Pierre Kobes

VDE VERLAG

Leitfaden Industrial Security

IEC 62443 einfach erklärt

Sicher.

Pilz bietet alles, was Sie für die Automation Ihrer Maschinen und Anlagen brauchen: innovative Komponenten und Systeme, bei denen Sicherheit und Automation in Hardware und Software verschmelzen.

Automatisierungslösungen für die Sicherheit von Mensch, Maschine und Umwelt.

www.pilz.com

PILZ
THE SPIRIT OF SAFETY

Pierre Kobes

Leitfaden Industrial Security

SIEMENS

Automatisierungs- und Antriebstechnik-Ausbildung leicht gemacht

Umfassende Unterstützung für Lehrende und Lernende in Bildungsstätten

Siemens Automation Cooperates with Education

Bei Siemens Automation Cooperates with Education (SCE) stehen Lernende und Lehrende im Mittelpunkt. SCE bietet Ihnen einen echten Mehrwert – in Form von Partnerschaften, Fachwissen oder Know-how für die Gestaltung von Lehrveranstaltungen.

Wir unterstützen bei der Vermittlung von Wissen der Automatisierungs- und Antriebstechnik und ermöglichen damit einfaches und strukturiertes Lernen.

Entdecke SCE

siemens.de/sce

Pierre Kobes

Leitfaden Industrial Security

IEC 62443 einfach erklärt

VDE VERLAG GMBH

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

ISBN 978-3-8007-4165-6 (Buch)
ISBN 978-3-8007-4166-3 (E-Book)

Titelbild: Cyber Security Operation Center (Quelle: www.siemens.com/presse)

Druck: Hubert & Co. (GmbH und Co. KG), Göttingen
Printed in Germany 2016-06

Vorwort

Der Schutz der kritischen Infrastrukturen gegen Cyberangriffe ist heute eines der wichtigen Ziele jeder Nation. Das im Jahr 2015 verabschiedete IT-Sicherheitsgesetz schreibt den Betreibern die Einhaltung von IT-Security-Mindeststandards vor. Die Normenreihe IEC 62443 hat zum Ziel, alle Anforderungen der Industrial Security abzudecken und bildet eine gute Basis für die Erstellung von ganzheitlichen Schutzkonzepten.

Als ich begann, auf dem Gebiet der IT-Sicherheit im industriellen Umfeld, der sogenannten Industrial Security tätig zu werden, wurde mir schnell klar, dass das Thema sehr vielfältig ist. Auf der einen Seite erfordert der Schutz gegen Cyberangriffe zahlreiche, zum Teil sehr unterschiedliche Maßnahmen. Beispielsweise sind Anwenderverwaltung und Patch-Management wichtige Bestandteile eines Schutzkonzepts. Zwei völlig unabhängige Maßnahmen, die jedoch in gleichem Maße wichtig sind. Auf der anderen Seite müssen oft sowohl Produkthersteller als auch Integratoren und Betreiber zu der Gestaltung von Schutzkonzepten beitragen.

In meiner Verantwortung für Standardisierung, Regulierung und Zertifizierung auf dem Gebiet der Industrial Security habe ich aktiv an der Gestaltung der Norm IEC 62443 mitgearbeitet. Entsprechend der Komplexität der Materie ist diese Norm sehr umfangreich. Das vorliegende Buch ist ein Versuch, die wesentlichen Konzepte, die für ganzheitliche Schutzkonzepte wichtig sind, darzustellen. Diese bilden auch die Grundlagen der Norm IEC 62443. Das Buch soll den Einstieg in die Norm erleichtern und einen Überblick über deren Inhalte geben. Es ist sowohl für Entscheider, technische Leiter, Geschäftsführer oder Ingenieure und Techniker, sowie Studierende gedacht.

Karlsruhe, Sommer 2016 *Pierre Kobes*

Inhaltsverzeichnis

1 Einleitung

Hackerangriffe auf Firmen, Verbände, oder Regierungsstellen machen deutlich, dass der sogenannte „Cyber War“ längst zur Realität geworden ist. Immer mehr geraten auch Industrieunternehmen und industrielle Anlagen ins Visier von Attacken, wie die zunehmenden Sicherheitsvorfälle in den letzten Jahren aus aller Welt deutlich machen. Ziele und Taktiken der Angriffe haben sich verändert, das Vorgehen wird zunehmend aggressiver und die Werkzeuge effektiver. Die veränderte Bedrohungslage erfordert ein grundlegendes Umdenken in Bezug auf Informations- und Zugriffsschutz, sowie das Vorgehen bei der Etablierung von Sicherheitskonzepten. Die Angreifer rüsten auf – sowohl Hersteller, als auch Betreiber von Automatisierungssystemen müssen sich diesen Bedrohungen stellen.

Schlagzeilen über Industrial Security finden sich mittlerweile auf den Titelseiten und in den Nachrichten. Meldungen über Hacker-Angriffe sind bereits an der Tagesordnung und man kommt nicht umhin sich der Tatsache zu stellen, dass von Jahr zu Jahr immer mehr Schwachstellen aufgedeckt werden. 1996 gab es erst eine Handvoll Meldungen über bekannt gewordene Sicherheitslücken und diese Zahl stieg bis in die letzten Jahre nahezu exponentiell auf mehrere Tausend an. Die Dunkelziffer der tatsächlich vorhandenen Schwachstellen liegt wohl noch um ein Vielfaches höher.

Im Office-Bereich werden bereits Standards für Maßnahmen zum Schutz von Informationen gegen Manipulation oder Datendiebstahl angewendet. Die Normserie ISO/IEC 27000 hat hier seit Jahren eine breite Akzeptanz gefunden. Im industriellen Umfeld konsolidieren sich verschiedene nationale Initiativen mehr und mehr in der Norm IEC 62443, auch bekannt als ISA-99. Sie adressiert die spezifischen Belange der IT-Sicherheit industrieller Anlagen. Obwohl die Definition der Norm in ihrer Gesamtheit noch nicht abgeschlossen ist, wächst ihre Akzeptanz in den relevanten Bereichen der Industrie. Bezeichnend ist, dass auch die amerikanische Behörde FDA (Food and Drug Administration) diese Norm referenziert. Grund genug, um sich mit dieser Norm auseinanderzusetzen.

Definition von „Industrial Security“

Der Begriff IT-Sicherheit oder Informationssicherheit wird allgemein verwendet, um den Schutz von Informationen gegen Manipulation und Diebstahl zu bezeichnen. Das Ziel der Informationssicherheit ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, die ein System verarbeitet, sicherzustellen. Die Reihenfolge entspricht hier auch der Priorität der Schutzziele. So ist es im Büroumfeld wichtiger, Informationen gegen unerlaubten Zugriff zu schützen als die Informationen unmittelbar und jederzeit dem Anwender zur Verfügung zu stellen. Es ist nicht ungewöhnlich, dass es am PC-Arbeitsplatz einige Sekunden dauern kann, bis sich das gewünschte Bild aufgebaut hat, oder der PC für einige Minuten nicht zur Verfügung steht, weil eine Aktualisierung des Betriebssystems vorgenommen wird.

Die IT-Sicherheit im Umfeld der Automatisierung hat einen etwas anderen Schwerpunkt. Hier geht es um den Schutz industrieller Anlagen vor unerlaubten physischen und digitalen Zugriffen. Diese können von krimineller Motivation kommen oder durch fahrlässiges Verhalten bewirkt sein. Beispielsweise könnte ein Mitarbeiter in einer Notsituation versuchen, die Festplatte des Produktionsrechners während der laufenden Produktion zu formatieren. Im Vordergrund der IT-Sicherheit in Automatisierungslösungen steht die Verfügbarkeit der Anlage. Es muss sichergestellt sein, dass die Produktion aufrechterhalten bleibt, auch wenn die Automatisierung durch Fehlhandlung oder Angriff beeinträchtigt wird. Die Priorität der Schutzziele sind in erster Linie die Verfügbarkeit und die Integrität der Automatisierungslösung in ihrer Kernfunktion, nämlich die Produktionsanlage zu steuern. Obwohl auch vertrauliche Daten wie zum Beispiel Rezepte in einer Automatisierungslösung bearbeitet werden können, steht oft der Schutz von Informationen gegen Datendiebstahl nicht im Vordergrund. Um sich von der IT-Sicherheit im Büroumfeld zu unterscheiden, wird oft der englische Begriff „Industrial Security“ für die IT-Sicherheit in Automatisierungslösungen verwendet. Es gibt im Deutschen keinen einfachen Begriff für den Einsatz von IT-Sicherheit in Automatisierungslösungen, daher werden wir im Folgenden in Abgrenzung zur Office-IT den Begriff „Industrial Security“ oder „IACS Security“ verwenden.

2 Anwendungsbereich und Rollen der IEC 62443

Die Norm IEC 62443 befasst sich mit der IT-Sicherheit sogenannter „Industrial Automation and Control Systems“ (IACS). Der Begriff IACS umfasst alle Bestandteile, die für den zuverlässigen und sicheren Betrieb einer automatisierten Produktionsanlage erforderlich sind. Das sind auf der einen Seite vernetzte Komponenten, die eine Automatisierungslösung realisieren, wie z. B. Steuerungen, Firewalls, Gateways, Switches, SCADA-Systeme oder PC-basierte Stationen. Dazu gehören auch alle Softwarekomponenten und Applikationen, die zur Automatisierung einer Produktion oder einer Prozessanlage eingesetzt werden. Die zweite Dimension eines IACS schließt die organisatorischen Prozesse für die Errichtung, den Betrieb und die Wartung der Automatisierungslösung ein. Dazu gehören Prozesse, die den Umgang und die Bedienung der Automatisierungslösung spezifizieren, die Festlegung interner Verantwortungsketten und Eskalationsprozesse, ebenso wie die Einbindung des involvierten Personals zum Beispiel mit Schulungsmaßnahmen.

Obwohl die Norm ursprünglich von der Automatisierungstechnik in der Prozessindustrie getrieben wurde, deckt ihr Anwendungsbereich nahezu alle Industriebereiche ab, zum Beispiel die diskrete Fertigung, dazu auch die Gebäudeautomation, verteilte Versorgungssysteme für Strom, Öl oder Wasser sowie Pipelines und die Öl- und Gas-Produktion. Auch andere Branchen, die automatisierte oder ferngesteuerte Einrichtungen einsetzen, beispielsweise Transportnetzwerke, fallen in den Anwendungsbereich der IEC 62443.

Die Norm beeinflusst potenziell alle Aktivitäten, die erforderlich sind für den vorhersagbaren und sicheren Betrieb der Produktion, den Schutz des Personals und der Produktion, die Verfügbarkeit, Effizienz und Qualität der Produktion, sowie den Schutz der Umwelt und die Gesetzeskonformität.

Grundlegend für das Verständnis der Norm IEC 62443 ist, dass der Schutz einer Anlage gegen gewollten oder ungewollten Missbrauch durch Cyberangriffe nicht mit einer einzigen Maßnahme erreicht werden kann, sondern von verschiedenen Beteiligten mitgestaltet werden muss. In der Norm werden grundsätzlich drei Basisrollen unterschieden, die alle ihren Beitrag liefern müssen: der Hersteller (*Product Supplier*), der Integrator (*System Integrator*) und der Betreiber (*Asset Owner*). Wir werden im Weiteren die Abkürzungen H, I und B für diese Rollen verwenden. Die englische Bezeichnung „Asset Owner“, die in der Norm IEC 62443 verwendet wird, bedeutet eigentlich „Eigentümer“; man hat angenommen, dass im Normalfall der Eigentümer auch die Anlage betreibt. Wir wählen hier den Begriff „Betreiber“.

Der Hersteller ist verantwortlich für Entwicklung, Vertrieb und Pflege der Anlagenkomponenten, die in der Automatisierungslösung eingesetzt werden. Der Integrator verantwortet das Design und die Inbetriebsetzung der Automatisierungslösung. Der Betreiber ist verantwortlich für den Betrieb und die Wartung der Automatisierungslösung sowie ihren Abbau am Ende des Lebenszyklus der Anlage. Wichtig ist hier zu erkennen, dass wir von Rollen sprechen, die von unterschiedlichen Organisationen wahrgenommen werden können. Es ist durchaus nicht unüblich, dass die Wartung der Anlage von einem externen Dienstleister durchgeführt wird, obwohl sie vom Rollenkonzept der Norm her in der Verantwortung des Betreibers liegt,

der die Vorgaben und die Kontrolle der Wartungsaktivitäten bestimmen muss. Anderseits haben viele Betreiber eigene Abteilungen, die die Aufgaben der Rolle Integrator übernehmen.

Tabelle 1 Rollen und Verantwortungen der Stakeholder des IACS

Verantwortung	Rolle
Entwicklung, Vertrieb und Pflege der Anlagenkomponenten, die in der Automatisierungslösung eingesetzt werden	Hersteller
Design und Inbetriebsetzung der Automatisierungslösung	Integrator
Betrieb, Wartung und Abbau der Automatisierungslösung	Betreiber (Dienstleister Wartung)

Die Aktivitäten und Maßnahmen der Industrial Security, die im Rahmen eines bestimmten Projekts durchgeführt werden, unterscheiden sich eindeutig von denjenigen, die unabhängig davon erfolgen. So werden die Komponenten einer Automatisierungslösung in der Regel nicht für ein spezifisches Projekt entwickelt, sondern für eine geplante Einsatzumgebung. Die Funktionalitäten werden spezifiziert, um eine möglichst breite Palette von Anwendungsfällen abzudecken. Typischerweise werden Steuerungen eines bestimmten Typs oft in vielen ganz unterschiedlichen Automatisierungslösungen eingesetzt, von Werkzeugmaschinen bis hin zu sehr komplexen Systemen, die z. B. in der Öl- und Gas-Industrie zum Einsatz kommen.

Im Gegensatz dazu haben die Aktivitäten des Integrators und des Betreibers immer das Ziel, die Vorgaben und die Randbedingungen eines bestimmten Automatisierungsprojekts zu erfüllen.

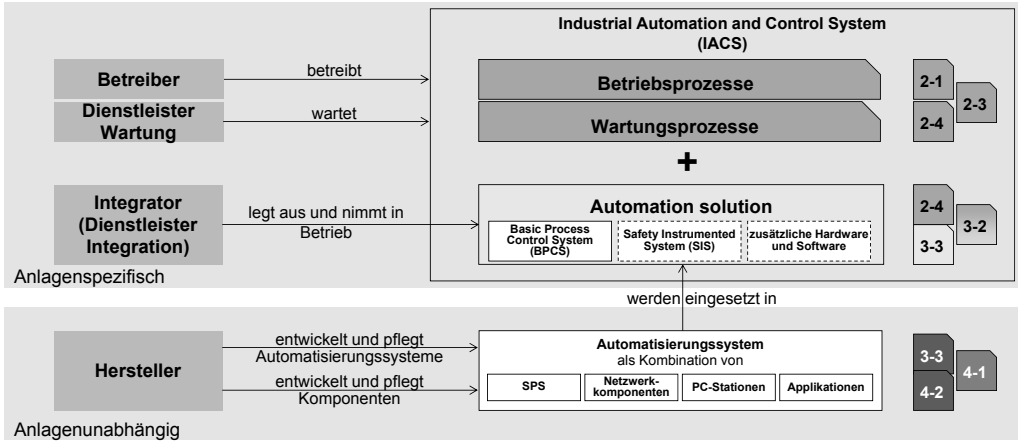

Bild 1 Basisrollen in der IEC 62443

3 Struktur der IEC 62443

Die Norm IEC 62443 ist in vier thematisch zusammenhängende Abschnitte gegliedert, die jeweils aus mehreren Dokumenten bestehen.

In dem ersten Abschnitt werden übergeordnete Aspekte behandelt wie allgemeine Konzepte, Terminologien und Methoden. Obwohl sich die IT-Sicherheit prinzipiell nicht messen lässt, soll ein Dokument entstehen, das Metriken zur Konformität definiert.

Der zweite Abschnitt spezifiziert organisatorische Maßnahmen und Prozesse, die als Bestandteil eines Defense-in-Depth-Konzepts relevant sind. Die Anforderungen richten sich an die für Betrieb und Wartung verantwortlichen Organisationen sowie an die Integratoren, die für die Erstellung der Automatisierungslösungen zuständig sind. Der Abschnitt beinhaltet auch ein Dokument, das Empfehlungen für das Patch Management während der Betriebsphase enthält.

