus kann auch eine mangelhafte Auswertung oder eine unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

## **2.8. Unzureichendes Testkonzept**

Industrielle Steuerungsanlagen unterliegen oft hohen Verfügbarkeitsanforderungen. Denn Störungen oder technische Ausfälle können unter Umständen schwerwiegende Schäden und hohe Folgekosten nach sich ziehen. Aus diesem Grund sind OT-Systeme oft ausfallsicher konzipiert.

Werden Änderungen an einer solchen Umgebung nicht sorgfältig geplant, abgestimmt und in einer realitätsnahen Umgebung getestet, besteht die Gefahr, dass logische oder softwaretechnische Fehler übersehen werden und Störungen in der Anlage auftreten. Selbst vom herstellenden Unternehmen freigegebene Updates können bei der Modifikation oder Anpassung von Parametern Störungen an der Anlage verursachen.

## **2.9. Mangelnde Life-Cycle-Konzepte**

Neben spezifischen ICS-Komponenten werden zunehmend Komponenten und Software aus der Office-IT eingesetzt. Aufgrund der sehr langen Lebenszyklen in der OT werden diese Komponenten in der Regel deutlich länger betrieben als in der Office-IT üblich, teilweise auch über die Support-Zyklen der herstellenden Unternehmen hinaus.

Dies hat zur Folge, dass nach dem Ablauf der Unterstützung der herstellenden Unternehmen keine Updates gegen Schwachstellen mehr zur Verfügung gestellt werden. Dem gegenüber stehen oftmals öffentlich dokumentierte Schwachstellen sowie Werkzeuge, die diese Schwachstellen ausnutzen. Dies ermöglicht auch nicht versierten Angreifenden ein erfolgreiches Eindringen in die OT-Systeme. Das gilt auch, wenn Updates nicht oder nur mit sehr großer Verzögerung eingespielt werden.

Die langen Einsatzzeiten können zudem zu Problemen bei der Beschaffung von Ersatzteilen führen, etwa wenn diese nicht mehr produziert werden. Dies gilt auch für mögliches Know-how zur Pflege und Wartung von Alt-Systemen, über das neue Mitarbeitende nicht mehr verfügen.

Zudem enthalten ICS-Komponenten häufig detaillierte Informationen über den geregelten oder überwachten Prozess. Auch aus sonstigen übertragenen Werten, wie Mess- oder Steuerungsdaten, lassen sich diese Informationen teilweise rekonstruieren. Gleiches gilt für Steuerungsprogramme oder -parameter. Angreifende könnten so an Geschäftsgeheimnisse gelangen.

## **2.10. Unzureichende Sicherheitsanforderungen bei der Beschaffung**

Aufgrund nicht ausreichender Sicherheitsanforderungen und aus Kostengründen wird bei der Beschaffung häufig die Informationssicherheit nicht berücksichtigt. Dadurch können in ICS-Komponenten mitunter schwerwiegende Schwachstellen, z. B. in Hardware oder Software enthalten sein, die sich später nur sehr aufwändig beheben lassen.

## **2.11. Einsatz unsicherer Protokolle**

Die ICS-Komponenten kommunizieren untereinander über verschiedene Netzprotokolle und Standards. Neben Protokollen und Standards aus der Office-IT wie Ethernet, TCP/IP, WLAN oder GSM werden OT-spezifische Protokolle eingesetzt. Diese sind nicht immer unter dem Gesichtspunkt der Informationssicherheit entwickelt worden und bieten demgemäß teilweise keine oder nur eingeschränkte Sicherheitsmechanismen. Informationen werden häufig im Klartext und ohne Integritätssicherung oder Authentisierung übertragen.

Angreifende mit Zugang zum Netz könnte die Inhalte der Kommunikation auslesen oder verändern und auf diese Weise die Prozesse beeinflussen, etwa indem Sensordaten vorgetäuscht oder Steuerungsbefehle gefälscht werden. Dies trifft in besonderem Maße auf Protokolle zu, die für die Kommunikation über frei zugängliche Gebiete eingesetzt werden, etwa bei Funkprotokollen oder im Rahmen der Standortvernetzung.

## **2.12. Unsichere Konfigurationen von ICS-Komponenten**

In der Standardkonfiguration von ICS-Komponenten werden Sicherheitsmaßnahmen nicht immer aktiviert. Dadurch können Unbefugte leicht Zugriff erlangen. Der Betrieb unsicher konfigurierter Komponenten kann darüber hinaus auch die Sicherheit anderer Komponenten der Umgebung bedrohen, etwa wenn Zugangsdaten zu diesen ausgelesen werden können oder sie in einer Vertrauensstellung zu anderen Systemen stehen.

Beispielsweise könnten Standardpasswörter gebraucht, Klartextprotokolle zur Systemverwaltung genutzt, nicht erforderliche Dienste betrieben, ungesicherte Schnittstellen wie z. B. USB- oder Firewire-Ports verwendet oder Sicherheitsfunktionen deaktiviert werden.

## **2.13. Abhängigkeiten der OT von IT-Netzen**

Die OT wird mittlerweile immer weniger völlig autark betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, wirken sich Ausfälle oder Sicherheitsvorfälle im IT-Netz auch auf die OT aus.

Insbesondere wenn diese Systeme und Netze nicht unter der direkten Kontrolle des Betreibenden stehen, kann die Verfügbarkeit der OT und seiner Prozesse stark beeinträchtigt werden. Darüber hinaus kann ein Vorfall oder Fehler in der Regel nur mit externer Unterstützung behoben werden.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen, gemeinsam genutzte Infrastrukturkomponenten, eine Betriebsführung und Überwachung durch Dienstleistende oder die Nutzung von Cloud-Diensten.

### 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* 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, IT-Betrieb, 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.1.A1 Einbindung in die Sicherheitsorganisation (B)**

Ein Managementsystem für Informationssicherheit (ISMS) für den Betrieb der OT-Infrastruktur **MUSS** entweder als selbständiges ISMS oder als Teil eines Gesamt-ISMS existieren.

Eine gesamtverantwortliche Person für die Informationssicherheit im OT-Bereich **MUSS** benannt werden. Er oder sie **MUSS** innerhalb der Institution bekannt gegeben werden.

##### **IND.1.A2 ENTFALLEN (B)**

Diese Anforderung ist entfallen.

##### **IND.1.A3 Schutz vor Schadprogrammen (B)**

Beim Einsatz von Virenschutz-Software auf OT-Komponenten **MUSS** berücksichtigt werden, ob und in welcher Konfiguration der Betrieb von Virenschutz-Software vom herstellenden Unternehmen unterstützt wird. Ist dies nicht der Fall, **MUSS** der Bedarf an alternativen Schutzverfahren geprüft werden.

Die Virensignaturen **DÜRFEN NICHT** von OT-Systemen direkt aus dem Internet bezogen werden.

##### **IND.1.A18 Protokollierung (B) [OT-Betrieb (Operational Technology, OT)]**

Jede Änderung an ICS-Komponenten **MUSS** protokolliert werden. Außerdem **MÜSSEN** alle Zugriffe auf ICS-Komponenten protokolliert werden.

##### **IND.1.A19 Erstellung von Datensicherungen (B) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]**

Programme und Daten **MÜSSEN** regelmäßig gesichert werden. Auch nach jeder Systemänderung an OT-Komponenten **MUSS** eine Sicherung erstellt werden.

## 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.1.A4 Dokumentation der OT-Infrastruktur (S)

Alle sicherheitsrelevanten Parameter der OT-Infrastruktur SOLLTEN dokumentiert sein. In einem Bestandsverzeichnis SOLLTEN alle Software- und Systemkomponenten geführt werden. Hieraus SOLLTEN die eingesetzten Produkt- und Protokollversionen sowie die Zuständigkeiten hervorgehen. Zu den eingesetzten Komponenten SOLLTEN eventuelle Restriktionen der herstellenden Unternehmen oder regulatorische Auflagen bestimmt sein. Diese Dokumentation und ein Systeminventar SOLLTEN beispielsweise in einem Leitsystem geführt werden.

Zusätzlich SOLLTE ein aktueller Netzplan Zonen, Zonenübergänge (Conduits), eingesetzte Kommunikationsprotokolle und -verfahren sowie Außenschnittstellen dokumentieren. Bei den Schnittstellen SOLLTEN aktive Netzkomponenten und manuelle Datentransferverfahren, z. B. durch Wechseldatenträger, berücksichtigt werden. Zonen und Conduits schützen die OT-Infrastruktur, indem die Automatisierungslösung in Zellen und Kommunikationskanälen strukturiert werden SOLLTE.

### IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts (S) [Planende]

Die OT-Infrastruktur SOLLTE auch horizontal in unabhängige Funktionsbereiche, wie etwa Anlagen, segmentiert werden. Die einzelnen Zonen SOLLTEN, so weit wie möglich, im Betrieb voneinander unabhängig sein. Insbesondere die Zonen, in denen der technische Prozess gesteuert wird, SOLLTEN bei einem Ausfall der anderen Zonen für einen gewissen Zeitraum weiter funktionstüchtig sein. Auch SOLLTE die Abkopplung nach einem Angriff weiter funktionieren. Dieser Zeitraum SOLLTE geeignet definiert und dokumentiert werden. Das Netz SOLLTE manipulations- und fehlerresistent konzipiert werden.

### IND.1.A6 Änderungsmanagement im OT-Betrieb (S)

Für Änderungen an der OT SOLLTE ein eigener Änderungsprozess definiert, dokumentiert und gelebt werden.

### IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT (S)

Die Institution SOLLTE einen Prozess zur Verwaltung von Zugängen und zugeordneten Berechtigungen für den Zugriff auf die OT etablieren. Die Berechtigungsverwaltung SOLLTE den Prozess, die Durchführung und die Dokumentation für die Beantragung, Einrichtung und den Entzug von Berechtigungen umfassen.

Die Berechtigungsverwaltung SOLLTE gewährleisten, dass Berechtigungen nach dem Minimalprinzip vergeben und regelmäßig überprüft werden. In der Berechtigungsverwaltung SOLLTEN die Zugriffe auf IT-Systeme für Mitarbeitende, Administrierende und Dritte geregelt sein. Jeder oder jede Beteiligte SOLLTE regelmäßig zu den einzuhaltenden Regelungen sensibilisiert werden. Die Einhaltung SOLLTE überprüft werden. Fehlverhalten SOLLTE sanktioniert werden.

### IND.1.A8 Sichere Administration (S) [IT-Betrieb]

Für die Erstkonfiguration, Verwaltung und Fernwartung in der OT SOLLTEN entweder sichere Protokolle oder abgetrennte Administrationsnetze mit entsprechendem Schutzbedarf genutzt werden. Der Zugang zu diesen Schnittstellen SOLLTE auf die Berechtigten eingeschränkt sein. Es SOLLTE nur der Zugriff auf die Systeme und Funktionen gewährt sein, die für die jeweilige Administrationsaufgabe benötigt werden.

Die Systeme und Kommunikationskanäle, mit denen die Administration oder Fernwartung durchgeführt wird, SOLLTEN das gleiche Schutzniveau aufweisen wie die verwaltete OT-Komponente.

### **IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen (S)**

Für die Nutzung von Wechseldatenträgern und mobilen Endgeräten SOLLTEN Regelungen aufgestellt und bekannt gegeben werden. Der Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen SOLLTE beschränkt werden. Für Medien und Geräte von Dienstleistenden SOLLTEN ein Genehmigungsprozess und eine Anforderungsliste existieren. Die Vorgaben SOLLTEN allen Dienstleistenden bekannt sein und von diesen schriftlich bestätigt werden.

Auf den OT-Komponenten SOLLTEN alle nicht benötigten Schnittstellen deaktiviert werden. An den aktiven Schnittstellen SOLLTE die Nutzung auf bestimmte Geräte oder Medien eingeschränkt werden.

### **IND.1.A10 Monitoring, Protokollierung und Detektion (S) [OT-Betrieb (Operational Technology, OT)]**

Betriebs- und sicherheitsrelevante Ereignisse SOLLTEN zeitnah identifiziert werden. Hierzu SOLLTE ein geeignetes Log- und Event-Management entwickelt und umgesetzt werden. Das Log- und Event-Management SOLLTE angemessene Maßnahmen umfassen, um sicherheitsrelevante Ereignisse zu erkennen und zu erheben. Es SOLLTE zudem einen Reaktionsplan (Security Incident Response) enthalten.

Der Reaktionsplan SOLLTE Verfahren zur Behandlung von Sicherheitsvorfällen festlegen. Darin abgedeckt sein SOLLTEN die Klassifizierung von Ereignissen, Meldewege und Festlegung der einzubeziehenden Organisationseinheiten, Reaktionspläne zur Schadensbegrenzung, Analyse und Wiederherstellung von Systemen und Diensten sowie die Dokumentation und Nachbereitung von Vorfällen.

### **IND.1.A11 Sichere Beschaffung und Systementwicklung (S)**

Sollen OT-Systeme beschafft, geplant oder entwickelt werden, SOLLTEN Regelungen zur Informationssicherheit getroffen und dokumentiert werden. Die Unterlagen SOLLTEN Teil der Ausschreibung sein.

Bei Beschaffungen, Planungen oder Entwicklungen SOLLTE die Informationssicherheit in dem gesamten Lebenszyklus berücksichtigt werden. Voraussetzungen und Umsetzungshinweise für einen sicheren Betrieb von ICS-Komponenten von den herstellenden Unternehmen SOLLTEN frühzeitig eingeplant und umgesetzt werden. Für ICS-Komponenten SOLLTEN einheitliche und dem Schutzbedarf angemessene Anforderungen an die Informationssicherheit definiert werden. Diese SOLLTEN berücksichtigt werden, wenn neue ICS-Komponenten beschafft werden. Die Einhaltung und Umsetzung SOLLTE dokumentiert werden.

Die Institution SOLLTE dokumentieren, wie sich das System in die Konzepte für die Zoneneinteilung, das Berechtigungs- und Schwachstellen-Management sowie für den Virenschutz einfügt und diese gegebenenfalls anpassen. Es SOLLTE geregelt sein, wie der Betrieb aufrechterhalten werden kann, falls einer der Kooperationspartner keine Dienstleistungen mehr anbietet.

### **IND.1.A12 Etablieren eines Schwachstellen-Managements (S)**

Für den sicheren Betrieb einer OT-Umgebung SOLLTE die Institution ein Schwachstellen-Management etablieren. Das Schwachstellen-Management SOLLTE Lücken in Software, Komponenten, Protokollen und Außenschnittstellen der Umgebung identifizieren. Außerdem SOLLTEN sich daraus erforderliche Handlungen ableiten, bewerten und umsetzen lassen.

Grundlage dafür SOLLTEN Schwachstellenmeldungen von herstellenden Unternehmen oder öffentlich verfügbare CERT-Meldungen sein. Ergänzend hierzu SOLLTEN organisatorische und technische Audits zur Schwachstellenanalyse durchgeführt werden.

### **IND.1.A20 Systemdokumentation (S) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]**

Es SOLLTE eine erweiterte Systemdokumentation erstellt werden. Darin SOLLTEN Besonderheiten im Betrieb und die Möglichkeiten zur Systemverwaltung festgehalten werden. Außerdem SOLLTE dokumentiert werden, wenn ICS-Komponenten verändert werden.

### **IND.1.A21 Dokumentation der Kommunikationsbeziehungen (S) [OT-Betrieb (Operational Technology, OT)]**

Es SOLLTE dokumentiert werden, mit welchen Systemen eine ICS-Komponente welche Daten austauscht. Außerdem SOLLTEN die Kommunikationsverbindungen neu integrierter ICS-Komponenten dokumentiert werden.

### **IND.1.A22 Zentrale Systemprotokollierung und -überwachung (S) [OT-Betrieb (Operational Technology, OT)]**

Die Protokollierungsdaten von ICS-Komponenten SOLLTEN zentral gespeichert werden. Bei sicherheitskritischen Ereignissen SOLLTE automatisch alarmiert werden.

### **IND.1.A23 Aussonderung von ICS-Komponenten (S) [OT-Betrieb (Operational Technology, OT)]**

Wenn alte oder defekte ICS-Komponenten ausgesondert werden, SOLLTEN alle schützenswerten Daten sicher gelöscht werden. Es SOLLTE insbesondere sichergestellt sein, dass alle Zugangsdaten nachhaltig entfernt wurden.

## **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.1.A13 Notfallplanung für OT (H)**

Notfallpläne für den Ausfall und für die Kompromittierung jeder Zone SOLLTEN definiert, dokumentiert, nach jeder größeren Änderung getestet und regelmäßig geübt sein.

Zudem SOLLTE ein wirksames Ersatzverfahren für den Ausfall der (Fern-) Administrationsmöglichkeit definiert, dokumentiert und getestet sein.

### **IND.1.A14 Starke Authentisierung an OT-Komponenten (H)**

Zur sicheren Authentisierung von privilegierten Benutzenden in Steuerungssystemen SOLLTE ein zentraler Verzeichnisdienst eingerichtet werden (siehe Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). Die Authentisierung SOLLTE durch den Einsatz mehrerer Faktoren wie Wissen, Besitz oder Biometrie zusätzlich abgesichert werden.

Bei der Planung SOLLTE darauf geachtet werden, dass daraus entstehende Abhängigkeiten in der Authentisierung bekannt sind und bei der Umsetzung der Lösung berücksichtigt werden.

Es SOLLTE sichergestellt werden, dass die Authentisierung von betrieblich erforderlichen technischen Konten auch in Notfällen durchgeführt werden kann.

### **IND.1.A15 Überwachung von weitreichenden Berechtigungen (H)**

Die Institution SOLLTE ein Bestandsverzeichnis führen, das alle vergebenen Zutritts-, Zugangs und Zugriffsrechte auf kritische Systeme enthält. Das Verzeichnis SOLLTE beinhalten, welche Rechte ein

bestimmter Benutzer oder eine bestimmte Benutzende effektiv hat und wer an einem bestimmten System über welche Rechte verfügt.