Der dritte Abschnitt ist vorwiegend technischer Natur. Eines der Dokumente spezifiziert IT-Sicherheitsrelevante Anforderungen an die funktionalen Fähigkeiten der Automatisierungssysteme. Angesprochen sind vorwiegend die Hersteller, deren Beitrag für eine erhöhte Anlagensicherheit unerlässlich ist. Die Segmentierung des Kommunikationsnetzwerks ist eine wichtige Maßnahme zum Schutz gegen Cyberangriffe, um die Auswirkungen innerhalb der Automatisierungslösung einzuschränken. Sie muss in enger Zusammenarbeit zwischen Betreiber und Integrator festgelegt werden. Auf Basis einer Risikoanalyse legt man ein zu erreichendes Level der Schutzmaßnahmen für jede Zone und jeden Kanal fest. Dies ist Gegenstand eines weiteren Dokuments, das Methoden und Mittel beschreibt, um die Automatisierungslösung in Zellen und Kommunikationskanälen, sog. „*zones*“ und „*conduits*“, zu strukturieren. In Anlehnung an die deutsche Übersetzung der DKE werden wir im Weiteren die deutschen Begriffe „die Zone“ und „das Conduit“ verwenden. Letztendlich ist in diesem Abschnitt ein technischer Bericht über aktuelle Schutztechniken gegen Cyberangriffe enthalten.

Der vierte Abschnitt richtet sich an die Hersteller von Komponenten, die in Automatisierungslösungen eingesetzt werden. Allgemein gilt, dass die IT-Sicherheit integraler Bestandteil des Entwicklungsprozesses sein sollte. Damit sollen möglichst das Entstehen von Schwachstellen vermieden und Maßnahmen zur Stärkung ihrer Robustheit gegen Cyber-Bedrohungen vorgenommen werden. Dies wird in einem der beiden Dokumente dieses Abschnitts behandelt. Das zweite Dokument spezifiziert Anforderungen an funktionale Fähigkeiten von Komponenten. Dabei werden vier Komponenten-Klassen unterschieden:

- eingebettete Geräte („*Embedded Devices*“), z. B. Steuerungen,
- Host-Geräte („*Host Devices*“), z. B. PC-basierte Stationen,
- Netzwerkkomponenten („*Network Devices*“), z. B. Firewalls oder Gateways und
- Software-Produkte („*Applications*“).

Obwohl die Norm in ihrer Gesamtheit noch nicht verabschiedet ist, kann sie schon heute angewendet werden. Die Inhalte der wesentlichen Dokumente sind ausreichend stabil, um als Basis zur Erstellung eines Schutzkonzepts für industrielle Anlagen genutzt werden zu können:

- *IEC 62443-3-3, System security requirements and security levels:* Spezifiziert die funktionalen Anforderungen an die Automatisierungssysteme. Die Anforderungen richten sich sowohl an den Hersteller von Automatisierungssystemen als auch an den Integrator, der die funktionalen Eigenschaften der Automatisierungslösung auslegt und konfiguriert. Das Dokument wurde im Jahr 2013 als internationale Norm veröffentlicht.
- *IEC 62443-2-4, Requirements for IACS solution suppliers:* Spezifiziert die Anforderungen an die Integrations- und den Wartungsprozesse. Das Dokument wurde 2015 als internationale Norm veröffentlicht.
- *IEC 62443-2-1, Requirements for an IACS security management system:* Spezifiziert die organisatorischen Maßnahmen und Prozesse des Betreibers. Das aktuelle Dokument ist ein Profil der Norm ISO 27001 / 27002, die im Office-Bereich seit Jahren weitgehend angewendet wird. Das Dokument ist noch nicht als Standard verabschiedet; man kann sich in der Zwischenzeit jedoch auf die Norm ISO 27001 / 27002 stützen.

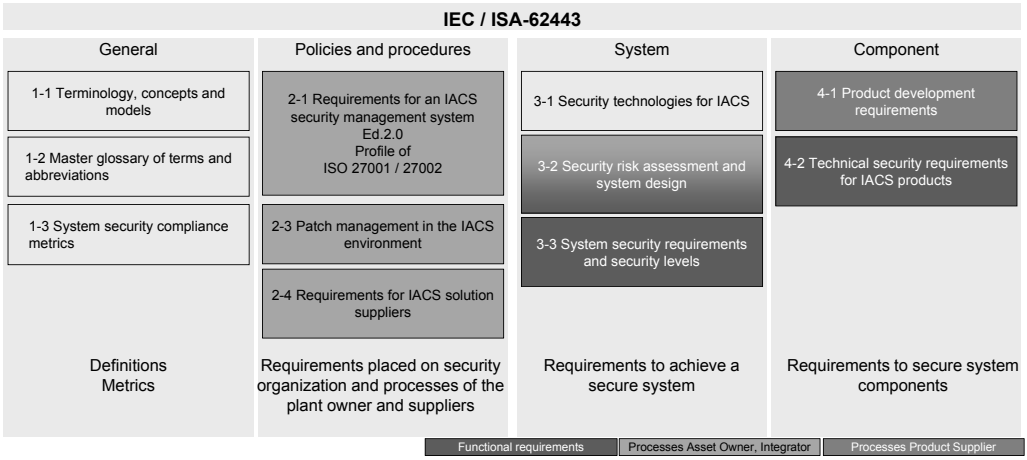

Bild 2 Struktur der IEC 62443

4 Konzepte der IEC 62443

Die Norm IEC 62443 basiert auf einigen übergeordneten Grundkonzepten. In der ersten Edition des Teils IEC 62443-1-1 [2], der 2009 veröffentlicht wurde, sind einige dieser Konzepte beschrieben. Ein Aktualisierung des Dokuments ist in Arbeit, das die folgenden Konzepte detaillierter beschreiben wird.

4.1 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Defense in Depth – dieses wichtige Konzept basiert auf der Erkenntnis, dass beim Schutz der industriellen Anlagen gegen Cyberangriffe die Beteiligung aller Stakeholder erforderlich ist: Betreiber, Integrator und Hersteller. Eine einzige Maßnahme ist im Allgemeinen nicht ausreichend, um einen angemessenen Level der Schutzmaßnahmen zu erreichen. Vielmehr müssen mehrere, untereinander abgestimmte und koordinierte Maßnahmen umgesetzt werden, die jeweils als Verteidigungslinien angesehen werden können. Die „*Defense in Depth*"-Strategie wird seit langem im militärischen Bereich angewendet. Schon im Mittelalter wurden die Burgen mit mehreren Verteidigungslinien ausgestattet: mit Festungsgraben, Zugbrücke, Außenmauer, Innenmauer, Bergfried und zuletzt der gepanzerten Tür am Zimmer des Feudalherrn. Überwindet der Angreifer eine Hürde, so steht ihm die nächste Verteidigungslinie entgegen. Die verschiedenen Bestandteile der Norm IEC 62443 unterstützen die Auslegung einer Defense-in-Depth-Strategie zum Schutz gegen Cyberangriffe.

Wenn man sich die Verteidigungslinien als Schalenmodell vorstellt, dann sind die äußeren Schichten beim Betreiber zu finden. Eine Grundvoraussetzung jedes Schutzkonzepts beginnt mit der Sensibilisierung der Mitarbeiter für die Gefahren von Cyberangriffen. Die Anlage muss physisch geschützt sein mit einer Zugangskontrolle aller autorisierten Personen. Die Norm fordert organisatorische Maßnahmen: definierte Prozesse zum Betrieb der Automatisierungslösung oder Maschine aber auch Kompetenzaufbau durch Informationsveranstaltungen oder Schulungen und klare Verantwortlichkeitsstrukturen in der Organisation. Zum Beispiel ist es sehr wichtig, die Rollen und Privilegien aller Anwender der Automatisierungslösung zu definieren und auf das minimal Notwendige einzugrenzen. Zu nennen ist auch die Festlegung der Maßnahmen im Voraus, die das Aufrechterhalten des Betriebs im Fall eines erfolgreichen Cyberangriffs sicherstellen sollen, sog. *„Business Continuity Plan"*.

Weitere Verteidigungslinien werden in der Auslegung der Automatisierungslösung gebildet, z. B. durch die Segmentierung des Kommunikationsnetzwerks in Firewall-geschützte Zellen oder den Zugriffsschutz mit Passwörtern. Zur Unterstützung der vom Betreiber festgelegten Rollen und Privilegien sollte die Automatisierungslösung so konfiguriert werden, dass die Anwender nur solche Aktionen durchführen können, die für ihre Aufgabe notwendig sind, sog. *„least privilege"*. Solche Maßnahmen werden in der Regel durch den Integrator umgesetzt.

Die inneren Verteidigungslinien werden über die Geräte und Komponenten der Automatisierungslösung bzw. der Maschine realisiert: durch dort integrierte Sicherheitsfunktionen. Zum

Beispiel werden Virenscanner oder weiße Listen (White Listing) zum Schutz gegen Malware eingesetzt. Schutz gegen Manipulation bieten Verschlüsselung, Hash-Techniken oder auch signierte Firmware-Downloads. Angriffe zum Herausfinden der Passwörter, sog. *„password guessing“*, werden durch Verzögerungen zwischen nacheinander folgenden Anmeldeversuchen abgewehrt.

Zu erwähnen ist auch, dass die Prozesse des Integrators möglichst darauf ausgelegt werden sollten, dass während des Designs der Automatisierungslösung nicht zusätzliche Angriffsmöglichkeiten geschaffen werden. Dazu gehört zum Beispiel das gezielte Löschen aller vorübergehenden Accounts, der Schutz der System- und Default-Accounts durch strenge Passwörter oder die systematische Aktualisierung aller Schutzmaßnahmen gegen Malware. Security-Maßnahmen sollten auch Bestandteil der Entwicklungsprozesse des Herstellers sein, mit dem Ziel, möglichst Schwachstellen in den Produkten auszuschließen. Dazu gehören Risikoanalysen, Programmierrichtlinien, statische und dynamische Codeanalysen oder Penetrationstests.

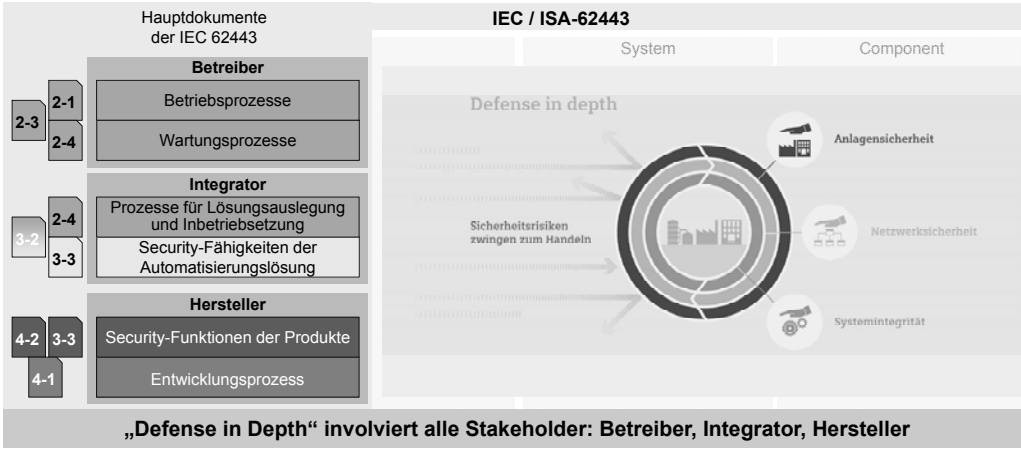

Bild 3 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Dass Schwachstellen und damit Angriffsvektoren durch die jeweiligen Stakeholder erzeugt werden können, zeigt folgendes Beispiel im Thema Anwenderverwaltung und Zugriffskontrolle (*„User Management and Access Control, UMAC“*). In den Produkten findet man oft noch fest codierte Passwörter. Gelingt es einem Angreifer, den Code auszulesen und zu analysieren, wird es für ihn ein Leichtes sein, solche Passwörter ausfindig zu machen. Dafür sind im Internet zuhauf Werkzeuge verfügbar. Eine andere typische Schwachstelle ist die Möglichkeit, Privilegien zu erhöhen und sich zum Beispiel durch Überwinden der Anwenderverwaltung als Administrator anzumelden. Damit stehen dem Angreifer alle Mittel zum Missbrauch zur Verfügung. Die Hersteller können solche Schwachstellen durch klare Regeln für die Programmerstellung im Entwicklungsprozess vermeiden. In der Verantwortung des Integrators liegt wie bereits erwähnt der Schutz der bei der Werksauslieferung vorhandenen System- und Default-Accounts durch Ändern der Default-Passwörter. Während der Auslegung der Automatisierungslösung werden in der Regel temporäre Accounts angelegt, die hohe Privilegien besitzen und durch schwache Passwörter geschützt sind. Während der Designphase möchte

ja der Entwickler nicht aufwendig bei jedem Einloggen ein langes, komplexes Passwort eingeben müssen. Eine häufig anzutreffende Schwachstelle ist, dass diese Accounts vor der Übergabe der Lösung an den Betreiber nicht gelöscht wurden. Man kann sich vorstellen, was ein Angreifer dadurch anrichten kann. Durch entsprechende Vorgaben in den Prozessen des Integrators können solche Schwachstellen leicht vermieden werden. Schließlich liegt es am Betreiber, die Namen der Personen, die den definierten Rollen zugewiesen sind, während der Betriebsphase zu pflegen. Da diese oft viele Jahre dauert, ist die Verantwortung des Betreibers besonders groß. Wenn zum Beispiel ein Administrator die Firma verlässt, ist es von eminenter Wichtigkeit, dessen Account zu löschen. Möchte diese Person der Firma schaden, wären die Verteidigungsmöglichkeiten sehr eingeschränkt. Eine andere wichtige Aufgabe des Betreibers ist, dafür zu sorgen, dass die Passwörter vertraulich behandelt werden und regelmäßig geändert werden. Hier sind die Betriebs- und Wartungsprozesse gefragt. Aus dem genannten Beispiel wird ersichtlich, dass alle der o. g. Maßnahmen umgesetzt werden müssen, um einen gewissen Schutz zu erreichen. Eine einzelne Schwachstelle reicht aus, um die gesamte Kette zu schwächen und die Anlage anfällig zu machen.

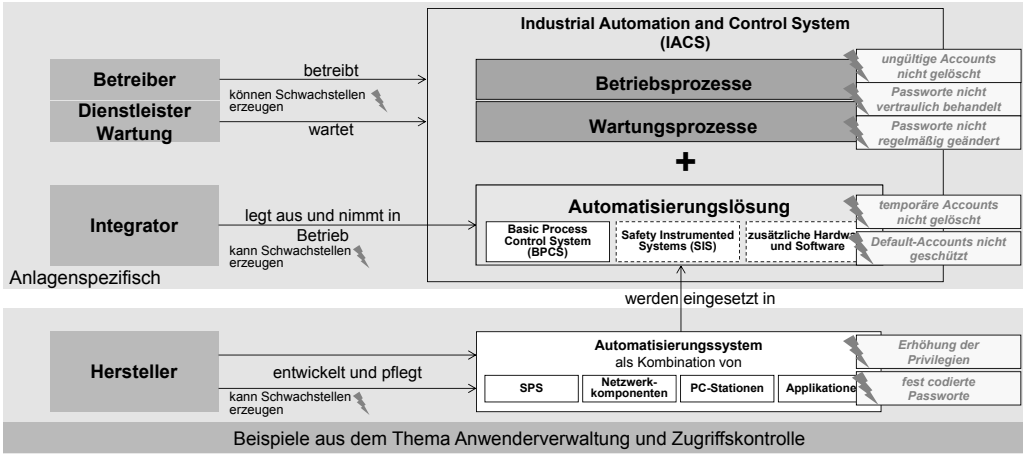

Bild 4 Beispiele von Schwachstellen bei Anwenderverwaltung und Zugriffskontrolle

4.2 Risikobewertung nach VDI/VDE 2182

Die Schutzmaßnahmen gegen Cyberangriffe ergeben sich aus der Bewertung der Bedrohungen und der Konsequenzen im Fall eines Angriffs auf die Betrachtungsgegenstände, die in der Verantwortung der jeweiligen Organisation sind. Für den Hersteller sind es seine Produkte, der Integrator wird die Automatisierungslösung betrachten und für den Betreiber steht die Produktionsanlage im Fokus.

Die prinzipielle Vorgehensweise gliedert sich in vier Phasen, die zyklisch wiederholt werden:

1. Planung / Bewertung der Risiken und der möglichen Gegenmaßnahmen
2. Festlegung der Schutzmaßnahmen

3. Bewertung ihrer Effizienz
4. Umsetzung der Maßnahmen

Sowohl die Projektvorgaben als auch die Bedrohungslage können sich im Laufe der Zeit verändern, sodass es erforderlich ist, das Vorgehen in zeitlich regelmäßigen Abständen oder auch ereignisgesteuert zu wiederholen, um die Maßnahmen ggf. anzupassen. In der Literatur wird diese Vorgehensweise oft als „Plan-Do-Check-Act“ oder PDCA bezeichnet. Die Norm IEC 62443 setzt voraus, dass solche PDCA-Zyklen von allen Stakeholdern durchgeführt werden. Das Vorgehensmodell der Richtlinie VDI/VDE 2182 [12], beschreibt detailliert die prinzipielle Vorgehensweise eines PDCA-Zyklus und erläutert die Abhängigkeiten zwischen den jeweiligen Zyklen bei Hersteller, Integrator und Betreiber. Diese Richtlinie wird in der Norm referenziert und wird im Weiteren zusammengefasst.