Alle kritischen administrativen Tätigkeiten SOLLTEN protokolliert werden. Der IT-Betrieb SOLLTE NICHT die Protokolle löschen oder manipulieren können.

### **IND.1.A16 Stärkere Abschottung der Zonen (H)**

Bei hoch schutzbedürftigen oder schlecht absicherbaren ICS-Umgebungen SOLLTEN vorbeugend Schnittstellensysteme mit Sicherheitsprüffunktionen eingesetzt werden.

Durch Realisierung einer oder mehrerer Anbindungszonen (DMZ) in P-A-P-Struktur SOLLTEN durchgängige Außenverbindungen terminiert werden. Erforderliche Sicherheitsprüfungen SOLLTEN so erfolgen, dass die ICS-Anlage nicht angepasst werden muss.

### **IND.1.A17 Regelmäßige Sicherheitsüberprüfung (H)**

Die Sicherheitskonfiguration von OT-Komponenten SOLLTE regelmäßig und bedarfsorientiert bei plötzlich auftretenden neuen, bisher unbekanntem Gefährdungen überprüft werden. Die Sicherheitsüberprüfung SOLLTE zumindest die exponierten Systeme mit Außenschnittstellen oder Benutzendeninteraktion umfassen. Auch das realisierte Sicherheitskonzept SOLLTE regelmäßig überprüft werden. Die Sicherheitsüberprüfung SOLLTE als Konfigurationsprüfung oder auch durch automatisierte Konformitätsprüfungen erfolgen.

### **IND.1.A24 Kommunikation im Störfall (H) [Mitarbeitende, OT-Betrieb (Operational Technology, OT)]**

Alternative und unabhängige Kommunikationsmöglichkeiten SOLLTEN aufgebaut und betrieben werden.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

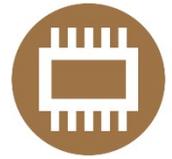
Das BSI hat mit dem Dokument „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld“ entsprechende Hilfestellungen zur Absicherung im ICS-Umfeld veröffentlicht.

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.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27019 „Information technology - Security techniques - Information security controls for the energy utility industry Vorgaben für die Absicherung von Energieversorgern“.

Der Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW) und Oesterreichs E-Wirtschaft bietet mit dem Dokument „Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ eine Hilfestellung zum sicheren Betrieb von Steuerungs- und Telekommunikationssystemen.

Die internationale Norm IEC 62443-2-1:2010 „Industrial communication networks - Network and system security: Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC)“, 2010, legt fest, was zur Einrichtung von IT-Sicherheit in Netzen und Systemen notwendig ist.



# 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.

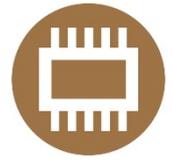
## 4. Weiterführende Informationen

### 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.



# IND.2.2

## Speicherprogrammierbare Steuerung (SPS)

### 1. Beschreibung

#### 1.1. Einleitung

Eine Speicherprogrammierbare Steuerung (SPS, englisch Programmable Logic Controller, PLC) ist eine ICS-Komponente. Sie übernimmt Steuerungs- und Regelaufgaben in der Betriebstechnik (englisch Operational Technology, OT). Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind fließend, so kann z. B. auch ein Fernwirkgerät (englisch Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen oder ein Programmable Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs zu vereinen. Jedoch ist die SPS immer noch das klassische Automatisierungsgerät, sodass in diesem Baustein die Begriffe SPS, RTU und PAC synonym verwendet werden.

Eine SPS verfügt über digitale Ein- und Ausgänge, ein Echtzeitbetriebssystem (Firmware) sowie weitere Schnittstellen für Ethernet oder Feldbusse. Die Verbindung zu Sensoren und Aktoren erfolgt über die analogen oder digitalen Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit Prozessleitsystemen erfolgt meist über die Ethernet-Schnittstelle und IP-basierte Netze.

Die möglichen Realisierungen sind vielfältig, eine Speicherprogrammierbare Steuerung kann als Baugruppe, Einzelgerät, PC-Einsteckkarte (Slot-SPS) oder als Software-Emulation (Soft-SPS) eingesetzt werden. Am häufigsten anzutreffen sind modulare Speicherprogrammierbare Steuerungen, die aus verschiedenen funktionalen Steckmodulen zusammengesetzt werden. Zunehmend werden auch weitere Funktionen wie das Visualisieren, Alarmieren und Protokollieren durch die SPS übernommen.

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.

Eine SPS wird 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 Daten über ein Netz verteilt.

## 1.2. Zielsetzung

Ziel dieses Bausteins ist es, alle Arten von Speicherprogrammierbaren Steuerungen abzusichern, unabhängig von herstellenden Unternehmen, Bauart, Einsatzzweck und -ort.

## 1.3. Abgrenzung und Modellierung

Der Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* ist auf jede SPS-Komponente einmal anzuwenden.

Der vorliegende Baustein ist anzuwenden, um alle Arten von Speicherprogrammierbaren Steuerungen und Geräten mit ähnlicher Funktion abzusichern. Er ergänzt den Baustein IND.2.1 *Allgemeine ICS-Komponente*. Dieser ist bei der Anwendung ebenfalls zu berücksichtigen.

Der Baustein enthält keine organisatorischen Anforderungen zur Absicherung einer ICS-Komponente. Dafür müssen die Anforderungen des Bausteins IND.1 *Prozessleit- und Automatisierungstechnik* umgesetzt werden. Ebenso wird der Bereich funktionale Sicherheit nicht behandelt. Hierfür ist der Baustein IND.2.7 *Safety Instrumented Systems* anzuwenden.

## 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.2.2 *Speicherprogrammierbare Steuerung (SPS)* von besonderer Bedeutung.

### 2.1. Unvollständige Dokumentation

Speicherprogrammierbare Steuerungen sind oft unvollständig dokumentiert, sodass nicht alle Produktfunktionen bekannt sind. Besonders lückenhaft sind häufig die Angaben über die verwendeten Dienste, Protokolle und Kommunikationsports sowie zur Berechtigungsverwaltung. Das erschwert jedoch die Gefährdungsanalyse, denn dadurch werden Schnittstellen, Funktionen sowie sicherheitsrelevante Mechanismen übersehen. Potenzielle Gefährdungen können dann nicht berücksichtigt werden. Zudem kann nicht oder nur eingeschränkt auf neue Schwachstellen reagiert werden, wenn diese nicht erfasst sind.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* 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	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**

Für diesen Baustein sind keine Basis-Anforderungen definiert.

### **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.2.2.A1 Erweiterte Systemdokumentation für Speicherprogrammierbare Steuerungen (S) [OT-Betrieb (Operational Technology, OT)]**

Steuerungsprogramme und Konfigurationen SOLLTEN immer gesichert werden, bevor an ihnen etwas verändert wird. Änderungen an der Konfiguration oder der Tausch von Komponenten SOLLTEN vollständig dokumentiert werden.

#### **IND.2.2.A2 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

#### **IND.2.2.A3 Zeitsynchronisation (S) [OT-Betrieb (Operational Technology, OT)]**

Die Systemzeit SOLLTE automatisch über eine zentrale automatisierte Zeitsynchronisation eingestellt werden.

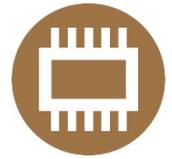
### **3.3. Anforderungen bei erhöhtem Schutzbedarf**

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Zum Baustein IND.2.2 *Speicherprogrammierbare Steuerung (SPS)* liegen keine weiteren Informationen vor.



# 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.

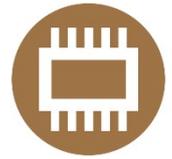
### IND.2.3.A3 Drahtlose Kommunikation (H)

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.



# 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 oder die Betreibende 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 die Betreibenden die Parameter verändern können, 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 herstellenden Unternehmen, 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 Automatisierungstechnik* 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

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.2.4 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. Mitarbeitende gefährdet werden oder die Produktion könnte erheblich beeinträchtigt werden.

### 2.2. Gezielte Manipulationen

Sind die Schnittstellen einer Maschine ungenügend geschützt, kann die Maschine manipuliert werden, z. B. über lokale Programmiergeräte oder Netzdienste. Dadurch können Werkstücke beschädigt werden oder ganze Produktreihen fehlerhaft sein. Bei einem Angriff könnte aber auch die Maschine selbst beschädigt werden, sodass auch dadurch ein wirtschaftlicher Verlust entsteht.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins *IND.2.4 Maschine* 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	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.2.4.A1 Fernwartung durch Maschinen- und Anlagenbauende (B) [OT-Betrieb (Operational Technology, OT)]**

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 Dienstleistenden MUSS vereinbart werden, wie sie die in der Maschine gespeicherten Informationen verwerten dürfen.

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

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

### **3.2. Standard-Anforderungen**

Für diesen Baustein sind keine Standard-Anforderungen definiert.

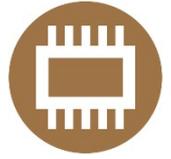
### **3.3. Anforderungen bei erhöhtem Schutzbedarf**

Für diesen Baustein 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.



# IND.2.7 Safety Instrumented Systems

## 1. Beschreibung

### 1.1. Einleitung

Safety Instrumented Systems (SIS) bilden eine Untergruppe der Industrial Control Systems (ICS). SIS werden eingesetzt, um Gefahren für technische Anlagen, die Umwelt und Personen abzuwehren. Der prinzipielle Aufbau von SIS unterscheidet sich kaum von den konventionellen Automatisierungssystemen. Der wesentliche Unterschied liegt in den erhöhten Anforderungen an die Zuverlässigkeit, mit der die von einem SIS auszuführenden Sicherheitsfunktionen (SIF) vollzogen werden. Das Maß an Zuverlässigkeit wird mit Hilfe des vierstufigen Sicherheits-Integritätslevels (SIL) ausgedrückt, diese werden in der IEC 61508 definiert. SIL1 ist hierbei die geringste und SIL4 die höchste Anforderung an die Zuverlässigkeit. Abhängig von der SIL-Stufe gelten unterschiedliche Anforderungen an die zulässige Ausfallrate von Komponenten, die Hardware-Fehlertoleranz der Architektur, die Unabhängigkeit von Prüfenden sowie weitere sicherheitsrelevante Punkte. Der gesamte Lebenszyklus eines SIS ist organisatorisch in ein Functional Safety Management (FSM) eingebettet.

Dieser Baustein ist unabhängig von der jeweiligen SIL-Stufe eines SIS umzusetzen. Die Informationssicherheit ist in jeder Lebensphase zu berücksichtigen, von der Entwicklung der Komponenten bis hin zu deren Anwendung, Betrieb und Außerbetriebnahme. Dabei ist zu beachten, dass die Sicherstellung der Integrität der SIS die höchste Priorität hat.

Ein weiteres wesentliches Merkmal von SIS ist die Unabhängigkeit und die Trennung von umgebenden IT-Systemen und von der Betriebstechnik (Operational Technology, OT). Das bedeutet, dass die Verfügbarkeit und Integrität des SIS nicht von ihnen beeinflusst werden dürfen.

### 1.2. Zielsetzung

Das Ziel dieses Bausteins besteht darin, geeignete Anforderungen an SIS zu formulieren, die beim Aufbau eines Managementsystems für Informationssicherheit (ISMS) erfüllt werden müssen.

Der Begriff „SIS“ umfasst im Sinne dieses Bausteins die Komponenten Sensor, Aktor, die sicherheitsgerichtete speicherprogrammierbare Steuerung (SSPS), auch als Logiksystem bezeichnet, das Anwendungsprogramm sowie auch insbesondere die dazugehörigen Programmiergeräte (Engineering Station, Handhelds für die Sensor-/Aktor-Konfiguration) und Visualisierungseinrichtungen.

## 1.3. Abgrenzung und Modellierung

Der Baustein IND.2.7 *Safety Instrumented Systems* ist auf jede SIS-Komponente einmal anzuwenden.

Der vorliegende Baustein ergänzt die übergeordneten Bausteine IND.1 *Prozessleit- und Automatisierungstechnik* und IND.2.1 *Allgemeine ICS-Komponente* und setzt voraus, dass diese umgesetzt wurden.

## 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.2.7 *Safety Instrumented Systems* von besonderer Bedeutung.

### 2.1. Manipulation des Logiksystems

Die Manipulation des Anwendungsprogramms auf dem Logiksystem, bei der die Integrität eines SIS verletzt werden kann, stellt das größte Risiko dar. Anders als bei „einfachen“ OT-Komponenten, kann dies potenziell schwerste Auswirkungen auf die Sicherheit von Menschen, Umwelt und technischen Anlagen haben. Im Arbeitsblatt NA 163 des internationalen Verbands der Anwender von Automatisierungstechnik der Prozessindustrie NAMUR sind diesbezüglich folgende drei Kategorien zur Risikobeurteilung definiert:

- Unter Kategorie 1 werden Manipulationen zusammengefasst, welche die Sicherheitsfunktion (SIF) auslösen, ohne dass der Anforderungsfall eingetreten ist. Die Auswirkungen sind im Sinne der funktionalen Sicherheit nicht gefährlich, da das SIS den sicheren Zustand herbeigerufen hat. Die Manipulationen führen allerdings zu einer Betriebsunterbrechung. Ursache dafür können beispielsweise Schadsoftware oder menschliche Fehlhandlungen sein.
- Kategorie 2 beschreibt einen Fall, bei dem die Sicherheitsfunktion deaktiviert ist und dadurch kein Schutz mehr geboten ist. Ein inakzeptables Ergebnis wird erst erreicht, wenn der Anforderungsfall eingetreten ist. Die Auswirkungen werden als gefährlich eingestuft, da das SIS seine primäre Aufgabe nicht erfüllen kann. Angriffsszenarien werden als komplex eingestuft, da die Manipulation des Logiksystems allein nicht ausreicht, um einen Schaden zu verursachen.
- Die dritte Kategorie behandelt das gravierendste Szenario, indem eine oder mehrere Sicherheitsfunktionen deaktiviert werden und der Anforderungsfall vorsätzlich herbeigeführt wird. Auch hier werden die Auswirkungen als gefährlich und die Angriffsszenarien als sehr komplex eingestuft. Denn um den Anforderungsfall herbeiführen zu können, müssen Angreifende neben Kenntnissen über die Manipulation des SIS auch über fundierte Kenntnisse zu den physikalischen Prozessen verfügen.

Im Dezember 2017 wurde erstmals über eine Schadsoftware berichtet, die gezielt SIS manipuliert hat. Der Weg des Angriffs führte über die Engineering Station, auf der sich die spezielle Software für die Programmierung und Parametrierung befand. Die dort installierte Malware suchte von dort aus gezielt nach verbundenen Logiksystemen eines bestimmten herstellenden Unternehmens und lud darauf ausführbaren Code, der das Anwendungsprogramm (die Logik) manipulierte. Aufgrund eines Fehlers in diesem Code schlug die Gültigkeitsüberprüfung fehl. Daraufhin löste die Sicherheitsfunktion aus und fuhr die angegriffene Anlage in einen sicheren Zustand herunter. Der Angriff war zwar nicht erfolgreich, hätte aber sowohl aufgrund seiner Auswirkung als auch seiner Komplexität der Kategorie 2 oder 3 zugeordnet werden können.

## 2.2. Unzureichende Überwachungs- und Detektionsverfahren

Eine wesentliche Funktion von Automatisierungssystemen liegt darin, Betriebszustände des zu automatisierenden Prozesses zu überwachen. So werden für gewöhnlich den Prozess betreffende Warnungen (z. B. bei überschrittenen Füllständen) und technische Parameter (z. B. Temperatur, Ventilstellung) berücksichtigt. Im Gegensatz dazu wird die unterstützende IT-Infrastruktur oft nicht überwacht.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse nicht oder nur unzureichend überwacht, können Angriffsversuche, Netzengpässe oder absehbare Ausfälle nicht frühzeitig erkannt werden.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.2.7 *Safety Instrumented Systems* 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	OT-Leitung
Weitere Zuständigkeiten	Planende, ICS-Informationssicherheitsbeauftragte, Wartungspersonal

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.2.7.A1 Erfassung und Dokumentation (B) [Planende, Wartungspersonal]**

Alle zum SIS gehörenden Hardware- und Softwarekomponenten, relevante Informationen, Verbindungen sowie Rollen und Zuständigkeiten MÜSSEN gesondert erfasst und dokumentiert werden.

#### **IND.2.7.A2 Zweckgebundene Nutzung der Hard- und Softwarekomponenten (B) [Wartungspersonal]**

Die Hard- und Softwarekomponenten, die zum SIS gehören oder im Zusammenhang mit diesem genutzt werden, DÜRFEN NICHT zweckentfremdet werden.

#### **IND.2.7.A3 Änderung des Anwendungsprogramms auf dem Logiksystem (B) [Wartungspersonal]**

Bereits vorhandene Schutzmechanismen am Logiksystem MÜSSEN aktiviert sein. Wenn dies nicht möglich ist, MÜSSEN alternative Maßnahmen ergriffen werden. Anwendungsprogramme auf den Logiksystemen DÜRFEN NUR von autorisierten Personen geändert oder zur Übertragung freigegeben werden.

## 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.2.7.A4 Verankerung von Informationssicherheit im Functional Safety Management (S) [ICS-Informationssicherheitsbeauftragte]**

Alle Prozesse und Zuständigkeiten bezüglich der Informationssicherheit von SIS SOLLTEN klar definiert sein. Im Functional Safety Management SOLLTEN diese beschrieben und namentlich genannt sein.