Betrachtungsgegenstand kann eine Komponente, eine Automatisierungslösung oder eine Anlage sein. Voraussetzung ist eine vollständige Systemdokumentation der Security-relevanten Eigenschaften des Betrachtungsgegenstands. Sie beschreibt den bestimmungsgemäßen Gebrauch, die verwendete Hardware, die Betriebssysteme und Firmware, die Kommunikationsdienste, die Applikationssoftware, Lebenszyklusaspekte sowie die Handlungsanweisungen für Engineering, Inbetriebnahme und Wartung.

Die Dokumentation des PDCA-Zyklus soll jeden Prozessschritt beschreiben. Festgehalten werden das Ergebnis des jeweiligen Schritts, das Vorgehen bei der Ergebnisfindung, die Begründung der Bewertung der einzelnen Schritte, die verwendeten Hilfsmitteln, die Beteiligten an dem Prozess sowie die Liste der noch offenen Punkte.

Die Anwendung des Vorgehensmodells setzt die Durchführung einer Strukturanalyse voraus, die zum Ziel hat, den Betrachtungsgegenstand (Komponente, Automatisierungslösung oder Anlage) in seinen funktionalen Anforderungen möglichst genau zu spezifizieren und die Einsatzumgebung zu beschreiben. Die funktionalen Anforderungen umfassen den genauen Umfang mit Funktionen, Schnittstellen und Datenflüssen, die Anwendung und die Netzwerkinfrastruktur. Die Einsatzumgebung schließt im Wesentlichen die Beschreibung von Einflussgrößen auf den Betrachtungsgegenstand, z. B. der Topografie (Gebäude, Umwelt), ein. Bei einer Komponente, in der die projektspezifischen Einflussgrößen nicht bekannt sind, geht man von einem typischen Einsatzfeld aus.

Das Vorgehensmodell besteht aus acht Schritten, die wie in einer Kette hintereinander angereiht sind und sequenziell durchgeführt werden. Das Ergebnis eines Glieds bildet die Eingangsinformation des jeweiligen nächsten Glieds.

- Schritt 1: Assets identifizieren
  - Eingangsinformationen: Ergebnis der Strukturanalyse
  - Aktionen: Die relevanten Assets aus der Strukturanalyse werden definiert und gegliedert. Hilfreich ist dabei, den Betrachtungsgegenstand in eine hardwareorientierte Sicht zu gliedern.
  - Ergebnisse: Liste der identifizierten Assets
- Schritt 2: Bedrohungen analysieren
  - Eingangsinformationen: Liste der identifizierten Assets

  - Aktionen: In diesem Schritt werden relevante Bedrohungen für jedes Asset des Betrachtungsgegenstands analysiert. Je nach Zustand des Betrachtungsgegenstands werden die Szenarien festgehalten, die für verschiedene Bedrohungen relevant sind und in einer Bedrohungsmatrix zusammengestellt.
  - Ergebnisse: Bedrohungsmatrix
- Schritt 3: relevante Schutzziele ermitteln
  - Eingangsinformationen: Bedrohungsmatrix
  - Aktionen: In diesem Schritt werden die für den Betrachtungsgegenstand relevanten Schutzziele festgelegt. Für jedes identifizierte Asset soll entschieden werden, welche Schutzziele relevant sind.
  - Ergebnisse: Bedrohungsmatrix mit relevanten Schutzzielen
- Schritt 4: Risiken analysieren und bewerten
  - Eingangsinformationen: Bedrohungsmatrix mit relevanten Schutzzielen
  - Aktionen: Die bestehenden Risiken, die sich aus Bedrohungen ergeben, werden analysiert und bewertet. Aus dem Gefahrenpotenzial und der Einfachheit des Angriffs werden die Wahrscheinlichkeiten für das Eintreten der im vorherigen Schritt identifizierten Bedrohungen bewertet. Somit werden die für den Betrachtungsgegenstand potenziellen Bedrohungen sowie der jeweils daraus resultierende Schaden abgeschätzt. Statistische Daten liegen in der Regel nicht vor, sodass die Risikobewertung meist qualitativer Art ist.
  - Ergebnisse: tabellarische Risikobewertungen mit relevanten Bedrohungen
- Schritt 5: Schutzmaßnahmen aufzeigen und Wirksamkeit bewerten
  - Eingangsinformationen: tabellarische Risikobewertungen mit relevanten Bedrohungen
  - Aktionen: In diesem Schritt werden Maßnahmen und deren Wirksamkeit gegen die relevanten Bedrohungen beschrieben. Passende Schutzmaßnahmen werden mithilfe von Katalogen, Erfahrungen und sonstigen Dokumenten ausgewählt. Oft wird einer Bedrohung durch mehrere, verschiedene Schutzmaßnahmen entgegengewirkt. Jeder empfohlenen Schutzmaßnahme werden die entsprechenden Kosten zugeordnet, um eine wirtschaftliche Bewertung der Gesamtlösung zu ermitteln.
  - Ergebnisse: Liste von möglichen Schutzmaßnahmen, deren Wirksamkeit und Kosten
- Schritt 6: Schutzmaßnahmen auswählen
  - Eingangsinformationen: Liste von möglichen Schutzmaßnahmen, deren Wirksamkeit und Kosten
  - Aktionen: Aus der Vielzahl der aufgezeigten Schutzmaßnahmen wird eine angemessene, wirtschaftlich sinnvolle Gesamtlösung als beste Kombination von Maßnahmen ausgewählt. Dabei müssen die Ziele des Unternehmens und die Konformität mit der Unternehmenspolitik insbesondere in Bezug auf die IT-Sicherheit berücksichtigt werden.
  - Ergebnisse: Schutzmaßnahmen ausgewählt
- Schritt 7: Schutzmaßnahmen umsetzen
  - Eingangsinformationen: Schutzmaßnahmen ausgewählt
  - Aktionen: Die einzelnen Schutzmaßnahmen sollen im Kontext der Gesamtlösung umgesetzt werden. In diesem Zug ist ein Betriebskonzept zu entwerfen, das die nach-

haltige Umsetzung der Lösung gewährleistet. Ist der Betrachtungsgegenstand eine Automatisierungslösung oder eine Anlage, deckt das Betriebskonzept die gesamte Betriebsphase ab. Für ein Produkt betrifft das Betriebskonzept die Vermarktungsphase.

  - Ergebnisse: Schutzmaßnahmen umgesetzt und Betriebskonzept erstellt

- Schritt 8: Prozessaudit durchführen
  - Eingangsinformationen: alle Dokumentationen
  - Aktionen: In den Audits wird überprüft, ob alle definierten Maßnahmen zur Erreichung der festgelegten Schutzziele sowie zum Schutz gegen die relevanten Bedrohungen ausreichend sind und erfolgreich implementiert wurden. Die Audits sind durch Personen durchzuführen, die nicht im Prozess beteiligt waren.
  - Ergebnisse: Auditbericht

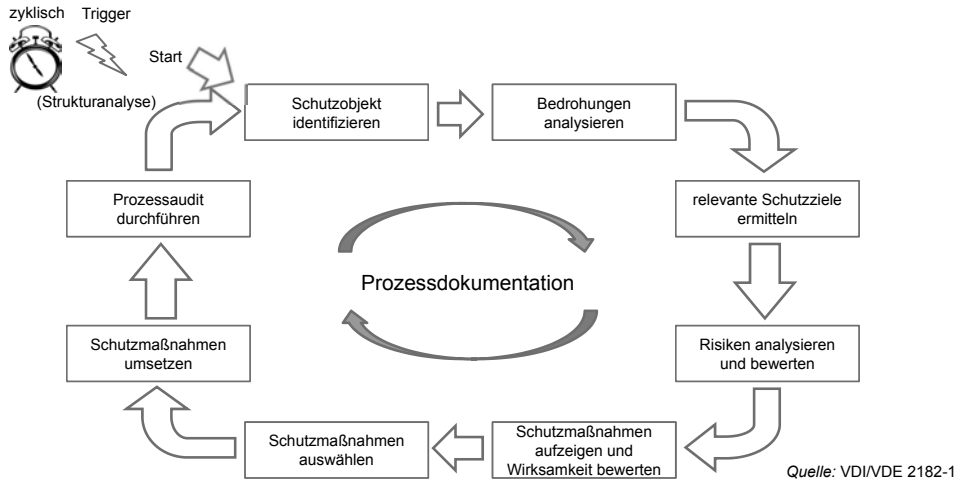

Bild 5 Prinzipielle Vorgehensweise nach VDI/VDE 2182 / Zyklus PDCA (Plan-Do-Check-Act)

Das Vorgehensmodell sollte auf verschiedene Betrachtungsgegenstände beim Hersteller, Integrator oder Betreiber angewendet werden. Die Zyklen beeinflussen sich dabei gegenseitig, es sind in beiden Richtungen Informationen auszutauschen, um die jeweiligen Zyklen durchführen zu können.

In den Zyklen des Herstellers werden als Eingangsinformationen die Anforderungen der geplanten Zielmärkte bei der Entwicklung der Produkte herangezogen. Diese kann man als Zusammenfassung aus den Anforderungen einer Vielzahl von Projekten sehen. Aus dieser Betrachtungsweise werden sie aus Ausgangsinformationen von Zyklen der Integratoren und der Betreiber gebildet. Als Ausgangsinformation muss der Hersteller eine Dokumentation erstellen, die die Security-Funktionen und -Eigenschaften des Produkts beinhaltet und zusätzlich alle relevanten Informationen für die Integration und Nutzung dieser Fähigkeiten in einer möglichst sicheren Automatisierungslösung. Es müssen alle Informationen vorliegen, die zur Beurteilung des Einsatzes des Automatisierungsgeräts oder -systems aus Security-Gesichtspunkten erforderlich sind, etwa die verwendeten Protokolle, Anforderungen an die umgebende IT-Infrastruktur oder die Möglichkeiten, das Produkt zu härten. Der Hersteller

soll auch während der Lebenszeit des Produkts einen kontinuierlichen Support leisten, um die Aufrechterhaltung seines Security-Zustands zu gewährleisten, z. B. durch Bereitstellung von Updates und Patches.

Für den Integrator besteht im Wesentlichen die Eingangsinformation für seine Zyklen aus den Security-Anforderungen der Automatisierungslösung. Diese sollten vom Betreiber in der Regel als Bestandteil eines Lastenhefts festgelegt werden. Die Anforderungen sind projektspezifisch und berücksichtigen sowohl die Produktions- bzw. Prozessbedingungen als auch die umgebende IT-Infrastruktur und die Richtlinien zur IT-Sicherheit des Betreibers. Oft kann man Security-Anforderungen durch mehrere Varianten eines Maßnahmenbündels erfüllen, die meist aus einer Mischung aus Technik und Prozessen bestehen. Die PDCA-Zyklen des Integrators müssen daher in enger Abstimmung mit dem Betreiber erfolgen, um die Gesamtlösung aus funktionalen und organisatorischen Maßnahmen zu optimieren. Der Integrator muss die Security-Funktionen und -Eigenschaften der Automatisierungslösung dokumentieren und alle relevanten Informationen für einen sicheren Betrieb und zur Aufrechterhaltung des Schutz-Levels entlang des Lebenszyklus der Anlage zur Verfügung stellen. Diese bilden die Eingangsinformationen für die Zyklen, die durch den Betreiber während der Betriebs- und Wartungsphasen durchgeführt werden.

Der Betreiber muss während der gesamten Betriebsphase, die in vielen Projekten viele Jahre dauert, immer wieder PDCA-Zyklen durchlaufen, um das Schutz-Level der Anlage zu prüfen und aufrecht zu halten. Grundsätzlich ist der Schutz einer Anlage oder einer Produktion nur dann möglich, wenn der Betreiber weitere Maßnahmen umsetzt, die nur in seiner Verantwortung liegen können. Zum Beispiel ist es erforderlich, durch eine dokumentierte Richtlinie die Behandlung der Passwörter zu regeln. Diese muss insbesondere die Sicherstellung der Vertraulichkeit, die Festlegung der Passwortkomplexität sowie die Vorgaben für die regelmäßige Änderung der Passwörter abdecken. Eine weitere wichtige Maßnahme ist die Verwaltung der Anwender einschließlich der regelmäßigen Pflege der Liste der zugelassenen Anwender mit ihren Rechten und Pflichten. Eine Anpassung der Maßnahmen kann erforderlich sein, wenn sich die Bedrohungslage verändert oder wenn durch operative Anforderungen die Automatisierungslösung verändert wird. Das sind typische Auslöser von PDCA-Zyklen beim Betreiber.

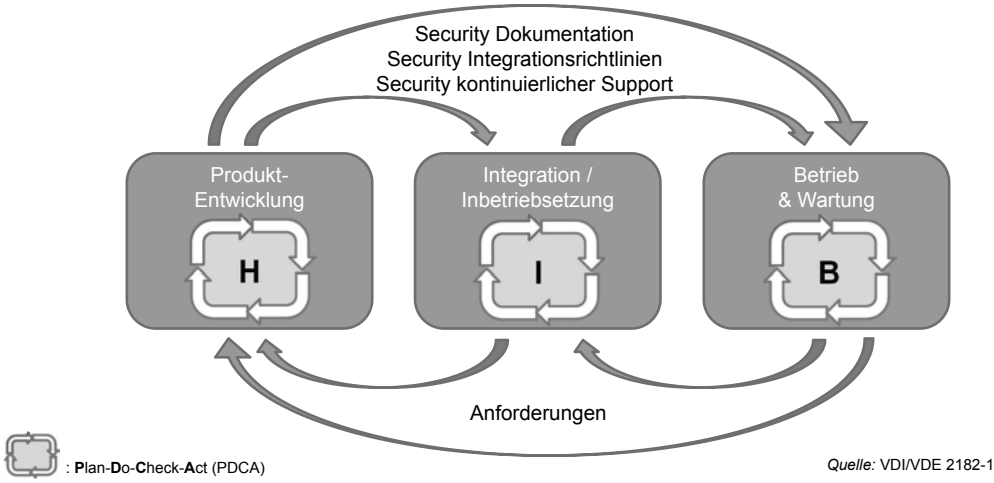

Bild 6 Abhängigkeiten der PDCA-Zyklen

4.3 Die Norm IEC 62443 in Produkt- und Anlagenlebenszyklen

Obwohl einige Produkte für ein spezifisches Projekt entwickelt wurden, hat in der Regel der Produkthersteller das Ziel, einen gegebenen Zielmarkt mit Produkten und Systemen für eine möglichst breite Palette von Anwendungen zu bedienen. Die Produktlebenszyklen sind daher unabhängig von dem Lebenszyklus einer bestimmten Anlage.

Einsatz der Norm in den Produktlebenszyklen

Typischerweise kann man den Produktlebenszyklus in die Phasen Spezifikation, Design und Entwicklung, Vermarktung und Pflege und Ausphasen gliedern. Welche Bestandteile der Norm IEC 62443 können den Hersteller dabei unterstützen?

Um möglichst die Erzeugung von Schwachstellen während der Entstehung des Produkts zu vermeiden, sollte der Hersteller einen stringenten Entwicklungsprozess einhalten, der in allen Phasen die Security als nichtfunktionale Anforderungen integriert. In der Norm IEC 62443 wurde dies im Teil *„IEC 62443-4-1 Product development requirements“* [10] behandelt. Das Dokument deckt den gesamten Entwicklungsprozess ab, von der Spezifikation bis zur Testphase. Darüber hinaus werden Anforderungen an der Behandlung von eventuellen Schwachstellen spezifiziert, die während der Vermarktung auftreten könnten. Es werden ergänzende, Security-spezifische Anforderungen an den Entwicklungsprozess beschrieben.

Die funktionalen Anforderungen an die Produkte befinden sich in den Teilen *„IEC 62443-3-3 System security requirements and Security-Levels“* [9] und *„IEC 62443-4-2 Technical security requirements for IACS products“* [11]. Der Hersteller sollte in seinen Produkten die Security-Funktionen integrieren, die zur Unterstützung der allgemeinen Schutz-Anforderungen des Zielmarkts benötigt werden. Die Produkt-Funktionen werden vom Integrator in der Automatisierungslösung eingesetzt und entsprechend der Projektanforderungen konfiguriert. Gegebenenfalls müssen zusätzliche Maßnahmen und Produkte hinzugefügt werden, um den geforderten Schutz-Level zu erreichen. Der Teil IEC 62443-3-3 spezifiziert die Anforderungen an ein Automatisierungssystem. Im Teil IEC 62443-4-2 werden die daraus abgeleiteten Anforderungen an spezifische Komponenten eines Systems beschrieben. Es wird zwischen SPS oder ähnlichen Komponenten (*embedded device*), Netzwerkkomponenten (*network device*), PC-basierten Stationen (*host device*) oder Applikationssoftware (*application*) differenziert.