### **IND.2.7.A5 Notfallmanagement von SIS (S) [ICS-Informationssicherheitsbeauftragte]**

Die Behandlung von Sicherheitsvorfällen SOLLTE in einem Vorfalldaktionsplan festgehalten werden. Dieser SOLLTE die Rollen und Zuständigkeiten festhalten und die zu ergreifenden Maßnahmen enthalten.

### **IND.2.7.A6 Sichere Planung und Spezifikation des SIS (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]**

Vorsehentliche oder unautorisierte Änderungen an der Spezifikation, Implementierung und an den Engineering-Daten SOLLTEN verhindert werden.

### **IND.2.7.A7 Trennung und Unabhängigkeit des SIS von der Umgebung (S) [Planende, Wartungspersonal]**

Das SIS SOLLTE rückwirkungsfrei von seiner Umgebung betrieben werden, um seine Sicherheitsfunktionen gewährleisten zu können. Prozesse, die potenziell Auswirkungen auf das SIS haben, SOLLTEN dem Änderungsmanagementprozess des Functional Safety Management unterstellt werden.

### **IND.2.7.A8 Sichere Übertragung von Engineering Daten auf SIS (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]**

Die Integrität der Engineering-Daten SOLLTE während der Übertragung auf SIS sichergestellt werden.

### **IND.2.7.A9 Absicherung der Daten- und Signalverbindungen (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]**

Sofern keine Rückwirkungsfreiheit von Daten- und Signalverbindungen (Unidirektionalität) nachgewiesen werden kann, SOLLTEN diese Verbindungen geeignet abgesichert werden.

### **IND.2.7.A10 Anzeige und Alarmierung von simulierten oder gebrückten Variablen (S) [Planende]**

Variablen der SIS, die durch Ersatzwerte besetzt (simuliert) oder von außen gebrückt werden, SOLLTEN in geeigneter Weise überwacht werden. Die Werte SOLLTEN den Benutzenden fortlaufend angezeigt werden. Grenzwerte SOLLTEN definiert werden. Wenn diese Grenzwerte erreicht werden, SOLLTEN die zuständigen Personen in geeigneter Weise alarmiert werden.

### **IND.2.7.A11 Umgang mit integrierten Systemen (S) [Planende, Wartungspersonal, ICS-Informationssicherheitsbeauftragte]**

Für integrierte Systeme SOLLTE eine passende Strategie entwickelt werden, die den Umgang mit Komponenten regelt, welche die funktionale Sicherheit (Safety) betreffen.

### 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.2.7.A12 Sicherstellen der Integrität und Authentizität von Anwendungsprogrammen und Konfigurationsdaten (H) [Planende]

Es SOLLTE darauf geachtet werden, dass die herstellenden Unternehmen geeignete Mechanismen entwickeln und integrieren, die die Integrität und Authentizität von Konfigurationsdaten und Anwendungsprogrammen auf dem Logiksystem oder auf den damit verbundenen Sensoren und Aktoren gewährleisten. Jegliche Software, die als Download angeboten wird, SOLLTE vor Manipulation geschützt werden. Verletzungen der Integrität SOLLTEN automatisch erkannt und gemeldet werden.

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

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27019 „Information technology - Security techniques - Information security controls for the energy utility industry“ Vorgaben für die Absicherung von Energieversorgern.

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.

Die internationalen Normen

- IEC 61508-1:2010 „Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements“, International Electrotechnical Commission (IEC)
- IEC 61511-1:2016 „Functional safety - Safety instrumented systems for the process industry sector“, International Electrotechnical Commission (IEC)
- IEC 62443-2-1:2010 „Industrial communication networks - Network and system security, Part 2-1: Establishing an industrial automation and control system security program“, International Electrotechnical Commission (IEC)
- IEC 62443-2-4:2015 „Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers“, International Electrotechnical Commission (IEC)
- IEC 62443-4-1: ENTWURF „Security for industrial automation and control systems - Technical security requirements for IACS components, Part 4-1: Secure product development life-cycle requirements“, International Electrotechnical Commission (IEC)
- IEC 62443-4-2: ENTWURF „Technical security requirements for IACS components, Part 4-2: Technical security requirements for IACS components“, International Electrotechnical Commission (IEC)

stellen weitere Hilfsmittel zur Einrichtung von IT-Sicherheit in Safety Instrumented Systems zur Verfügung.

Der Internationale Verband der Anwender von Automatisierungstechnik der Prozessindustrie Namur hat zur Risikobeurteilung das Dokument „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen“ veröffentlicht.

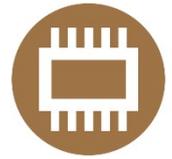
Im „Guide to Industrial Control Systems (ICS) Security“: NIST Special Publication 800-81 wird beschrieben, wie IT-Sicherheit im ICS-Umfeld eingeführt werden kann.

Zur Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) wurde die Richtlinie VDI/VDE 2180 veröffentlicht.

Die Richtlinie VDI/VDE 2182

- Blatt 2.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Betreiber - Presswerk“ sowie
- Blatt 3.3 „Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Prozessautomation für Betreiber - LDPE-Anlage“

bietet ein Vorgehensmodell und Anwendungsbeispiele für Informationssicherheit im ICS-Umfeld.



# IND.3.2 Fernwartung im industriellen Umfeld

## 1. Beschreibung

### 1.1. Einleitung

Die Betriebstechnik (OT) einer Institution besitzt häufig eine dezentrale Infrastruktur. Verschiedene Bereiche der OT können räumlich weit auseinanderliegen. Zudem bestehen Industrial-Control-Systeme (ICS) meist aus einer Vielzahl von Produkten verschiedener herstellenden Unternehmen, d. h. aus unterschiedlichen ICS-Komponenten und IT-Systemen für OT-Anwendungen. Daher benötigt die Betriebstechnik einer Institution in der Regel zahlreiche Fernwartungszugänge.

Diese Fernwartungszugänge sind häufig Einzellösungen in Form individuell zusammengestellter Hard- und Softwarekomponenten. Infolgedessen wird eine Vielzahl unterschiedlicher Techniken für die OT-Fernwartung eingesetzt. Die Lebenszyklen der Fernwartungslösungen entsprechen dabei meist denjenigen der Produkte, auf die zugegriffen wird, d. h. die Fernwartungslösungen für OT werden unter Umständen wesentlich länger eingesetzt als dies in der IT üblich ist. Verschiedenste Zugänge, Dienste und Schnittstellen sind parallel vorhanden. Die Schnittstellen kommunizieren mittels unterschiedlichster Protokolle.

Manche Anlagenteile in der OT werden auch als geschlossene Einheit von den herstellenden Unternehmen realisiert (sogenannte Package Units). Diese Anlagenteile enthalten häufig mehrere dezentrale Zugänge für die Fernwartung, die die herstellenden Unternehmen von vornherein für ihren eigenen Zugriff betriebsbereit integriert haben.

Fernwartungszugänge im industriellen Umfeld werden in der Regel vom OT-Betrieb und Wartungspersonal genutzt, um OT-Komponenten zu konfigurieren, zu kontrollieren, zu warten und zu reparieren. Nur in Ausnahmefällen, z. B. bei Störungen, nutzen auch weitere Mitarbeitende OT-Fernwartungszugänge.

Auf OT-Komponenten wird via Fernwartung von verschiedenen Institutionen aus zugegriffen. Nicht nur das interne Personal des Betreibenden, sondern auch externes Personal von herstellenden Unternehmen, Integratoren und Dienstleistenden nutzt Fernwartungszugänge.

Grundsätzlich erfolgt ein Fernwartungszugriff in dasjenige Sicherheitssegment eines OT-Netzes, in dem der Fernwartungsdienst bereitgestellt wird. Der Fernwartungsdienst kommuniziert dann aus diesem Segment heraus mit dem zu wartenden Zielsystem, z. B. mit einer ICS-Komponente.

## 1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit der Fernwartung im industriellen Umfeld zu gewährleisten.

## 1.3. Abgrenzung und Modellierung

Der Baustein IND.3.2 *Fernwartung im industriellen Umfeld* ist einmal auf die gesamte OT einer Institution anzuwenden, sobald diese Möglichkeiten zur Fernwartung enthält. Von den jeweiligen Einsatzgebieten der ICS ist abhängig, ob weitere Anforderungen an die Fernwartung im industriellen Umfeld definiert werden müssen, die in diesem Baustein nicht allgemeingültig aufgeführt werden können. Je nach Einsatzgebiet können auch die Maßnahmen unterschiedlich sein, die umgesetzt werden sollten, um die Anforderungen zu erfüllen.

Um ein IT-Grundschatz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- die spezifischen Aspekte der OT-Fernwartung, die über die allgemeine Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung hinausgehen sowie
- die spezifischen Aspekte der OT-Fernwartung, die von der allgemeinen Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung abweichen.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- die allgemeine Verwaltung von Netzkomponenten und IT-Systemen per Fernwartung durch den IT-Betrieb in der Büro- und Gebäude-IT (siehe OPS.1.2.5 *Fernwartung*) (Die diesbezüglichen Anforderungen sind grundsätzlich auch in der OT zu erfüllen.)
- die allgemeinen Aspekte zu Netzarchitektur und -design, sowie zu der Segmentierung (siehe NET.1.1 *Netzarchitektur und -design*)
- die individuellen Aspekte der Hard- und Software-Komponenten, aus denen die jeweilige Fernwartungslösung besteht, z. B. Netzkomponenten, Server- und Clientsysteme, OT-Anwendungen (Hier sind die jeweils zutreffenden Bausteine zu modellieren.)
- die allgemeinen Aspekte der Protokollierung (siehe OPS.1.1.5 *Protokollierung*)
- die allgemeinen Aspekte des Outsourcings (siehe OPS.2.3 *Nutzung von Outsourcing*)
- die allgemeinen Aspekte cloudbasierter Fernwartungslösungen (siehe OPS.2.2 *Cloud-Nutzung*)
- die allgemeinen Aspekte webbasierter Fernwartungslösungen (siehe APP.3.1 *Webanwendungen und Webservices*)
- die allgemeinen Aspekte der Absicherung von ICS auf Bedienebene (siehe IND.1 *Prozessleit- und Automatisierungstechnik* und IND.2.7 *Safety Instrumented Systems*)

Dieser Baustein behandelt **nicht**

- die Beobachtung und Bedienung von ICS auf Prozessebene sowie
- steuernde Zugriffe per Fernwartung auf ICS, z. B. Anlaufen oder Stoppen von Anlagen. Solche Zugriffe können grundsätzlich Personen- und Sachschäden vor Ort verursachen!

## 2. Gefährdungslage

Da IT-Grundschatz-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.3.2 *Fernwartung im industriellen Umfeld* von besonderer Bedeutung.

## 2.1. Unvollständig dokumentierte Fernwartungszugänge in der OT

Die Fernwartungszugänge in der OT einer Institution sind in der Regel zahlreich und vielfältig. Darüber hinaus greift eine große Anzahl von internen und externen Personen darauf zu. Die Verwaltung von Fernwartungszugängen im industriellen Umfeld ist daher grundsätzlich unübersichtlich und fehleranfällig. Es besteht eine größere Gefahr als in der Büro- und Gebäude-IT, dass die diversen Zugänge unzureichend erfasst und dokumentiert werden, d. h. nicht überprüfbar sind.

Wenn unbekannte, offene OT-Fernwartungszugänge nicht dokumentiert sind, können die Betreibenden Zugriffe nicht unterbinden. In der Folge können unautorisierte Benutzende die physischen Abläufe eines ICS direkt beeinflussen, was z. B. zu Fehlverhalten einzelner Komponenten, zum Stillstand einer ganzen Produktionsanlage bis hin zu Gefahren für Leib und Leben von Mitarbeitenden vor Ort führen kann. Werden z. B. Anlagen inklusive dezentraler Komponenten für die Fernwartung als Gesamtsystem (Package Unit) vom herstellenden Unternehmen realisiert, unterliegen diese zunächst keiner ausreichenden Kontrolle durch die Betreibenden. Diese müssen jede OT-Fernwartungskomponente einzeln erfassen und häufig aktiv umkonfigurieren.

Wenn einige OT-Fernwartungszugänge z. B. nur dezentral erfasst und dokumentiert werden, dann besteht auch die Gefahr, dass notwendige Änderungen an einzelnen Zugängen unterbleiben oder durchgeführte Änderungen nicht nachvollziehbar sind.

## 2.2. Unzureichende Verfügbarkeit durch Abhängigkeiten von der Büro- und Gebäude-IT

ICS sind in Teilen auf einen vollständig unterbrechungsfreien Informationsfluss angewiesen. Dies gilt insbesondere für sämtliche Echtzeit-Datenströme. Bereits sehr kurze Unterbrechungen der Verfügbarkeit von Daten, die in der Büro- und Gebäude-IT toleriert werden können, können in einem ICS kritisch sein. Darüber hinaus können durch Abhängigkeiten von Netzen, Diensten oder IT-Systemen Sicherheitslücken entstehen. Dies wird häufig bei der Planung übersehen, wenn die OT und die Büro- und Gebäude-IT einer Institution miteinander kommunizieren.

Wenn Abhängigkeiten zwischen OT und Büro- und Gebäude-IT nicht beachtet und infolgedessen Sicherheitslücken nicht geschlossen werden, dann können Sicherheitsvorfälle schnell auf die gesamte OT übergreifen.

Wenn zentrale Komponenten und Dienste der Büro- und Gebäude-IT für die Fernwartung der OT genutzt werden (übergreifende Administration), dann kann es auch zu Abstimmungsfehlern zwischen Büro- und Gebäude-IT sowie OT kommen. In der Folge kann die Behebung kritischer Fehler in den ICS der OT verzögert werden. Ein Beispiel ist ein zentrales VPN-Gateway für den Fernzugriff, das durch eine Organisationseinheit außerhalb der OT bereitgestellt und nicht entsprechend abgestimmt betrieben wird, sodass es bei Bedarf nicht schnell genug zur Verfügung steht. Der Stillstand einer Anlage kann sich dann erheblich verlängern.

## 2.3. Unzureichende Regelungen für die Nutzung von OT-Fernwartungszugängen

OT-Fernwartungszugänge haben einen sehr großen potentiellen Benutzendenkreis außerhalb der betreibenden Institution. Gleichzeitig ist die lückenlose Verfügbarkeit von Echtzeitdaten in einem ICS unerlässlich, während die Verfügbarkeit von Daten der Büro- und Gebäude-IT in der Regel etwas weniger zeitkritisch ist. Allgemeine Regelungen, wie Fernwartungszugänge für die Büro- und Gebäude-IT genutzt werden, sind für die OT häufig unpassend oder lassen zu viel Spielraum.

Wenn die Nutzung von OT-Fernwartungszugängen nur unzureichend vertraglich geregelt ist, dann fehlen klare Vorgaben, wie der Benutzendenkreis jedes einzelnen Zugangs einzuschränken ist. Die Betreibenden können dann nicht kontrollieren, wer ihre OT-Fernwartungszugänge nutzt. So können z. B. Zugangsdaten bei Integratoren, Herstellenden und Wartungsdienstleistenden an Benutzende weitergegeben werden, die den Betreibenden unbekannt sind. Dies ist für ein ICS nicht tolerierbar.

Wenn restriktive Nutzungsregelungen speziell für die OT fehlen, dann können die Betreibenden auch nicht angemessen kontrollieren, wie OT-Fernwartungszugänge genutzt werden. Im Falle eines (Sicherheits-)Vorfalls wird dann z. B. die (forensische) Analyse erschwert, weil Ursachen nicht schnell genug erkannt werden können. Dies kann kostenintensive Produktionsstillstände verlängern.

Wenn OT-Fernwartungszugänge gemeinsam mit oder von der Büro- und Gebäude-IT bereitgestellt und betrieben werden und diese gemeinsame Nutzung der Hard- oder Software des Zugangs nicht eindeutig geregelt ist, dann können inkonsistente Konfigurationen auftreten. Diese erfüllen dann nur die Sicherheitsanforderungen der Büro- und Gebäude-IT, nicht jedoch abweichende oder zusätzliche Sicherheitsanforderungen der OT.

## **2.4. Unzureichende menschliche Kontrolle über OT-Fernwartungssitzungen**

Die Daten und Konfigurationseinstellungen innerhalb eines ICS sowie Personen, Sachen und Produktionsprozesse vor Ort können durch sämtliche Zugriffe aus anderen Zonen gefährdet sein, die nicht oder nur unzureichend durch internes Personal vor Ort kontrolliert werden. Insbesondere das Personal externer Wartungsdienstleistenden, Integratoren und herstellenden Unternehmen verfügt zwar über die notwendige Spezialkenntnis der zu wartenden Anlage, Maschine oder Komponente, weiß jedoch nicht, welche schädlichen Auswirkungen die konkrete Fernwartungssitzung im Gesamtsystem haben kann.

Wenn die Verläufe und Inhalte von OT-Fernwartungssitzungen von den Betreibenden nicht angemessen kontrolliert werden können, dann können Konfigurationsfehler mit hohem Gefährdungspotential sowie unabsichtliches oder absichtliches Fehlverhalten des Wartungspersonals nicht schnell genug erkannt und nachvollzogen werden. Dann sind Ausfälle oder Manipulationen von Echtzeit-Datenströmen möglich oder Schadsoftware kann sich unbemerkt in der gesamten OT ausbreiten. Schäden an Leib und Leben des Bedienungspersonals vor Ort oder hohe finanzielle Schäden durch Produktionsausfälle bis zur Zerstörung ganzer Anlagen können dann die Folge sein. Auch die Offenlegung von Betriebsgeheimnissen ist möglich. Zudem kann die Integrität der hergestellten Produkte beeinträchtigt werden, z. B. durch Manipulation von Rezepten, sodass Ausschuss produziert wird, der unter Umständen schwer zu erkennen ist. Wenn mangelhafte Produkte nicht als solche erkannt werden, dann kann dies die Reputation der Institution schädigen.