Beim Thema Updates und Patches kann der Hersteller weitere Unterstützung in dem Teil *„IEC 62443-2-3 Patch Management in the IACS environment“* [5] finden. Das Dokument gibt Handlungsempfehlungen für einen abgestimmten Prozess zwischen den beteiligten Parteien, um eine Aktualisierung der Softwarekomponenten durch Patches möglichst effizient zu gestalten. Das Beispiel eines Security-Patches eines Betriebssystems verdeutlicht die Abhängigkeiten der Prozesse der Stakeholder. Der Hersteller von Applikationssoftware, die unter dem Betriebssystem abläuft, muss prüfen, ob die Software nach wie vor fehlerfrei unter dem aktualisierten Betriebssystem abläuft. Gegebenenfalls müssen mehrere Versionen der Applikationssoftware geprüft werden. Diese Kompatibilitätsinformation ist Bestandteil des in Abschnitt 4.2 beschriebenen kontinuierlichen Supports. Dann kommt der Integrator ins Spiel, der die Aussage treffen muss, ob der Security-Patch für die Automatisierungslösung

relevant ist und Empfehlungen für das Einspielen des Patches gibt. Oft kann der Betreiber selbst dieses anhand der vom Integrator gelieferten Dokumentation durchführen. Als Letzter muss der Betreiber handeln, indem er abhängig von den Betriebsbedingungen den Zeitpunkt und das Vorgehen für das Einspielen des Patches festlegt. Dies kann zum Beispiel während der nächsten planmäßigen Wartung erfolgen. Das Dokument schlägt auch eine Struktur zur Identifikation und Beschreibung der Patches vor. Hilfreich kann auch für den Hersteller der Teil *„IEC 62443-3-1 Security technologies for IACS“* [7] sein. Er beinhaltet eine Auflistung der IT-Sicherheits-Maßnahmen nach aktuellem Stand der Technik, die nach Einsatzbereich und Effizienz bewertet werden.

Einsatz der Norm in den Anlagenlebenszyklen

Ähnlich wie beim Produktlebenszyklus kann der Anlagenlebenszyklus in die Phasen Spezifikation, Integration und Inbetriebnahme, Betrieb und Wartung und letztendlich Dekommissionierung aufgeteilt werden. Im Gegensatz zum Produktlebenszyklus unterscheiden sich die Hauptverantwortlichen für die jeweilige Durchführung von Phase zu Phase.

In der Regel beginnt der Prozess mit der funktionalen Spezifikation des Projekts. Hier ist der Betreiber gefragt. Er sollte ein Lastenheft erstellen, das die Risiken und strategischen Anforderungen seiner Organisation berücksichtigt, zum Beispiel die übergeordnete IT-Sicherheits-Richtlinie oder die physische Umgebung der Anlage. Das Dokument *„IEC 62443-2-1 Requirements for an IACS security Management System“* [4] ist ein guter Leitfaden, um die verschiedenen Dimensionen der IT-Sicherheit zu berücksichtigen. Ein wesentlicher Bestandteil des Lastenhefts ist die Vorgabe der Schutzziele der Anlage in Abhängigkeit ihrer Kritikalität. Die Bewertung basiert auf den Konsequenzen eines Missbrauchs für das Geschäft des Betreibers oder für die Umwelt. Zum Zeitpunkt der Erstellung dieses Buchs[1)] war das Dokument IEC 62443-2-1 noch nicht als Standard angenommen. Es ist jedoch beschlossen, dass es als Profil der ISO/IEC 27001/27002 strukturiert wird. Es sollen lediglich die spezifischen Anforderungen für den Einsatz der ISO 27001/27002 im industriellen Umfeld beschrieben werden. Daher kann diese Norm verwendet werden, bis das Dokument veröffentlicht wird.

Die Schutzziele werden in die nächste Phase des Anlagenlebenszyklus, der Integration und Inbetriebnahme, verwendet, um die projektspezifische Automatisierungslösung zu designen und zu implementieren. Hier liegt die Hauptverantwortung beim Integrator. Oft ist ein iterativer Prozess erforderlich, in dem Integrator und Betreiber sich eng abstimmen müssen, um eine optimale Gesamtlösung zu erstellen. Das daraus resultierende Schutzkonzept besteht in der Regel aus einem Bündel funktionaler und organisatorischer Maßnahmen, die von beiden Rollen zu verantworten sind. Spezifisch für den Integrator sind folgende Industrial-Security-relevanten Aufgaben zu erfüllen:

- Auslegen einer Systemarchitektur in Zonen und Conduits
- Auswahl und Integration der Produkte, um der Security-Funktionen und -Eigenschaften mithilfe der Dokumentation und der Integrationsrichtlinien in die Automatisierungslösung optimal einzusetzen

[1)] Frühjahr 2016

- Konfiguration und Parametrierung der Produkte, insbesondere Durchführung von Härtungsmaßnahmen
- Einrichten der Rollen und Privilegien der Anwender unter Berücksichtigung des Prinzips des sog. *„least privilege“*
- Validierung, dass die Automatisierungslösung die vorgegebenen Schutzziele erfüllt
- Minimierung der möglichen Einführung zusätzlicher Schwachstellen durch adäquate Prozesse

Das Dokument *„IEC 62443-2-4 Requirements for IACS solution suppliers“* [6] spezifiziert Anforderungen an die Prozesse des Integrators mit dem Ziel, möglichst zu vermeiden, dass zusätzliche Schwachstellen bei der Auslegung der Automatisierungslösung entstehen. Beispielsweise ist es sehr wichtig, alle temporären Accounts, die zwischenzeitlich für den Design, den Test und die Inbetriebnahme angelegt wurden, vor der Übergabe an den Betreiber wieder zu löschen. Der Integrator wird bei der Auslegung der Systemarchitektur durch das Dokument *„IEC 62443-3-2 Security risk assessment and system design“* [8] unterstützt, die eine Vorgehensweise für die Segmentierung der Automatisierungslösung in Zonen und Conduits beschreibt. Er wird sich auch auf das Dokument IEC 62443-3-3 für die Umsetzung der Security-Funktionen und -Eigenschaften der Automatisierungslösung stützen können.

Der Betreiber ist in der Regel hauptverantwortlich für die Betriebs- und Wartungsphase der Anlage. Neben den funktionalen Security-Funktionen und -Eigenschaften der Automatisierungslösung spielen die Betriebs- und Wartungsprozesse eine wichtige Rolle zur Aufrechterhaltung der Schutzziele während der gesamten Betriebsphase. Um das akzeptierte Restrisiko nicht steigen zu lassen, muss stetig eine kontinuierliche Überprüfung der Maßnahmen erfolgen. Dafür ist es sehr sinnvoll, ein IT-Sicherheits-Management-System einzuführen und zu betreiben. Für die Betriebsprozesse kann der Betreiber sich auf das Dokument *„IEC 62443-2-1 Requirements for an IACS security management system“* [4] stützen, um sowohl prozedurale Vorgaben zu definieren als auch eine Security-Organisation festzulegen und zu betreiben. Einige Elemente eines IT-Sicherheits-Management-Systems wurden bereits angesprochen. Als weiteres Beispiel muss der Betreiber die erforderlichen Prozessschritte beschreiben, die für das Aufrechterhalten des Betriebs im Falle eines Cyberangriffs notwendig sind (*business continuity plan)*. Die Vorgaben des Teils *„IEC 62443-2-4 Requirements for IACS solution suppliers“* [6] sind auch für die Wartungsprozesse relevant. Das Dokument richtet sich an einen Dienstleister, der vom Betreiber für die Wartung beauftragt wurde. Oft verantwortet eine Organisation des Betreibers selbst diese Aufgabe. Wie bereits erwähnt spielt die Aktualisierung der Softwarekomponenten durch Patches während dieser Phase eine wichtige Rolle für die Industrial Security, siehe dazu das Dokument *„IEC 62443-2-3 Patch Management in the IACS environment“* [5]. Bei Änderung der Automatisierungslösung, die durch betriebsbedingte Änderung der Anforderungen oder durch Änderung der Bedrohungslage erforderlich sein kann, müssen die Schutzziele aufrechterhalten bleiben. In dem Fall sind die wesentlichen Dokumente der Integrationsphase relevant.

Letztendlich ist bei der De-Kommissionierung von Komponenten oder von kompletten Anlagen zu vermeiden, dass vertrauliche Informationen unerlaubt ausgelesen werden können. Ein gezieltes Löschen der Speicher in den Geräten ist daher sehr sinnvoll.

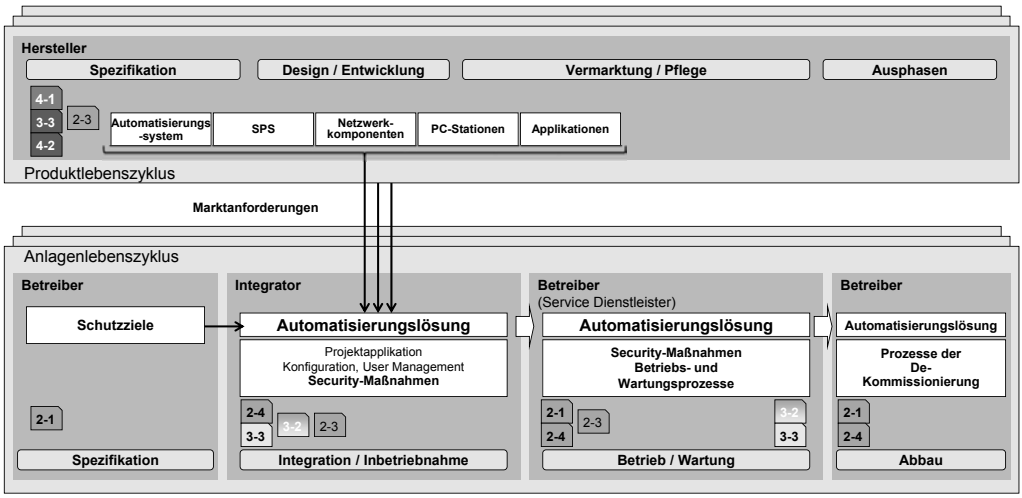

Bild 7 Produkt- und Anlagenlebenszyklen

4.4 PDCA-Zyklen in Produkt- und Anlagenlebenszyklen

Wie bereits erwähnt sind die PDCA-Zyklen der Hersteller, Integratoren und Betreiber ineinander verflochten. Wie sind die Abhängigkeiten im Rahmen der Produkt- und Anlagenlebenszyklen zu verstehen?

Hersteller

Die PDCA-Zyklen der Hersteller sind weitgehend von denjenigen der Integratoren und Betreiber entkoppelt. Als Eingangsinformationen werden die Marktanforderungen berücksichtigt, die man als Synthese vieler Anlagenanforderungen zusammenfassen kann. Während des Produktlebenszyklus sollte der Hersteller mehrere PDCA-Zyklen durchführen. Der erste sollte bereits in der Spezifikationsphase erfolgen und sich auf die Security-Anforderungen des Produkts fokussieren. Die Datenströme im Produkt und deren Auswirkung auf die Funktionen des Produkts werden analysiert. Man fokussiert sich auf die Zugänglichkeit der Datenströme für einen potenziellen Angreifer und den daraus entstehenden möglichen Missbrauch. Daraus werden Gegenmaßnahmen festgelegt und priorisiert, um eine möglichst hohe Resilienz zu erreichen. Man geht von Bedrohungen aus, die in der geplanten Einsatzumgebung zu erwarten sind. Weitere PDCA-Zyklen sollten in der Design- und Entwicklungsphase stattfinden, um funktionale Gegenmaßnahmen zu definieren. Während der Vermarktungsphase sollte der Hersteller proaktiv über entdeckte Schwachstellen kommunizieren und diese durch Updates beheben. Wird das Produkt vom Markt genommen, sollten Integratoren und Betreiber frühzeitig informiert werden und Ersatz oder Alternativen vorgeschlagen werden. Allgemein üblich ist die Bereitstellung der Dokumentation über die Security-Funktionen und -Eigenschaften des Produkts. Darüber hinaus sollten aber auch Richtlinien und Leitfäden gegeben werden, die

die möglichst sicherere Integration des Produkts in eine Automatisierungslösung beschreiben. Letztendlich muss der Hersteller während der Gesamtlebenszeit des Produkts einen kontinuierlichen Support für projektspezifische Aktivitäten gewährleisten, beispielsweise durch der Bereitstellung von Updates und Patches.

Integrator und Betreiber

In der Spezifikationsphase des Anlagenlebenszyklus sollte sich der Inhalt der PDCA-Zyklen des Betreibers auf die Aufrechterhaltung des Betriebs im Falle eines Angriffs fokussieren. Für die Auslegung der Automatisierungslösung ist besonders wichtig, dass der zu erreichende Security-Level für die Automatisierungslösung festgelegt wird. Dieser leitet sich aus der Kritikalität des betrachteten Assets für das Geschäft des Betreibers ab. Auf der einen Seite sollte der Betreiber Vorgaben für die Auslegung der Automatisierungslösung spezifizieren, auf der anderen Seite Maßnahmen festlegen, die er selbst durchführen muss, etwa den physischen Zugang zu wichtigen Teilen der Automatisierungslösung.

Der Integrator wird die funktionale Ausführung der Automatisierungslösung betrachten und seine PDCA-Zyklen durchführen mit dem Ziel, in enger Abstimmung mit dem Betreiber das Schutzkonzept zur Erfüllung der vorgegebenen Schutzziele festzulegen. Das Schutzkonzept besteht in der Regel aus einem Bündel abgestimmter funktionaler und organisatorischer Maßnahmen im Rahmen einer Defense-in-Depth-Strategie. Der Integrator muss die Security-Funktionen und -Eigenschaften der Automatisierungslösung dokumentieren und alle Betriebsrichtlinien erstellen, die benötigt werden, um:

- die Automatisierungslösung sicher im Rahmen der Spezifikation zu betreiben, zu warten und abzubauen,
- eine Änderung der Anlage unter Beibehaltung des vorgegebenen Levels der Schutzmaßnahmen durchzuführen,
- regelmäßige Prüfungen der Effizienz der Schutzmaßnahmen durchzuführen und
- den Schutz der Anlage auf Veränderungen der Bedrohungslage anzupassen.

Die Dokumentation sollte auch empfohlene Schulungsmaßnahmen für das Personal beinhalten, das für den Betrieb und die Wartung zuständig ist.

Während der gesamten Betriebs- und Wartungsphase sollten PDCA-Zyklen im Rahmen von regelmäßigen Audits oder beim Entdecken von neuen Schwachstellen durchgeführt werden, um sicherzustellen, dass die vorgegebenen Schutzziele stets durch die funktionalen und organisatorischen Maßnahmen zu erfüllen sind. Die Hersteller müssen den Betreiber zeitnah über jede Schwachstelle und über deren Behebung, z. B. durch einen Patch informieren. Oft ist die Unterstützung des Integrators notwendig, um die Relevanz der gemeldeten Schwachstelle und des Patches für die Automatisierungslösung zu ermitteln. Auch Änderungen der Bedrohungslage, die zu einer Schwächung des Anlagenschutzes führen könnten, sollten beobachtet werden und Maßnahmen zur Behebung oder Umgehung der Schwächung sollten vorgeschlagen werden.

Letztendlich müssen die Schutzziele – zumindest teilweise – aufrechterhalten bleiben, wenn die Automatisierungslösung abgebaut wird oder eine Komponente aus dem Betrieb genommen

wird. Im Vordergrund steht die Sicherstellung der Vertraulichkeit sensitiver Information, wie Rezepte oder Passwörter, die in den Komponenten abgespeichert sind und durch einen potenziellen Angreifer ausgelesen werden können. Ein gezieltes Bereinigen solcher Informationen ist erforderlich und muss in der Dokumentation der Hersteller beschrieben sein.

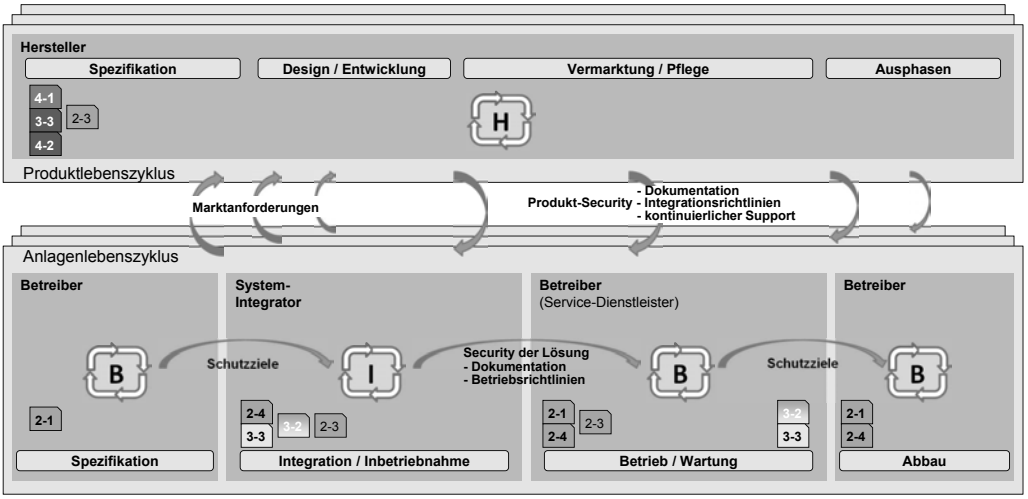

Bild 8 PDCA-Zyklen in Produkt- und Anlagenlebenszyklen

4.5 Security-Levels (Security-Level, SL) nach IEC 62443-3-3

Im Bereich der funktionalen Sicherheit („*safety*“) werden die Sicherheitsanforderungen in Stufen unterteilt, die in der internationalen Normung gemäß IEC 61508/IEC61511 auch als Sicherheits-Integritätslevel (SIL) bezeichnet werden. Ein Level der funktionalen Sicherheit ist eine Ganzzahl, die die Fähigkeit der Anlage oder des Geräts kennzeichnet, Schaden für die Umwelt oder Personen zu vermeiden. Der SIL-Wert basiert auf der Restfehlerwahrscheinlichkeit und kann quantitativ gemessen werden.

Im Gegensatz zur funktionalen Sicherheit ist die Anzahl unterschiedlicher Faktoren, die die Industrial Security beeinflussen, viel größer. Zum Beispiel kann ein Missbrauch durch eine falsche Behandlung eines erlaubten Anwenders der Automatisierungslösung verursacht werden. Dem entgegen wirken unter anderem die Anwenderverwaltung und die rollenbasierte Einschränkung der Aktionen auf das minimal Nötige. Die Anlage kann auch durch gewollten Missbrauch angegriffen werden, oft erfolgt der Angriff in mehreren Schritten. Systemhärtung, Netzwerksegmentierung und Schutz gegen Malware sind in diesem Fall Beispiele geeigneter Schutzmaßnahmen. In den genannten Beispielen sind die Schutzmaßnahmen völlig unabhängig voneinander, tragen aber alle zur Erreichung eines gegebenen Levels der Schutzmaßnahmen bei. Die Zusammenfassung des Security-Levels in einer einzigen Zahl ist daher offenbar bei der IT-Sicherheit nicht möglich. Bevor auf die Mehrdimensionalität der Security-Levels eingegangen wird, wollen wir die Vorgehensweise beschreiben.

Der Standard beschreibt im Teil 3-2 wie, basierend auf einer Risikobetrachtung, die Automatisierungsanlage in Zonen und Conduits aufgeteilt wird. Der Ausgangspunkt dabei ist das Schutzziel, das vom Betreiber in der Spezifikationsphase des Anlagenlebenszyklus ermittelt wird. Die Security-Levels (*Security-Levels, SL*) stellen einen qualitativen Ansatz dar, um den Schutz einer Zone oder eines Conduits zu definieren. Man kann sie verwenden, um den Schutz von Zonen im Rahmen der Netzwerkarchitektur zu differenzieren. Sie werden von Herstellern, Integratoren und Anwendern benutzt, um die Produkte und Maßnahmen auszuwählen, die in der Automatisierungslösung eingesetzt werden.

Erwähnenswert ist, dass ein Angriff, der heute mit wenig Kompetenz und Mitteln durchführbar ist, deutlich folgenreicher sein kann als noch vor wenigen Jahren. Es sind neue Werkzeuge und Programme im Internet verfügbar, die einen vergleichbaren Angriff viel leichter machen.

Zur Definition der Security-Levels werden Kompetenz, Ressourcen und Motivation für die Überwindung des Schutzes der Automatisierungslösung unterschieden. Diese Art zu differenzieren wurde bewusst gewählt, um der Tatsache Rechnung zu tragen, dass die Leistungsfähigkeit der potenziellen Angreifer mit der Zeit zunimmt. Die Definitionen der Security-Levels können unverändert bleiben, die Mittel und die Kompetenzen zur Überwindung der Schutzmaßnahmen einer gegebenen Anlage können im Laufe der Zeit einfacher werden. Schutzmaßnahmen, die heute einem gegebenen Security-Level entsprechen, können zukünftig gegebenenfalls nur noch für ein niedrigeres Security-Level ausreichend sein. Die PDCA-Zyklen während der Betriebsphase sind erforderlich, um gegebenenfalls die Maßnahmen anzupassen.

In der Norm IEC 62443 werden vier Security-Levels definiert:

- SL 1: Schutz gegen ungewollten, zufälligen Missbrauch,
- SL 2: Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation,
- SL 3: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und moderater Motivation,
- SL 4: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation.

Zum heutigen Zeitpunkt ist keine Methode bekannt, die IT-Sicherheit mathematisch zu messen. Die Wirkung der Maßnahmen und damit die Bewertung des Schutzes entsprechend der o. g. Definitionen können nur qualitativ erfolgen. Der Betreiber muss beispielsweise für die betrachtete Anlage die spezifische Bedeutung der Begriffe „niedrig“, „mittel“ und „hoch“ definieren. Langfristig könnte man sich eine quantitative Methode vorstellen, wenn genügend statistische Daten über Bedrohungen, Risiken und Ereignisse vorliegen.

Die Vorgehensweise nutzt drei Ausprägungen der Security-Levels:

- Zu erreichende Security-Levels (*Target SLs, SL-T*): Sie stellen die Security-Levels für eine Zone oder ein System dar, die zu erreichen sind. Sie werden in der Regel mithilfe der Bewertung der Risiken und des erforderlichen Schutzes ermittelt, um die Fortsetzung des Betriebs sicherzustellen. Ein bewährtes Mittel dazu ist die Durchführung der bereits erwähnten PDCA-Zyklen.

- Erreichte Security-Levels (*Achieved SLs, SL-A*): Diese sind die durch die Maßnahmen der Automatisierungslösung erreichten Security-Levels. Sie werden benutzt, um zu bewerten, ob die Security-Funktionen und -Eigenschaften der Automatisierungslösung die Vorgaben der zu erreichenden Security-Levels erfüllen.
- Erreichbare Security-Levels (*Capability SLs, SL-C*): Sie werden auf Produkte (Systeme oder Komponenten) angewendet und stellen den Level dar, der erreicht werden kann, wenn die Funktionen und Eigenschaften des Produkts ausgenutzt und korrekt in einer Automatisierungslösung umgesetzt werden.

Ausgehend von den zu erreichenden Security-Levels wird eine Automatisierungslösung ausgelegt, in der die Funktionalitäten der eingesetzten Produkte eingesetzt und konfiguriert werden, um den vorgegebenen Level zu erfüllen. In der Regel ist das ein iterativer Prozess, um die optimale Lösung zu finden. Abhängig von ihren Funktionalitäten bezüglich IT-Sicherheit wird der Integrator die Systeme und Komponenten wählen, um das Ziel-Security-Level zu erreichen. Zusätzliche funktionale oder organisatorische Ausgleichsmaßnahmen können gegebenenfalls eingesetzt werden. Dies sollte in enger Abstimmung zwischen Integrator und Betreiber erfolgen, um die wirtschaftlich optimale Gesamtlösung zu erreichen.

Die erste Zone wird gebildet, indem die Grenzen der Automatisierungslösung sowie alle Conduits mit der umgebenden Infrastruktur spezifiziert werden. Dann wird die Architektur in weitere Zonen und Conduits aufgeteilt, indem die Auswirkung eines Missbrauchs auf das Geschäft des Betreibers bewertet wird. Dabei kann die finanzielle Auswirkung, die Auswirkung auf die Umwelt oder die Auswirkung auf die Vertraulichkeit sensibler Daten herangezogen werden. Für jede Zone wird das Ziel-Security-Level festgelegt. Ein detailliertes Konzept der Automatisierungslösung ist dafür nicht erforderlich; es genügt, sich auf die zu erfüllenden Funktionen und die Conduits zwischen den Zonen zu beziehen.

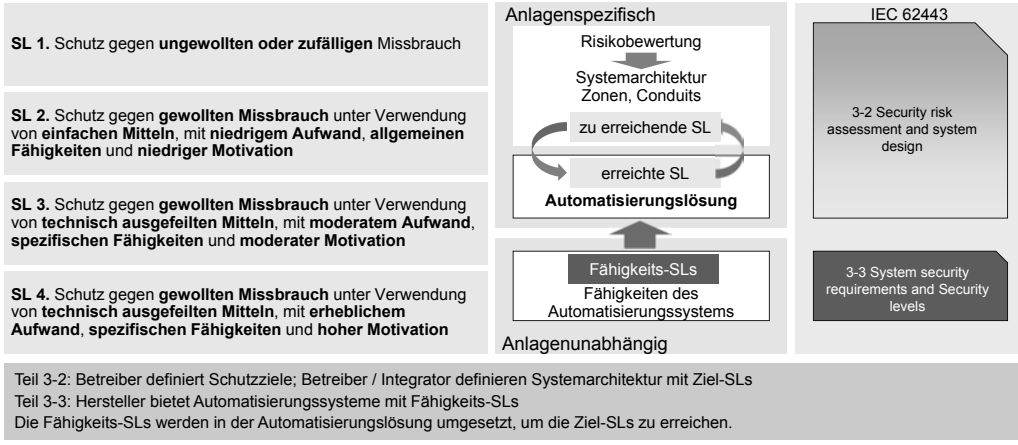

Bild 9 Security-Level SL nach IEC 62443-3-3

5 Ganzheitlicher Ansatz, Schutz-Levels

In dem vorherigen Abschnitt wurden die Security-Levels beschrieben, so wie sie im heutigen Stand[1)] der Norm stehen. Im Folgenden wollen wir verdeutlichen, dass die Security-Levels noch keine vollständige Aussage über den Schutz einer Anlage im laufenden Betrieb gegen Angriffe geben. Wir wollen die Ergänzung beschreiben, um ausgehend von Security-Levels auf eine vollständigere Bewertung des Schutzes der Anlagen mithilfe von sog. Schutz-Levels (*Protection Levels*) zu kommen.

Wie in vielen anderen Gebieten, entwickelt sich mit der Entstehung der Norm IEC 62443 auch die Nachfrage nach dem Nachweis der Konformität zu der Norm. Allgemein stellen sich die Fragen nach der Bewertung und Differenzierung der Produkte und Systeme bezüglich ihrer Security-Funktionen und -Eigenschaften. Einige kommerzielle Firmen bieten die Prüfung der Robustheit von Automatisierungskomponenten gegenüber Angriffen, die eine Überflutung verfälschter Protokollpakete verwenden. Das Ziel ist dabei, das Produkt mit sog. *„Denial of Service"*-Attacken außer Funktion zu setzen. Weitere Anbieter zertifizieren Prozesse von Integratoren gebündelt mit den Fähigkeiten von Automatisierungssystemen, die von diesen Integratoren eingesetzt werden. Die Security-Levels nach IEC 62443-3-3 bieten die Vorlage, um Automatisierungskomponenten oder -systeme zu differenzieren. Die Aussage, ein Produkt mit Funktionen und Eigenschaften, die dem Level 3 entsprechen, wäre „sicherer" als ein Produkt auf Level 2, ist jedoch für den Betreiber der Automatisierungslösung mit großer Vorsicht zu genießen, wie die weiteren Ausführungen zeigen werden.

Bewertungen und Zertifizierungen, die Produkte, Systeme oder Prozesse losgelöst von spezifischen Projektanforderungen bewerten, können bei dem Betreiber einer Anlage dazu beitragen, ein gewisses Vertrauen aufzubauen, dass damit seine spezifischen Anforderungen besser zu erfüllen als mit anderen Produkten, die solche Zertifikate nicht haben. Dies ist aber keineswegs sichergestellt, denn Fehler in Design und Implementierung der Automatisierungslösung können durchaus dazu führen, dass trotz Einsatz funktional sehr fähiger Produkte und Systeme der Schutz trotzdem schwach ist. Beispielsweise spielen Netzwerkarchitektur und Anwenderverwaltung in einem ganzheitlichen Schutzkonzept eine wesentliche Rolle. Diese sind in jedem Projekt spezifisch auszulegen und können sehr unterschiedlich sein. Durch geschickten Einsatz einiger leistungsfähiger Netzwerkkomponenten kann ein sehr guter Schutz erreicht werden, auch wenn etwa die Steuerungen einen relativ niedrigen Level aufweisen. Umgekehrt kann eine Automatisierungslösung mit flacher Netzwerkarchitektur und schlechter Konfiguration trotz des Einsatzes von Steuerungen mit sehr guten Security-Funktionen und -Eigenschaften einen niedrigen Schutz aufweisen. Es muss ganz klar herausgestellt werden, dass eine Automatisierungslösung mit einem zu erreichenden Level nicht den Einsatz von Produkten und Systemen mit gleichem Level erfordert. Umgekehrt entstehen durch Einsatz von Produkten und Systemen mit einem gegebenen Security-Level nicht zwangsläufig Automatisierungslösungen mit dem gleichen Level.

[1)] Frühjahr 2016

Bei den Schutz-Levels geht es um die Auslegung und Bewertung des Schutzes von Anlagen im Betrieb

Aus Sicht des Betreibers sind Bewertungen von Produkten, Systemen oder Prozessfähigkeiten nützliche Indikatoren. Eine Bewertung über den Schutz seiner Anlage oder Produktion in Betrieb kann jedoch nur vor Ort erfolgen und muss alle Maßnahmen eines ganzheitlichen Schutz-Konzepts abdecken. Dies ist der Anwendungsbereich der Schutz-Levels. In-fine ist der Schutz von Anlagen und Produktionen im operativen Betrieb das Ziel aller Anstrengungen von Herstellern, Integratoren und Betreibern. Auch wenn die Staaten neue Regelungen zum Schutz von kritischen Infrastrukturen erlassen, z. B. das in 2015 verabschiedete IT-Sicherheitsgesetz, geht es um Anlagen und Produktionen im operativen Betrieb.

Das Konzept des Schutz-Levels gibt hier einen Rahmen und eine Methode, um die Konformität zur Norm IEC 62443 zu bewerten. Sie kombiniert die Bewertung der technischen Security-Funktionen und -Eigenschaften der Automatisierungslösung mit der Bewertung der organisatorischen Betriebs- und Wartungsprozesse. Dabei ist besonders wichtig, dass man alle relevanten Dimensionen der Industrial Security behandelt, weil potenzielle Angreifer immer versuchen werden, die schwächste Stelle auszunutzen. So wie die Stärke einer Kette durch das schwächste Glied bestimmt wird, so ist die Effizienz eines Schutz-Konzepts durch die schwächste, möglicherweise fehlende Maßnahme bestimmt. Da die Dokumente der IEC 62443 seit mehreren Jahren durch viele Experten bearbeitet wurden, kann man davon ausgehen, dass sowohl die organisatorischen Vorgaben der Teile 2-1 und 2-4 als auch die funktionalen Anforderungen des Teils 3-3 alle Dimensionen abdecken, die für die Industrial Security relevant sind. Eine Konformitätsbewertung, die alle Anforderungen dieser drei Dokumente einschließt, würde eventuelle Lücken in dem Schutzkonzept aufdecken.

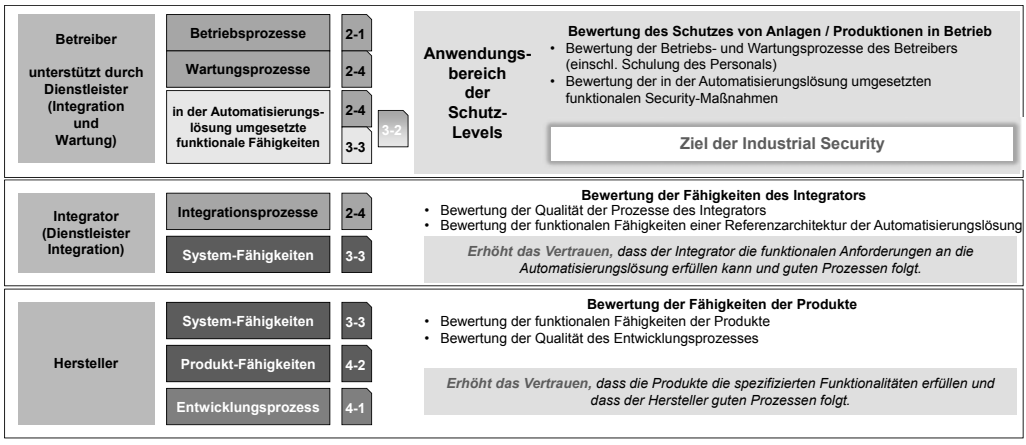

Bild 10 Anwendungsbereich der Schutz-Levels

Organisatorische und funktionale Maßnahmen müssen zusammen bewertet werden

Die Security-Funktionen und -Eigenschaften der Automatisierungslösung liefern einen wichtigen Beitrag zum Schutz gegen Cyberangriffe. Die Norm hat sich in der Bewertung und Differenzierung mit den Security-Levels bisher auf diesen Anteil beschränkt. Betrachtet man den Schutz einer Anlage im operativen Betrieb ist dies jedoch nicht ausreichend. Die Betriebs- und die Wartungsprozesse des Betreibers beeinflussen maßgeblich den Schutz, wie es an folgendem Bespiel verdeutlicht wird. Es wird angenommen, dass der Integrator die Automatisierungslösung so ausgelegt hat, dass eine leistungsfähige Verwaltung der Anwender mit starken Passwörtern und eine rollenbasierte Beschränkung der Aktionen der Anwender auf das minimal Notwendige gegeben ist. Bezüglich dieser Dimension der Industrial Security bietet die Automatisierungslösung die Möglichkeit, einen guten Schutz zu realisieren. Dieser Schutz kann aber zunichte gemacht werden, wenn z. B. der Betreiber nicht die Passwörter vertraulich behandelt oder regelmäßig ändert. Der Betreiber muss auch stetig die Anwender verwalten. Eine oft vorgefundene Schwachstelle liegt darin, dass die Accounts von Personen, die die Firma verlassen haben, nach wie vor aktiv sind, weil kein gezieltes Löschen stattgefunden hat. Ein ehemaliger, verärgerter Mitarbeiter kann sich zu einem potenziellen Angreifer entwickeln, der besonders gefährlich sein kann, wenn er etwa Administratorrechte hatte. Insofern ist die Definition der Security-Levels nach Teil 3-3, die im Abschnitt 4 dargestellt wurden, nicht ganz zutreffend, weil sie sich nur auf die Security-Funktionen und -Eigenschaften der Automatisierungslösung bezieht. Eine korrekte Definition wäre gegeben, wenn der Ausdruck „Schutz gegen…“ durch den Ausdruck „Fähigkeit zum Schutz gegen…“ ersetzt wäre. Der Schutz bezüglich einer bestimmten Dimension der Industrial Security ist nur dann gegeben, wenn auf der einen Seite die Automatisierungslösung die technischen Funktionen und Eigenschaften bietet und auf der anderen Seite diese im Betrieb und während der Wartung durch entsprechende Prozesse sicher eingesetzt werden. Der sichere Umgang mit den Security-Funktionen und -Eigenschaften der Automatisierungslösung ist in den Betriebs- und Wartungsprozessen festzulegen und deren Einhaltung durch das verantwortliche Personal während der gesamten Betriebsphase ist sicherzustellen.