Ein Beispiel sind dezentrale OT-Fernwartungskomponenten innerhalb von Anlagen, die als Gesamtsystem von herstellenden Unternehmen realisiert werden (Package Units). Diese Fernwartungszugänge sind häufig so konstruiert, dass die herstellenden Unternehmen zu jeder Zeit auf die Anlage zugreifen können. Geschieht dies ohne Abstimmung mit dem Personal des oder der Betreibenden, dann können z. B. Gefahrensituationen im aktuellen Produktionsablauf entstehen.

## **2.5. Direkte IP-basierte Zugriffsmöglichkeiten auf ICS aus unsicheren Zonen**

Die Daten innerhalb eines ICS sowie Personen, Sachen und Produktionsprozesse vor Ort sind grundsätzlich durch direkte IP-basierte Zugriffsmöglichkeiten aus anderen Zonen und Netzen gefährdet. Dies gilt z. B. aufgrund der besonderen Patch-Zyklen in der OT, die wesentlich länger sein können als z. B. in der Büro-IT. Gleichzeitig erfolgen Fernwartungszugriffe auf ein ICS in der Regel aus nur eingeschränkt vertrauenswürdigen Netzen. Solche Netze sind nicht nur private Netze fremder Institutionen, sondern auch andere Zonen des eigenen Netzes. Nur eingeschränkt vertrauenswürdige

Zonen in der eigenen Institution sind z. B. solche der internen Büro- und Gebäude-IT oder auch weitere Zonen des OT-Netzes (z. B. zur Betriebs- und Produktionsführung mit MES, ERP).

Direktzugriffe aus anderen Zonen und Netzen auf ein ICS, z. B. über eine lokale Verbindung oder über VPN, können Schadprogramme einschleusen und gezielte Angriffe begünstigen. In der Folge können in den zu schützenden OT-Zonen Gefahren für Leib und Leben bestehen, hohe finanzielle Schäden durch Ausfallzeiten drohen oder vertrauliche Informationen wie z. B. Betriebsgeheimnisse in falsche Hände gelangen.

## **2.6. Unsichere alternative OT-Fernwartungszugänge für Störungen**

Insbesondere bei Störungen müssen OT-Fernwartungszugänge zuverlässiger und leistungsfähiger sein als in der Büro- und Gebäude-IT. Im industriellen Umfeld werden daher eigens alternative Fernwartungszugänge für schnelle Zugriffe eingerichtet. Diese stellen die Betriebsfähigkeit des ICS auch dann sicher, wenn der jeweilige primäre Zugang ausfällt oder nicht ausreichend performant ist, um z. B. kritische Fehlerzustände an entfernten Anlagen schnell genug beheben zu können. Solche alternativen Fernwartungszugänge können jedoch besonders verwundbar bei einem Angriff sein.

Wenn ein schneller alternativer Fernwartungszugang, z. B. über Mobilfunk, geschaffen wird, dieser jedoch die Sicherheitsanforderungen der Institution nicht vollständig erfüllt, dann können Angreifende leichter in das OT-Netz eindringen.

## **2.7. Unsichere Konzeption von OT-Fernwartungszugängen**

Häufig besitzt ein ICS eine dezentrale Infrastruktur mit zahlreichen OT-Fernwartungszugängen unterschiedlicher herstellender Unternehmen. Sowohl die unübersichtliche weiträumige Verteilung der Zugänge als auch die vielfältigen proprietären Fernwartungslösungen erschweren eine angemessene zentrale Absicherung sämtlicher OT-Fernwartungszugänge durch die Betreibenden.

Wenn sich OT-Fernwartungszugänge in offen zugänglichen Bereichen befinden, dann können Angreifende über diese Zugänge leicht in OT-Netze eindringen und Manipulationen vornehmen.

Auch wenn OT-Fernwartungszugänge nur durch herstellungsseitig vorgesehene Sicherheitskomponenten geschützt werden und diese die Sicherheitsvorgaben der Institution nicht erfüllen, können Angreifende über diese Zugänge leicht in OT-Netze eindringen und Manipulationen vornehmen.

## **2.8. Veraltete technische Konzeption von OT-Fernwartungszugängen**

Aufgrund der langen Lebenszyklen im industriellen Umfeld gibt es nicht selten OT-Fernwartungslösungen, die zehn Jahre und länger eingesetzt werden und aufgrund ihres Alters Sicherheitslücken aufweisen. Darüber hinaus liegen oft historisch gewachsene spezielle Umgebungsbedingungen vor wie z. B. die Installation von Fernwartungszugängen in offen zugänglichen Bereichen.

Wenn OT-Fernwartungszugänge aufgrund langer Lebenszyklen nicht geeignet abgesichert sind, dann erleichtert dies einen unautorisierten Zugriff in ein ICS und auch in weitere Netze und Systeme innerhalb und außerhalb der OT. So werden Manipulationen möglich, die bis zu Gefährdungen von Leib und Leben führen können.

Darüber hinaus können integrierte Fernwartungszugänge in Anlagen seit vielen Jahren unbekannt sein. Infolge zunehmender Abhängigkeiten von anderen Netzen und Systemen durch jüngere technische Veränderungen können unautorisierte Zugriffe mit kritischen Folgen dann immer wahrscheinlicher werden.

### 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins IND.3.2 *Fernwartung im industriellen Umfeld* 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.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	OT-Betrieb
Weitere Zuständigkeiten	IT-Betrieb, Planende, Wartungspersonal, Datenschutzbeauftragte, Mitarbeitende

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.3.2.A1 Planung des Einsatzes der Fernwartung in der OT (B) [Planende]**

Im industriellen Umfeld MUSS für sämtliche Einrichtungen zur Fernwartung ein einheitliches, zentrales Fernwartungskonzept für die gesamte OT der Institution erstellt werden. In dem OT-Fernwartungskonzept MÜSSEN folgende Aspekte berücksichtigt werden:

- spezifische gesetzliche Vorgaben, z. B. Schutz von Personen,
- spezifische Vorgaben durch anlagenherstellende Unternehmen,
- spezifische Anforderungen durch dezentrale Infrastrukturen,
- spezifische Anforderungen an die Anbindungen für die Fernwartung,
- spezifische Anforderungen an die Verfügbarkeit der Fernwartung,
- spezifische Anforderungen durch Umgebungsbedingungen sowie
- spezifische Anforderungen durch Bestandsanlagen.

Alle diese Aspekte MÜSSEN mit sämtlichen beteiligten internen und externen Stellen abgestimmt werden.

Sämtliche Fernwartungszugänge, über die Zugriffe auf ein ICS der Institution möglich sind, MÜSSEN in einer zentralen Dokumentation erfasst werden.

Für neu anzuschaffende fernwartbare Maschinen MÜSSEN die Anforderungen an die Informationssicherheit mit den Liefernden abgestimmt werden.

Das Ziel SOLLTE eine Standardisierung der verwendeten Fernwartungslösungen sein. Sobald standardisierte Lösungen für die Fernwartung geplant werden, MÜSSEN sich die OT und die Büro- und Gebäude-IT gemeinsam abstimmen.

### **IND.3.2.A2 Konsistente Dokumentation der Fernwartung durch OT sowie Büro- und Gebäude-IT (B) [IT-Betrieb, Wartungspersonal]**

Im industriellen Umfeld MÜSSEN die OT und die Büro- und Gebäude-IT sämtliche OT-Fernwartungszugänge gemeinsam erfassen und dokumentieren.

Insbesondere bei Fernwartungskomponenten, die in Package Units integriert sind, MÜSSEN auch alle deaktivierten Zugänge dokumentiert werden.

### **IND.3.2.A3 Regelmäßige Prüfungen sowie Ausnahmegenehmigungen bestehender OT-Fernwartungszugänge (B) [IT-Betrieb]**

Sämtliche Anlagen MÜSSEN regelmäßig geprüft werden, ob alle ihre Fernwartungszugänge dem Soll-Zustand, d. h. dem aktuellen Fernwartungskonzept für die OT, entsprechen.

Für notwendige Abweichungen vom Konzept MUSS innerhalb der OT ein Genehmigungsprozess etabliert werden.

### **IND.3.2.A4 Verbindliche Regelung der OT-Fernwartung durch Dritte (B)**

Mit sämtlichen externen Benutzenden, d. h. herstellenden Unternehmen, Integratoren und Wartungsdienstleistenden, MÜSSEN angemessen restriktive Regelungen für die OT-Fernwartung vertraglich vereinbart werden. Diese vertraglichen Regelungen MÜSSEN zu jedem Zeitpunkt gewährleisten, dass externe Benutzende jegliche OT-Fernwartungszugänge ausschließlich kontrolliert und abgestimmt nutzen.

Intern MUSS festgelegt werden, über welche Fernwartungszugänge welche Tätigkeiten durch welche externen Benutzenden zulässig sind. Darüber hinaus MUSS festgelegt werden, welche internen Mitarbeitende Fernwartungszugriffe und -tätigkeiten von Externen autorisieren, beobachten und gegebenenfalls unterstützen.