Eine sinnvolle Bewertung der Schutz-Levels ergibt sich, wenn die funktionalen Maßnahmen und die dazugehörigen organisatorischen Maßnahmen in inhaltlich homogenen Clustern zusammengefasst sind. Eine Gruppe könnte beispielsweise alle Maßnahmen beinhalten, die das Verwalten und die Zugriffskontrolle der Anwender betreffen. Zu den organisatorischen Maßnahmen des Betreibers gehören unter anderem eine Richtlinie und ein Prozess, die die Anmeldung an das System regeln. Beschrieben werden muss, wie die Anmeldemechanismen erfolgen sollen, die Passwortlänge und -komplexität, der Erneuerungsabstand oder das vertrauliche Behandeln der Passwörter. Weiter ist zu beschreiben, welche Rollen innerhalb der Organisation auf die Automatisierungsanlage zugreifen dürfen, welche Aktionen sie ausführen dürfen und welche Beschränkungen sie haben müssen nach dem Prinzip der minimalen Rechte. Weiterer Bestandteil ist eine Prozedur zur Zuordnung von Personen zu den Rollen und der Pflege der gültigen Accounts. Es ist besonders wichtig, die Accounts immer auf dem aktuellen Stand zu halten, um zu vermeiden, dass z. B. Mitarbeiter, die die Firma verlassen haben, immer noch über einen gültigen Zugriff zu der Anlage verfügen. Weitere organisatorische

Maßnahmen adressieren insbesondere die Rolle des Integrators oder des Wartungsverantwortlichen. Hier ist besonders darauf zu achten, dass die Prozesse ein Löschen der temporär angelegten Accounts nach der Integration und Inbetriebnahme sicherstellen. Wichtig ist auch, dass der Integrator die System-Accounts, die bei der Auslieferung der Produkte mit Default-Passwörtern versehen sind, entsprechend der Passwort-Richtlinie des Betreibers schützt. Zu den funktionalen Maßnahmen gehören z. B. das Konfigurieren der Anmeldemechanismen mit Passwortmindestlänge und -komplexität oder Multifaktor-Authentifizierung. Weiter ist das Einrichten der erlaubten Rollen mit deren Rechten und Einschränkungen vorzunehmen. Funktionale Maßnahmen könnten auch der Aufbau einer PKI-Infrastruktur oder das Bereitstellen einer Station zur Verwaltung der gültigen Accounts beinhalten.

Die Bewertung der Maßnahmen eines ganzheitlichen Schutzkonzepts kann sinnvoll auf der Norm IEC 62443 basieren. Anforderungen zu organisatorischen Maßnahmen des Betreibers werden im Teil 2-1 bzw. ISO/IEC 27001 spezifiziert. Teil 2-4 adressiert die organisatorischen Maßnahmen des Integrators und des Wartungsverantwortlichen. Die in der Automatisierungslösung realisierten funktionalen Maßnahmen können anhand der Anforderungen des Teils 3-3 bewertet werden. Wie bereits erwähnt sollte man die zusammengehörigen funktionalen und organisatorischen Maßnahmen in Clustern zusammenfassen und gemeinsam bewerten.

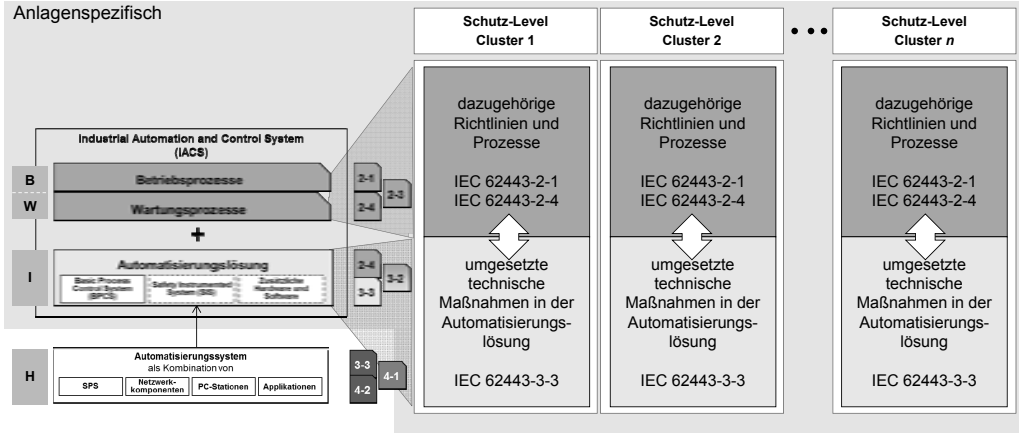

Bild 11 Aufteilung der Schutz-Level in Clustern

Welche Gruppierungen gewählt werden, hängt von verschiedenen Gesichtspunkten ab. Auf der einen Seite ist die Aussagekraft besser, wenn inhaltlich sehr homogene Cluster gebildet werden. Die Industrial Security ist jedoch sehr vielfältig und die verschiedenen Dimensionen sind oft unabhängig voneinander. Würde man nur die Homogenität zum Ziel haben, würde man auf zu viele Gruppen kommen. Die Handhabung vieler Schutz-Levels kann dann problematisch werden. Es muss die richtige Balance gefunden werden zwischen Homogenität (und dadurch Aussagekraft) der Cluster und Begrenzung der Anzahl zur besseren Handhabbarkeit. Wichtig ist bei dieser Überlegung, dass alle Anforderungen sowohl des Teils 2-1 bzw. ISO/IEC 27001 als auch des Teils 2-4 und des Teils 3-3 in den gewählten Clustern abgebildet werden.

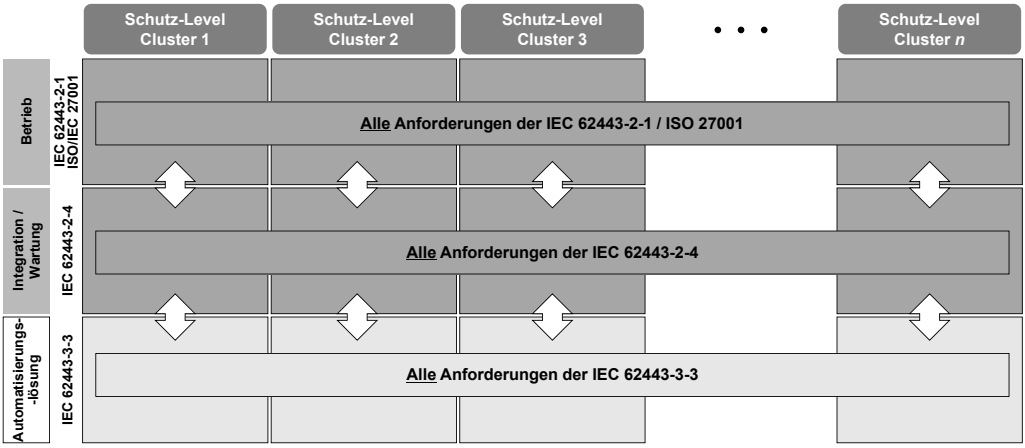

Bild 12 Alle Anforderungen müssen in den Clustern abgebildet werden.

Schutz-Levels werden über eine Matrix ermittelt

Wie könnte man in einer Bewertung sowohl organisatorische als auch funktionale Maßnahmen einschließen? Zu den funktionalen Maßnahmen hat die Norm bereits eine Einstufung in Form der Security-Levels vorgenommen. Man kann die Anforderungen des Teils 3-3 als Basis nehmen, um die in einer Anlage umgesetzten Security-Funktionen und -Fähigkeiten der Automatisierungslösung zu bewerten und zu unterscheiden zwischen potenziellen Schutz gegen ungewollten Missbrauch (SL 1) bzw. Angreifern unterschiedlicher Motivation, mit unterschiedlichen Kompetenzen und Ressourcen (SL 2 bis SL 4). Es geht hier um die im vorhergehenden Abschnitt bezeichneten „erreichten Security-Levels" (*Achieved, SL-A*). Falls die eingesetzten Produkte und Systeme nicht die ausreichenden funktionalen Fähigkeiten bieten, um den Ziel-Security-Level zu erreichen, müsste unter Umständen der Integrator kompensierende Maßnahmen vornehmen. Diese sind oft technischer Art, es können aber auch organisatorische Maßnahmen sein. Es liegt auf der Hand, dass solche organisatorischen Maßnahmen nur dann als Beitrag zur Erreichung des Security-Levels herangezogen werden können, wenn deren Umsetzung stets sichergestellt ist, was einen hohen Reifegrad voraussetzt.

Bei der Bewertung der organisatorischen Maßnahmen basierend auf Teil 2-1 bzw. ISO/IEC 27001 und Teil 2-4 kann man sich nicht auf eine Differenzierung wie bei den Security-Levels stützen. Die Norm differenziert nicht die Prozessstärke nach Levels. Die im Rahmen eines ganzheitlichen Schutzkonzepts eingesetzten organisatorischen und die funktionalen Maßnahmen müssen zusammenpassen.

Das Beispiel der Identifizierung und Authentifizierung von menschlichen Nutzern soll dies verdeutlichen. Die funktionale Anforderung zu diesem Thema wird im Teil 3-3 in dem Punkt SR 1.1 „Identifizierung und Authentifizierung von menschlichen Nutzern" behandelt.

Die Basisanforderung wird dem Security-Level 1 zugeordnet und wird wie folgt formuliert:

- Das Automatisierungssystem muss die Fähigkeit haben, alle menschlichen Nutzer zu identifizieren und zu authentifizieren. Diese Fähigkeit muss an allen Schnittstellen, die

menschlichen Nutzern Zugang zum Automatisierungssystem gewähren, die Identifizierung und Authentifizierung durchsetzen, sodass die Trennung von Aufgaben und das Prinzip der minimal erforderlichen Rechte gemäß den anzuwendenden IT-Sicherheitsleitlinien und -Vorgehensweisen unterstützt wird.

Diese Anforderung wird erfüllt, wenn eine Identifizierung und Authentisierung von Gruppen erfolgt. Die Nutzer einer Gruppe nutzen den gleichen Account.

Die erste Steigerung von SR 1.1 ist dem Security-Level 2 zugeordnet und lautet:

- Eindeutige Identifizierung und Authentifizierung: Das Automatisierungssystem muss die Fähigkeit haben, alle menschlichen Nutzer eindeutig zu identifizieren und zu authentifizieren.

Für jeden Nutzer der Automatisierungslösung muss ein eigener Account eingerichtet werden. Das Account-Management der Automatisierungslösung muss die Zuweisung der individuellen Accounts auf die jeweiligen Rollen mit ihren Rechten und Einschränkungen erlauben.

Die weitere Steigerung (SL 3) betrifft die Stärke des Authentifizierungsmechanismus:

- Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze: Das Automatisierungssystem muss die Fähigkeit haben, eine Multifaktor-Authentifizierung für den Zugriff menschlicher Nutzer auf das Automatisierungssystem über ein nicht vertrauenswürdiges Netz einzusetzen.

Allgemein werden als nicht vertrauenswürdig alle Netze betrachtet, die außerhalb der Automatisierungslösung sind. Dies betrifft in der Regel auch das Büronetz innerhalb der betreibenden Firma. Die Authentisierung mit einem elektronischen Ausweis und die Eingabe eines Codes ist eine typische Multifaktor-Authentifizierung. Jeder Zugriff von außen muss über ein solches Einloggen erfolgen.

Die letzte Steigerung von SR 1.1 ist dem Security-Level 4 zugeordnet und lautet:

- Multifaktor-Authentifizierung über alle Netze: Das Automatisierungssystem muss die Fähigkeit haben, eine Multifaktor-Authentifizierung für den Zugriff aller menschlichen Nutzer auf das Automatisierungssystem zu verwenden.

Um den Security-Level 4 zu erreichen, muss jeder Zugriff auf die Automatisierungslösung, z. B. auch von einem Bedienpanel, das sich in dem internen Netzwerk der Automatisierungslösung befindet, mit einer Multifaktor-Authentifizierung erfolgen. Diese Anforderung ist auch unter dem Gesichtspunkt zu betrachten, dass damit eventuell der Umgang mit der Automatisierungslösung schwerfälliger wird.

Die Prozesse, die die Identifizierung und Authentifizierung und allgemein die Anwenderverwaltung festlegen, müssen bestimmen, welche Maßnahmen und welcher Security-Level in der Automatisierungslösung umgesetzt werden müssen. Zu unserem Beispiel findet man in der ISO/IEC 27001 die Anforderung:

- Eine Zugangssteuerungsrichtlinie ist auf Grundlage der geschäftlichen und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft.

Der Inhalt der Zugangssteuerungsrichtlinie wird nicht vorgeschrieben. Soll jedoch etwa das Schutzkonzept dem Level 3 entsprechen, muss in der Zugangssteuerungsrichtlinie gefordert werden, dass die Zugänge über unsichere Netze nur mit Multifaktor-Authentifizierung zu erfolgen haben, und die Automatisierungslösung muss funktional entsprechend aufgebaut werden (Security-Level 3). Wäre ein Level 2 ausreichend, dann würde in der Zugangssteuerungsrichtlinie lediglich die eindeutige Identifizierung und Authentifizierung der Anwender gefordert sein. Eine Abstufung der Prozesse in Levels nach deren Inhalt ist daher nicht sinnvoll, denn diese werden durch die geschäftlichen und sicherheitsrelevanten Anforderungen gegeben. Vielmehr kommt es darauf an, ob die Prozesse auch aktiv durch das Personal umgesetzt werden. Beschreibt beispielsweise die Zugangssteuerungsrichtlinie, dass die Passwörter eine Mindestkomplexität haben müssen und wird diese Regelung nicht umgesetzt, hat man damit eine potenzielle Angriffsfläche geschaffen.

Im Vergleich zu den umgesetzten funktionalen Maßnahmen ist es für organisatorische Maßnahmen wichtig, dass die Umsetzung durch das Personal sichergestellt sein muss. Das setzt voraus, dass die Prozesse dokumentiert sind und das Personal informiert bzw. geschult ist. Eine Kontrolle der Umsetzung ist oft sehr sinnvoll. Nur wenn dieser Zustand erreicht ist, können organisatorische Maßnahmen ihren Beitrag im Rahmen eines ganzheitlichen Schutzkonzepts leisten. Man bewertet in der Regel, die Fähigkeit einer Organisation, Prozesse aktiv zu „leben“ mit dem Reifegrad nach dem sog. „*Capability Maturity Model Integration* (*CMMI*)“. Das Modell unterscheidet fünf Reifegrade, die wir im Weiteren mit der Abkürzung ML (*Maturity Level*) bezeichnen werden:

1. Initial: Keine Anforderungen an die Organisation. Diesen Reifegrad hat jede Organisation automatisch.
2. Managed: Die Projekte werden durch Prozesse geführt. Ein ähnliches Projekt kann erfolgreich wiederholt werden.
3. Defined: Die Projekte werden nach einem angepassten Standardprozess durchgeführt und es gibt eine organisationsweite Kontrolle der Umsetzung der Prozesse.
4. Quantitatively Managed: Es wird eine statistische Prozesskontrolle durchgeführt.
5. Optimizing: Die Arbeit und Arbeitsweise werden mithilfe einer statistischen Prozesskontrolle verbessert.

In der Norm 62443 hat man in Anlehnung an das CMMI-Modell vier Reifegrade definiert. Man hat dabei im Wesentlichen die Levels vier und fünf in einem zusammengefasst:

1. ML 1, Initial: Die Prozesse sind ad-hoc, schwach kontrolliert und nicht voraussagbar.
2. ML 2, Managed: Es werden Prozesse reaktiv gelebt.
3. ML 3, Defined: Die Prozesse sind beschrieben und werden proaktiv umgesetzt.
4. ML 4, Optimized: Die Prozesse werden bewertet, kontrolliert und kontinuierlich verbessert.

Kombiniert man die Bewertung der umgesetzten funktionalen Maßnahmen der Automatisierungslösung nach Security-Level (SL 1 bis SL 4) und den Reifegrad bei der Umsetzung der dazugehörigen organisatorischen Maßnahmen (ML 1 bis ML 4) in einer zweidimensionalen Matrix, dann kann man jedem Feld der Matrix einen Schutz-Level zuordnen. Die Fähigkeit

zu Schutz entspricht bei den Schutz-Levels einem tatsächlichen Schutz, der durch die Ergänzung der funktionalen Maßnahmen durch die dazugehörigen organisatorischen Maßnahmen erreicht werden kann. Daher kann man für die Schutz-Levels die in der Norm enthaltene Definition der Security-Levels übernehmen. Wir werden für die Schutz-Levels die Abkürzung PL (*Protection Levels*) verwenden:

- PL 1: Schutz gegen ungewollten, zufälligen Missbrauch,
- PL 2: Schutz gegen gewollten Missbrauch unter Verwendung von einfachen Mitteln, mit niedrigem Aufwand, allgemeinen Kompetenzen und niedriger Motivation,
- PL 3: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit moderatem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und moderater Motivation,
- PL 4: Schutz gegen gewollten Missbrauch unter Verwendung von technisch ausgefeilten Mitteln, mit erheblichem Aufwand, automatisierungstechnisch spezifischen Kompetenzen und hoher Motivation.

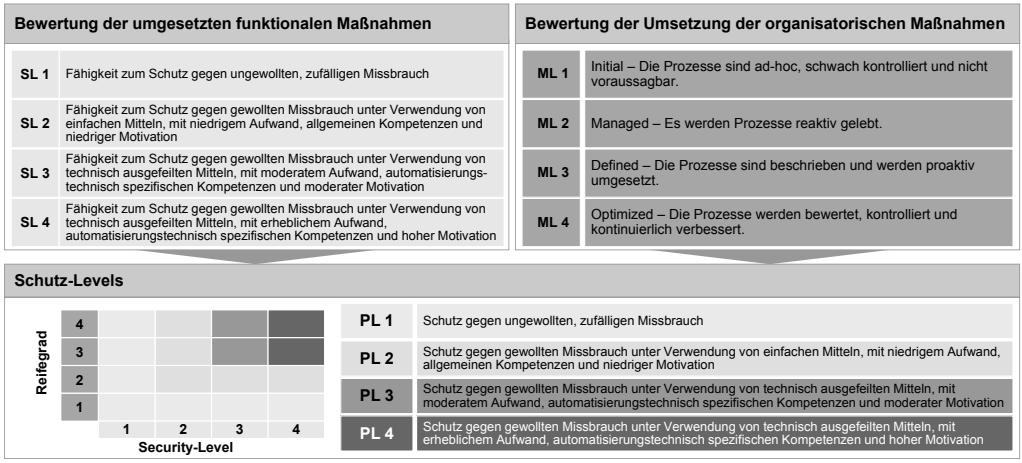

Bild 13 Bewertung von funktionalen und organisatorischen Maßnahmen in Schutz-Levels

Eine neu gegründete Standardisierungs-Arbeitsgruppe, soll die hier beschriebenen Konzepte in einem Normdokument festhalten. Die Zuordnung der Schutz-Levels zu den Kombinationen Reifegrad / Security-Level ist zum jetzigen Zeitpunkt[1)] noch nicht erfolgt. Der Arbeitsgruppe liegt der im Folgenden beschriebene Vorschlag vor, der mit den Prinzipien einer Defense-in-Depth-Strategie in Einklang steht. Grundsätzlich kann ein Schutz-Level PL nicht höher sein als der Security-Level SL der Automatisierungsanlage. Ist jedoch der Reifegrad niedrig, so kann der Schutz-Level PL auch niedriger als der Security-Level SL sein. In dem Vorschlag ist bei ML 1 der Schutz-Level immer gleich PL 1, unabhängig vom Security-Level der Automatisierungslösung, was die Tatsache widerspiegelt, dass nicht vorhandene oder nicht nachweislich umgesetzte organisatorische Maßnahmen zu erheblichen Schwachstellen führen können. Bei ML 2 kann der Schutz-Level höchstens gleich PL 2 sein, falls der Security-Level

1) Frühjahr 2016

der Automatisierungslösung größer oder gleich SL 2 ist. Man hat berücksichtigt, dass der Schutz-Level geschwächt werden kann, wenn die Umsetzung der organisatorischen Maßnahmen nicht nachhaltig bewiesen ist. Bei ML 3 und ML 4 entsprechen die Schutz-Levels PL den Security-Levels SL, was auf der Tatsache basiert, dass die organisatorischen Maßnahmen beschrieben und nachweislich umgesetzt werden müssen, um wirksam im Rahmen eines ganzheitlichen Schutzkonzepts ihren Beitrag zu leisten. Daraus folgt, dass bei einem gegebenen Security-Level der Automatisierungslösung der entsprechende Schutz-Level erst dann erreicht wird, wenn der Reifegrad beim Umsetzen der organisatorischen Maßnahmen wenigstens gleich ML 3 sein muss.

Gruppierung der Maßnahmen in Cluster

Wie bereits erwähnt, sind bei der Festlegung der Gruppierungen von zusammengehörenden Maßnahmen zum Teil gegenläufige Gesichtspunkte zu berücksichtigen. Auf der einen Seite ergeben möglichst homogene Cluster eindeutigere Aussagen zu dem Schutz-Level bezüglich des jeweiligen Clusters. Ginge man nur nach diesem Kriterium, würde es aufgrund der vielfältigen, oft unabhängigen Dimensionen der Industrial Security zu einer großen Zahl von Clustern führen. Man würde viele Schutz-Levels ermitteln, was wahrscheinlich zu einer komplexen Handhabung führen würde. In dem hier beschriebenen Ansatz hat man sich auf fünf Cluster festgelegt, die aus Sicht des Betreibers die wesentlichen Schwerpunkte für ein ganzheitliches Schutzkonzept bilden:

- **Cluster 1 – Abgesicherter physischer Zugang:** beinhaltet alle Security-Maßnahmen, um den physischen Zugang zu schützen und zu steuern;
- **Cluster 2 – Organisation der Security:** beinhaltet alle Security-Maßnahmen, um die IT-Sicherheit der Anlage zu organisieren;
- **Cluster 3 – Security im Design der Lösung:** beinhaltet alle Security-Maßnahmen, um den Schutz der Automatisierungslösung auszulegen;
- **Cluster 4 – Security während des Betriebs:** beinhaltet alle Security-Maßnahmen, um den sicheren Betrieb der Automatisierungslösung sicherzustellen;
- **Cluster 5 – Security während der Wartung:** beinhaltet alle Security-Maßnahmen, um die sichere Wartung der Automatisierungslösung sicherzustellen.

Um die jeweiligen Schutz-Levels pro Cluster zu ermitteln, wird jede Anforderung der drei Dokumente einem oder mehreren Clustern zugeordnet. Folgende Beispiele sollen dies verdeutlichen:

- *IEC 62443-3-3: SR 1.1 Identifizierung und Authentifizierung von menschlichen Nutzern: „Das Automatisierungssystem muss die Fähigkeit haben, alle menschlichen Nutzer zu identifizieren und zu authentifizieren."*

  Diese Anforderung ist relevant für die Auslegung der Automatisierungslösung, den Betrieb und die Wartung. Sie betrifft weder den physischen Schutz noch die Organisation der Security. Somit wird die Erfüllung der Anforderung zur Bewertung des Schutz-Levels der Cluster 3, 4 und 5 mitgezählt, jedoch nicht für die Cluster 1 und 2.

- *ISO/IEC 27001: A.12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen: „Entwicklungs-, Test- und Betriebsumgebungen sind voneinander getrennt, um das Risiko unbefugter Zugriffe auf oder Änderungen an der Betriebsumgebung zu verringern."*

  Diese Anforderung ist sowohl in der Organisation der IT-Sicherheit als auch bei der Auslegung der Automatisierungslösung, dem Betrieb und der Wartung zu berücksichtigen. Somit wird die Erfüllung der Anforderung zur Bewertung des Schutz-Levels der Cluster 2, 3, 4 und 5 mitgezählt, jedoch nicht für den Cluster 1.

- Beispiel 3, Anforderung aus der ISO/IEC 27001: *A.5.1.1 Informationssicherheitsrichtlinien: „Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht."*

  Diese Anforderung betrifft ausschließlich die Organisation der Security und trägt daher nur zur Bewertung des Clusters 2 bei.

Um die Schutz-Level zu ermitteln, wird die Erfüllung jeder Anforderungen der Teile 2-1 bzw. ISO/IEC 27001, 2-4 und 3-3 abgefragt und das jeweilige Ergebnis entsprechend der Zuordnung zu den jeweiligen Clustern mitgezählt. Falls Anforderungen für das betrachtete Projekt nicht relevant sind, zählen diese wie erfüllte Anforderungen. Die Dokumente wurden über Jahre durch viele Experten erarbeitet und in der Praxis verwendet. Daher kann man davon ausgehen, dass alle Dimensionen der Security, die in einem ganzheitlichen Schutzkonzept zu berücksichtigen sind, in den Dokumenten adressiert werden. Eine systematische Abfrage der Erfüllung der Anforderungen unterstützt das Aufdecken möglicher Lücken, die als schwächste Glieder der Verteidigungskette durch einen potenziellen Angreifer genutzt werden könnten.

Um der Vielfalt der Security Rechnung zu tragen, ist es sinnvoll Unterkategorien festzulegen, in denen jeweils ebenfalls ein Schutz-Level ermittelt werden kann. Die Abschnitte des Teils 3-3 fassen die funktionalen Anforderungen an die Automatisierungslösung thematisch in sog. grundlegenden Anforderungen (*Foundational Requirements – FR*) zusammen. In dem vorliegenden Vorschlag wurden diese Abschnitte für die Unterkategorien gewählt. Da diese sich ausschließlich mit der Automatisierungslösung befassen, sind der physische Zugang und die Organisation hinzuzufügen. Daher ergeben sich folgende neun Unterkategorien:

- physischer Zugang
- Organisation
- Identifizierung und Authentifizierung (FR 1)
- Nutzungskontrolle (FR 2)
- Systemintegrität (FR 3)
- Vertraulichkeit der Daten (FR 4)
- eingeschränkter Datenfluss (FR 5)
- rechtzeitige Reaktion auf Ereignisse (FR 6)
- Ressourcenverfügbarkeit (FR 7)

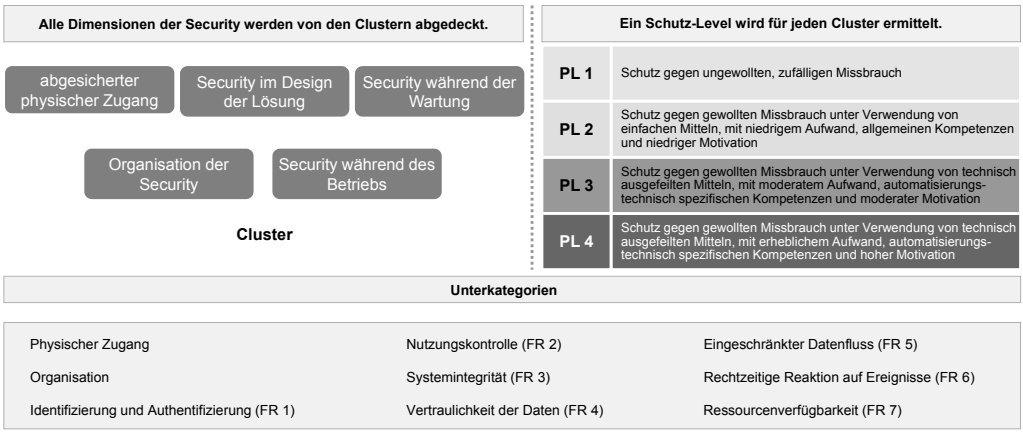

Bild 14 Schutz-Level nach Cluster und Unterkategorien

Im Abschnitt 4 haben wir die Aktivitäten in dem IACS-Lebenszyklus beschrieben. In der Spezifikationsphase sollten PDCA-Zyklen des Betreibers dazu führen, dass die zu erreichenden Levels der Schutzmaßnahmen unter Berücksichtigung der Kritikalität der Anlage festgelegt werden. Durch die systematische Analyse der Erfüllung jeder einzelnen Anforderung erkennt man die Lücken und Schwachstellen und kann die Maßnahmen zu ihrer Behebung festlegen. Mit der beschriebenen Vorgehensweise können die aktuellen erreichten Schutz-Levels ermittelt werden, die im Vergleich mit den zu erreichenden Levels der Schutzmaßnahmen dargestellt werden können.

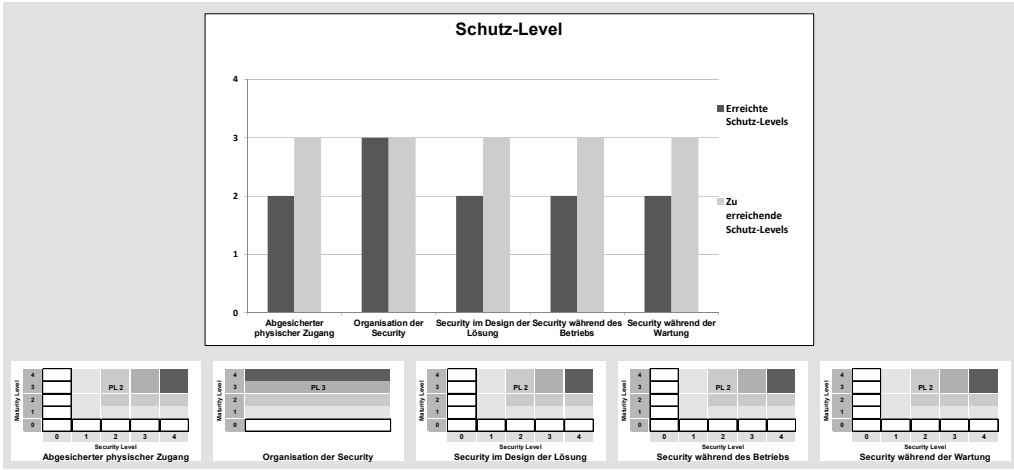

Bild 15 Zu erreichende Levels und erreichte Levels der Schutzmaßnahmen

6 Vorgehensweise zum Aufbau eines Schutzkonzepts

Bei der Etablierung von Sicherheitskonzepten sieht die Situation im Automatisierungsumfeld zum Teil anders aus als im Büroumfeld. Automatisierungsnetze abzusichern stellt eine große Herausforderung dar, weil dies mit anderen wichtigen Anforderungen wie Leistungsfähigkeit, Verfügbarkeit und Benutzerfreundlichkeit kollidiert. Hinzu kommt, dass die Absicherung eines Netzwerks oder Anlage ständige Aufmerksamkeit und Anpassungen erfordert und es nicht mit dem einmaligen Einrichten getan ist, wie es ansonsten beim Aufbau eines Automatisierungssystems üblich ist. Auch nach der Abnahme müssen Bedrohungen bewertet und ggf. mit Anpassungen und Updates reagiert werden, damit die Anlage auch sicher bleibt.

In dem vorliegenden Abschnitt wird eine Vorgehensweise beschrieben, die auf den Konzepten der IEC 62443 basiert. Fortschrittliche Firmen setzen bereits erfolgreich diese Konzepte um, etwa das Industrial Security Konzept von Siemens [13]. Das Ziel ist, die Risiken aus den Bedrohungen und Gefährdungen, denen industrielle Automatisierungsnetze ausgesetzt werden, zu minimieren und auch unter wirtschaftlichen Gesichtspunkten einen vertretbaren Schutz zu erreichen. Um für den Leser möglichst konkrete Lösungsvorschläge zu zeigen, wurde auf die in [13] dargestellten Beispiele zurückgegriffen.

6.1 Überblick

Wenn es um den Schutz der eigenen Anlagen geht, ist es wichtig, ein vernünftiges Bewusstsein für die Risiken zu haben. Es ist jedoch ebenso wichtig, ein gesundes Vertrauen in die eigenen Sicherheitsvorkehrungen und die Zuverlässigkeit der Mitarbeiter setzen zu können. Zu wenig Sicherheit ist fahrlässig, zu viel Sicherheit ist unwirtschaftlich. In diesem Spannungsfeld sollte man mit dem richtigen Augenmaß bedarfsgerechte und angepasste Maßnahmen für industrielle Anlagen implementieren.