Im industriellen Umfeld MUSS sichergestellt werden, dass Personen an oder in Anlagen und Maschinen weder direkt noch indirekt durch eine aktive Fernwartung gefährdet werden können.

Insbesondere bei Safety-Maschinen MUSS der oder die interne OT-Mitarbeitende sowohl organisatorisch als auch technisch die Hoheit über den Beginn und das Ende der Fernwartung haben. Vertraglich MUSS ausgeschlossen werden, dass der Remote-Zugriff ohne explizite Zustimmung der internen OT-Mitarbeitenden aufgebaut und aufrechterhalten werden kann.

### **IND.3.2.A5 Interne Abstimmung für die OT-Fernwartung mit der Büro- und Gebäude-IT (B) [Planende]**

Die OT, die Büro- und Gebäude-IT sowie alle weiteren beteiligten Organisationseinheiten MÜSSEN angemessen restriktive Regelungen für sämtliche Komponenten und Schnittstellen festlegen, die direkt oder indirekt OT-Fernwartung in der Institution ermöglichen. Diese internen Regelungen MÜSSEN zu jedem Zeitpunkt eine kontrollierte und abgestimmte Nutzung der jeweiligen OT-Fernwartungszugänge gewährleisten. Folgende Aspekte MÜSSEN geregelt werden:

- Prozesse
- Zuständigkeiten
- Berechtigungen

### **IND.3.2.A6 Absicherung jedes Fernwartungszugriffs auf die OT (B) [IT-Betrieb]**

Im industriellen Umfeld MUSS die OT jeden Zugriff auf ein IT-System, das einen Fernwartungsdienst für die OT bereitstellt, selbst steuern können. Hierfür MUSS der Zugriff durch mindestens eine Sicherheitskomponente in der Zuständigkeit der OT abgesichert werden.

Der Zugang zur Fernwartung SOLLTE für alle Zugriffe vereinheitlicht werden. Jeder Zugriff SOLLTE mithilfe zentraler Authentisierungskomponenten kontrolliert und explizit zugelassen werden.

Falls Komponenten von OT-Fernwartungszugängen dezentral liegen oder in Package Units integriert sind, dann MÜSSEN diese Zugänge durch eine zusätzliche Sicherheitskomponente abgesichert werden, die ihrerseits zentral liegt und nicht in eine Package Unit integriert ist.

## 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.3.2.A7 Technische Entkopplung von Zugriffen (S) [Planende]

Jeder Fernzugriff auf jegliche Komponenten in einer OT-Zone SOLLTE entkoppelt erfolgen. In jedem Fernwartungszugang in die OT SOLLTE ein IT-System positioniert sein, das die Verbindung vor dem Übergang in die OT-Zielzone terminiert und zum Fernwartungsdienst eine neue, überwachte und reglementierte Kommunikation aufbaut.

Alle für die Fernwartung benötigten Werkzeuge und Programme SOLLTEN auf dem IT-System des Fernwartungszugangs installiert und lauffähig sein sowie einen Mehrbenutzendenbetrieb unterstützen. Das IT-System SOLLTE ein Sprungserver oder ein vergleichbares Application Layer Gateway (ALG) sein, das in einem dedizierten Sicherheitssegment, z. B. in einer demilitarisierten Zone (DMZ) positioniert ist.

Für das IT-System zur Entkopplung der Zugriffe SOLLTE die OT zuständig sein, d. h. es liegt idealerweise in einer OT-DMZ.

### IND.3.2.A8 Explizite Freigabe jeder OT-Fernwartungssitzung (S) [Mitarbeitende]

Jede Fernwartungssitzung SOLLTE vorab durch einen oder einer OT-Mitarbeitenden der betreibenden Institution, der oder die für das Zielsystem der Sitzung zuständig ist, genehmigt werden. Erst danach SOLLTE der oder die OT-Mitarbeitende den Fernwartungszugang freischalten. Die explizite Freigabe SOLLTE sowohl im Bedarfsfall als auch während abgestimmter Wartungsfenster eingehalten werden. Die Freigabe SOLLTE grundsätzlich nur für einen begrenzten Zeitraum gültig sein, d. h. die zuständigen OT-Mitarbeitenden behalten die Hoheit über den Zeitpunkt der Fernwartung (siehe Anforderung IND.3.2.A3 *Regelmäßige Prüfungen sowie Ausnahmegenehmigungen bestehender OT-Fernwartungszugänge*).

Darüber hinaus SOLLTEN externe Fernwartungszugriffe ausschließlich von innen nach außen, d. h. aus dem OT-Netz heraus, aufgebaut werden.

### IND.3.2.A9 Sicherer Austausch von Dateien begleitend zur OT-Fernwartung (S) [Planende, IT-Betrieb]

Für einen Dateiaustausch im Rahmen der OT-Fernwartung, z. B. von Konfigurationsdateien, Updates oder Handbüchern, SOLLTE ein sicheres Vorgehen etabliert werden. Dies MUSS mindestens eine Überprüfung auf Schadsoftware beinhalten.

Der Verbindungsaufbau zwischen einem Datenaustauschsystem und der Dateiquelle SOLLTE nicht automatisiert erfolgen, sondern vor jedem Dateiaustausch von der OT der Institution initiiert und authentisiert werden. Ein Dateiaustausch SOLLTE grundsätzlich protokolliert werden.

### IND.3.2.A10 Beobachtung und Kontrolle von OT-Fernwartungssitzungen (S) [Mitarbeitende]

Im industriellen Umfeld MUSS sichergestellt werden, dass weder direkt noch indirekt Personen an oder in Anlagen und Maschinen sowie die Anlagen oder Maschinen selbst durch eine aktive Fernwartung gefährdet werden können. Darüber hinaus MUSS sichergestellt werden, dass eine aktive Fernwartung den Produktionsprozess nicht beeinträchtigt.

Falls Personen- oder Sachschäden möglich sind, MUSS sichergestellt sein, dass die OT-Mitarbeitenden die Fernwartungstätigkeiten vor Ort mitverfolgen können (Vier-Augen-Prinzip). Die OT-Mitarbeitenden SOLLTEN bei Bedarf eingreifen können sowie eine Fernwartungssitzung unterbrechen können.

### **IND.3.2.A11 Zentrale Verwaltung aller Konten für die OT-Fernwartung (S) [IT-Betrieb]**

Für den Fernwartungszugriff in der OT SOLLTEN ausschließlich Konten verwendet werden, die in einem zentralen Verzeichnisdienst der OT oder der Institution verwaltet 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.3.2.A12 Dedizierte Fernwartungslösung in der OT (H) [Planende]**

Für die Fernwartung im industriellen Umfeld SOLLTE eine dedizierte OT-Fernwartungslösung eingesetzt werden, die unabhängig von der Büro- und Gebäude-IT ist. Alle weiteren Funktionen auf den IT-Systemen zur OT-Fernwartung, insbesondere auch Funktionen zur Administration von IT-Systemen und Netzen außerhalb der OT, SOLLTEN deaktiviert bzw. unterbunden werden.

Falls eine maximale Unabhängigkeit realisiert werden soll, SOLLTE auch ein dedizierter Internet-Zugang für die OT-Fernwartung genutzt werden.

### **IND.3.2.A13 Protokollierung der Inhalte von Fernwartungszugriffen in der OT (H) [Planende, Datenschutzbeauftragte]**

Für die Fernwartung von OT-Anwendungen oder -Systemen SOLLTE die Protokollierung so ausgeweitet werden, dass sämtliche Tätigkeiten lückenlos und umgehend nachvollziehbar sind. Hierzu SOLLTEN ergänzend zur Protokollierung von Ereignissen und Sitzungsdaten auch die Inhalte von Fernwartungszugriffen protokolliert werden.

### **IND.3.2.A14 Technische Kontrolle von Fernwartungssitzungen (H) [Planende, Datenschutzbeauftragte]**

OT-Fernwartungssitzungen SOLLTEN ergänzend zu IND.3.2.A10 *Beobachtung und Kontrolle von OT-Fernwartungssitzungen* kontinuierlich durch eine technische Lösung reglementiert werden. Dabei SOLLTEN die Aktivitäten auf Befehlebene, d. h. manuelle und automatisierte Befehle, technisch überwacht und gegebenenfalls automatisch unterbunden werden.

Zusätzlich SOLLTEN Sitzungen komponentenübergreifend überwacht werden. Falls technisch überwacht wird, dann SOLLTE nicht nur bei konkreten Regelverstößen, sondern auch bei Anomalien im Benutzungsverhalten ein Alarm ausgelöst werden, z. B. sobald ein plötzlich erhöhtes Kommunikationsvolumen erkannt wird.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „Fernwartung im industriellen Umfeld“ im Überblick, wie Fernwartungszugänge im Industrieumfeld sicher betrieben werden können.

Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in seiner Veröffentlichung „ICS Security Kompendium“ die Absicherung von industriellen Systemen (ICS, Industrial Control Systems).