Die Herausforderung besteht darin, Gefahrenpotenziale signifikant zu minimieren und hinreichende, aber auch bezahlbare Sicherheit in der industriellen Automation zu erreichen. Eine Standardlösung, die immer anwendbar ist, gibt es leider nicht, da jede Anlage individuelle Randbedingungen, Gefährdungen und Schutzziele besitzt. Aber es gibt bewährte Vorgehensweisen bzw. eine überschaubare Anzahl von denkbaren Maßnahmen für ein effizientes Schutzkonzept, die betrachtet werden müssen. Wir haben gesehen, dass einzelne Sicherheitsmaßnahmen alleine immer lückenhaft und damit unzureichend sind. Eine einzelne Maßnahme kann leichter umgangen werden, als mehrere in Reihe. Hinzu kommt, dass vielfältigen Bedrohungen auch mit unterschiedlichen Maßnahmen entgegen getreten werden muss. Beispielsweise können Viren nicht effektiv mit Firewalls bekämpft werden und Zugriffsverletzungen nicht mit Virenscannern.

Das im Abschnitt 4.1 beschriebene Konzept der tiefgestaffelten Verteidigung (Defense-in-Depth) hat auch gezeigt, dass technische Schutzmaßnahmen allein nicht alle Schutzziele abdecken können, so dass begleitende und unterstützende organisatorische Maßnahmen unerlässlich sind. Somit kann nur ein Gesamtkonzept alle Risiken minimieren und wirkungsvollen Schutz bieten. Das Konzept soll eine Automatisierungsanlage sowohl rundum als auch in der Tiefe schützen. Das bedeutet einerseits, dass verschiedene sich ergänzende Schutzmechanismen vorhanden sind, um den unterschiedlichen Bedrohungen begegnen zu können (Rundumschutz), und andererseits, dass es mehrere Barrieren gibt, die von einem potenziellen Angreifer überwunden werden müssen.

Das Konzept beinhaltet als wesentliche Komponenten Anlagensicherheit, Netzwerksicherheit und Systemintegrität (Bild 3). Die erforderlichen hier aufgezeigten Sicherheitsmaßnahmen sollen lückenlos ineinandergreifen, um einen umfassenden und verlässlichen Schutz einer Automatisierungsanlage zu erreichen.

Für den sicheren Betrieb einer Anlage können letztendlich nur die Betreiber sorgen, aber Hersteller wie beispielsweise Siemens können dabei unterstützen, indem entsprechende Beratungsleistung und sicherheitstechnisch gehärtete Produkte mit Security-Funktionen zur Verfügung gestellt werden, damit die Schutzkonzepte auch tatsächlich umgesetzt werden können.

6.2 Anlagensicherheit

Die Anlagensicherheit ist im Wesentlichen durch den Betreiber sicherzustellen. Sie schafft die Voraussetzungen, dass technische Maßnahmen der Security nicht anderweitig umgangen werden können. Dazu gehören physikalische Zugangsschutzmaßnahmen wie Zäune, Drehkreuze, Kameras oder Kartenlesegeräte sowie organisatorische Maßnahmen insbesondere ein Management-Prozess zur Security, der die Sicherheit einer Anlage auch dauerhaft gewährleistet.

Physikalischer Zugangsschutz

Eine Grundvoraussetzung für den Schutz einer Anlage ist, dass der Zugang zu der Automatisierungslösung nur für die autorisierten Personen gewährt wird. Der Betreiber muss Maßnahmen und Prozesse einführen, um den Zugang nicht autorisierter Personen zur Umgebung der Anlage zu verhindern. Insbesondere sind die physikalische Trennung unterschiedlicher Produktionsbereiche mit differenzierten Zugangsberechtigungen und der physikalische Zugangsschutz für kritische Automatisierungskomponente (z. B. durch sicher verschlossene Schaltschränke) sicherzustellen.

Die Richtlinien für Schutzmaßnahmen zum physikalische Zugang haben auch Einfluss darauf, welche Maßnahmen der Security erforderlich sind und in welcher Stärke. Wenn beispielsweise zu einem Bereich von vornherein nur ausgesuchte berechtigte Personen Zugang haben, müssen die Netzzugangsschnittstellen oder Automatisierungssysteme nicht im gleichen Maß abgesichert werden, wie es bei öffentlich zugänglichen Bereichen der Fall wäre.

Management der Security

Ein unerlässlicher Bestandteil der Anlagensicherheit sind organisatorische Maßnahmen und die Einführung von Prozessen zur Security. Organisatorische Maßnahmen müssen mit den technischen Maßnahmen eng verzahnt sein und bedingen sich gegenseitig. Die meisten Schutzziele lassen sich auch nur durch eine Kombination beider Arten von Maßnahmen erreichen.

Zu den organisatorischen Maßnahmen gehört die Etablierung eines Management-Prozesses zur Security. Um fundiert entscheiden zu können, welche Maßnahmen sinnvoll sind, ist zunächst zu analysieren, welche Risiken konkret bestehen, die nicht toleriert werden können. Der im Abschnitt 4.2 beschriebene PDCA-Zyklus nach der Richtlinie VDI 2182 bietet hierfür eine gute Unterstützung. Sowohl die Eintrittswahrscheinlichkeit eines Risikos als auch die mögliche Schadenshöhe spielen eine Rolle. Werden Risikoanalyse und Ermittlung der Schutzziele vernachlässigt oder gar nicht durchgeführt, ist die Gefahr groß, dass unpassende, zu teure oder wirkungslose Maßnahmen getroffen werden und manche Schwachstellen nicht erkannt und nicht behoben werden.

Aus der Risikoanalyse ergeben sich dann Schutzziele, die als Basis für konkrete, organisatorische als auch technische Maßnahmen dienen. Die Maßnahmen müssen nach der Implementierung überprüft werden. Wie im Abschnitt 4.4 beschrieben, müssen die Risiken von Zeit zu Zeit oder wenn sich Änderungen ergeben haben, erneut bewertet werden, da sich die Bedrohungslage mittlerweile geändert haben könnte. Dann beginnt der Prozess wieder von vorne.

6.3 Netzwerksicherheit

Das zentrale Element des industriellen Schutzkonzepts ist die Netzwerksicherheit. Sie ist in der Regel durch den Integrator sicherzustellen. Die Netzwerksicherheit beinhaltet den Schutz von Automatisierungsnetzen vor unbefugten Zugriffen und die Kontrolle aller Schnittstellen zu anderen Netzen, z. B. zum Büronetzwerk oder insbesondere den Fernwartungszugängen zum Internet. Zum Bereich der Netzwerksicherheit gehört darüber hinaus auch der Schutz der Kommunikation vor Abhören und Manipulation, d. h. die Verschlüsselung der Datenübertragung und Authentisierung der jeweiligen Kommunikationsteilnehmer.

Sicherung der Schnittstellen zwischen Unternehmens- und Anlagennetz

Übergänge zu anderen Netzwerken können mittels Firewalls und gegebenenfalls Aufbau einer DMZ überwacht und geschützt werden. Der Ausdruck DMZ steht für demilitarisierte Zone und bedeutet sicherheitstechnisch abgeschirmte Zone. Die DMZ dient zur Bereitstellung von Daten für andere Netze, ohne direkten Zugang zum Automatisierungsnetz gewähren zu müssen. Üblicherweise ist eine DMZ so ausgelegt, dass davon auch kein Zugriff oder Verbindungsaufbau in das Automatisierungsnetz möglich ist, d. h. also selbst wenn ein Rechner in der DMZ von einem Hacker übernommen worden ist, bleibt das Automatisierungsnetz weiterhin geschützt.

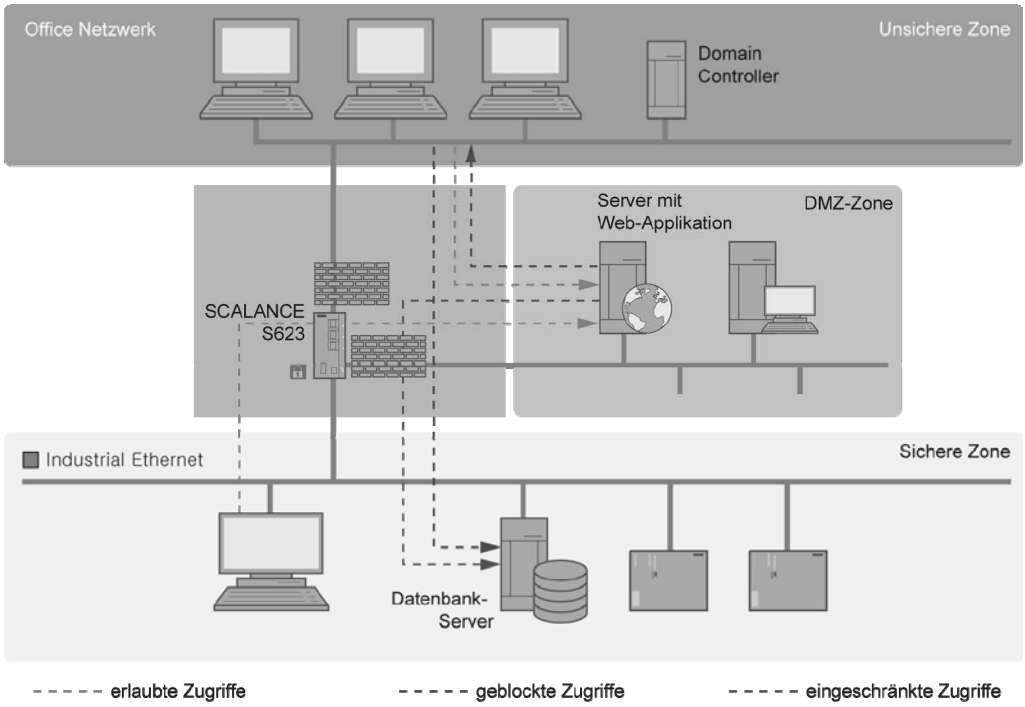

Bild 16 Einsatz einer „Demilitarisierten Zone" für den Datenaustausch zwischen Unternehmens- und Anlagennetz

Netzsegmentierung und Zellenschutzkonzept

Die sicherheitstechnische Segmentierung des Anlagennetzwerks in einzelne geschützte Automatisierungszellen dient der weiteren Risikominimierung und Erhöhung der Sicherheit. Dabei werden Teile eines Netzwerks, z. B. ein IP-Subnetz, von einer Security-Appliance geschützt und dadurch das Netz sicherheitstechnisch segmentiert. Somit können Geräte innerhalb dieser „Zelle" vor unbefugten Zugriffen von außen geschützt werden, ohne dabei die Echtzeitfähigkeit, Performance oder andere Funktionen zu beeinträchtigen.

Die Firewall kann nun den Zugriff auf die Zelle kontrollieren, wobei festgelegt werden kann, welche Netzteilnehmer miteinander und ggf. auch mit welchen Protokollen kommunizieren dürfen. Damit können nicht nur unbefugte Zugriffe unterbunden, sondern auch die Netz-Last reduziert werden, da nicht jede, sondern nur die gewollte und erforderliche Kommunikation passieren darf.

Die Aufteilung der Zellen und Zuordnung der Geräte erfolgt nach Kommunikations- und Schutzbedarf der Netzteilnehmer. Die Datenübertragung von und zu den Zellen kann zudem bei Bedarf mittels VPN von den Security Appliances verschlüsselt und so vor Datenspionage und Manipulation geschützt werden. Die Kommunikationsteilnehmer werden dabei authentifiziert und ggf. für die Zugriffe autorisiert. Beispielsweise kann mit den „Security Integrated"- Komponenten von Siemens wie den SCALANCE S Security Appliances oder den

Security CPs für das Automatisierungssystem das Zellenschutzkonzept umgesetzt und die Kommunikation gesichert werden.

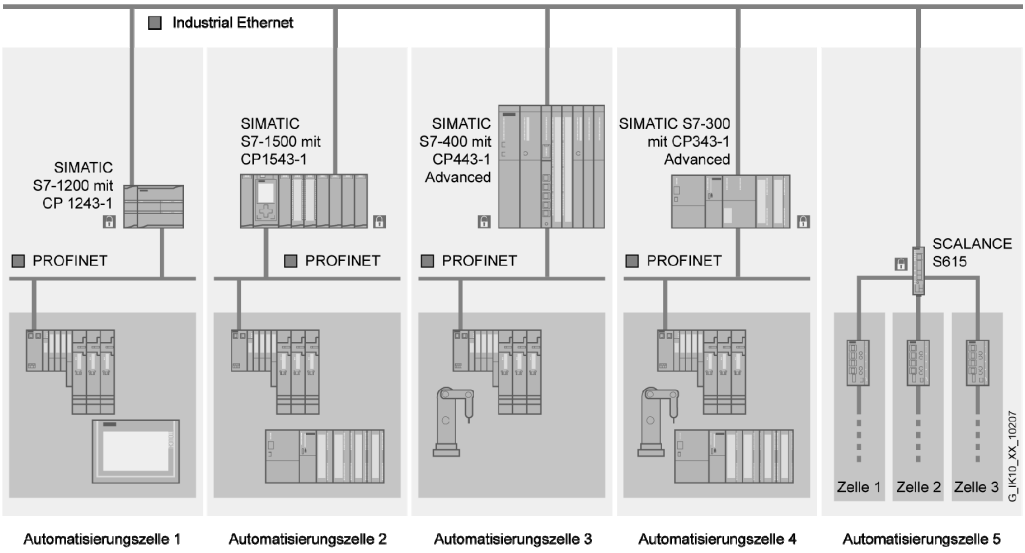

Bild 17 Netzsegmentierung und Zellenschutz mit Security Integrated Produkten (siehe Schloss-Symbol)

Sichere Fernzugriffe

Für Fernwartung oder Fernwirkungsanwendungen aber auch zur Überwachung von weltweit installierten Maschinen werden immer mehr Anlagen direkt über das Internet angebunden bzw. abgesetzte Anlagen über mobile Netze (GPRS, UMTS, LTE). Hier ist die Absicherung der Zugänge besonders wichtig. Mit Hilfe von Suchmaschinen, Portscannern oder automatischen Skripten können Hacker einfach und ohne großen Aufwand ungesicherte Zugänge finden. Hier gilt es die Authentifizierung der Kommunikationsteilnehmer, die Verschlüsselung der Datenübertragung und die Integrität der Daten sicherzustellen. Besonders dann, wenn es sich um Anlagen kritischer Infrastrukturen handelt. Das Eindringen unbefugter Personen, das Auslesen vertraulicher Daten und die Manipulation von Parametern oder von Steuerbefehlen können enormen Schaden anrichten, negative Auswirkungen auf die Umwelt haben und Menschen gefährden.

Als Schutzfunktionen haben sich hier besonders VPN-Mechanismen bewährt, die genau die Authentizität, Verschlüsselung und Schutz der Integrität zur Verfügung stellen. Die internetfähigen Security-Produkte von Siemens Industry unterstützen VPN und somit können Daten sicher über Internet oder mobile Netze übertragen und die Zugänge kontrolliert werden.

Bild 18 zeigt beispielsweise, wie Fernzugriffe mit Produkten von Siemens geschützt werden können. Normalerweise werden hierbei Geräte z. B. mittels Zertifikaten als vertrauenswürdige Kommunikationsteilnehmer authentifiziert und IP-Adressen oder DNS-Namen werden in den Firewall-Regeln verwendet, um Zugänge freizuschalten oder zu blockieren. Die VPN-Appliance und Firewall SCALANCE S bietet mit userspezifischen Firewall-Regeln darüber hinaus die Mög-

lichkeit, Zugriffsrechte auch an User zu binden. Hier loggen sich User an einem Webinterface mit Namen und Passwort ein und jedem berechtigten User wird ein spezieller Firewall-Regelsatz zugeordnet und er kann so gemäß seiner Rechte zugreifen. Der Vorteil ist hier, dass auch ganz klar nachvollzogen werden kann, wer zu einem bestimmten Zeitpunkt zugegriffen hat.

Die Variante SCALANCE S623 mit drei Firewall-Ports bietet zudem einen Ausweg aus einem Dilemma, den sich Systemintegratoren, OEMs und Endanwender oft gegenübersehen. Einerseits sollen Maschinenbauer zu Wartungszwecken in der Lage sein, auf ihre Maschinen beim Endanwender zuzugreifen, aber andererseits möchte die IT des Endanwenders nur ungern Firmenfremde in das Netzwerk lassen, in dem die Maschine steht. Mit dem SCALANCE S623 kann die Maschine mit dem Anlagennetzwerk verbunden werden und mit dem dritten Port der Firewall mit dem Internet. Damit kann der Zugriff vom Internet aus auf die Maschine erlaubt, aber der Zugriff vom Internet aus auf das Anlagennetzwerk unterbunden werden. Der Servicetechniker kann vom Internet Fernwartungszugriffe auf die Maschine durchführen, hat aber keinen direkten Zugang zum Anlagennetzwerk.

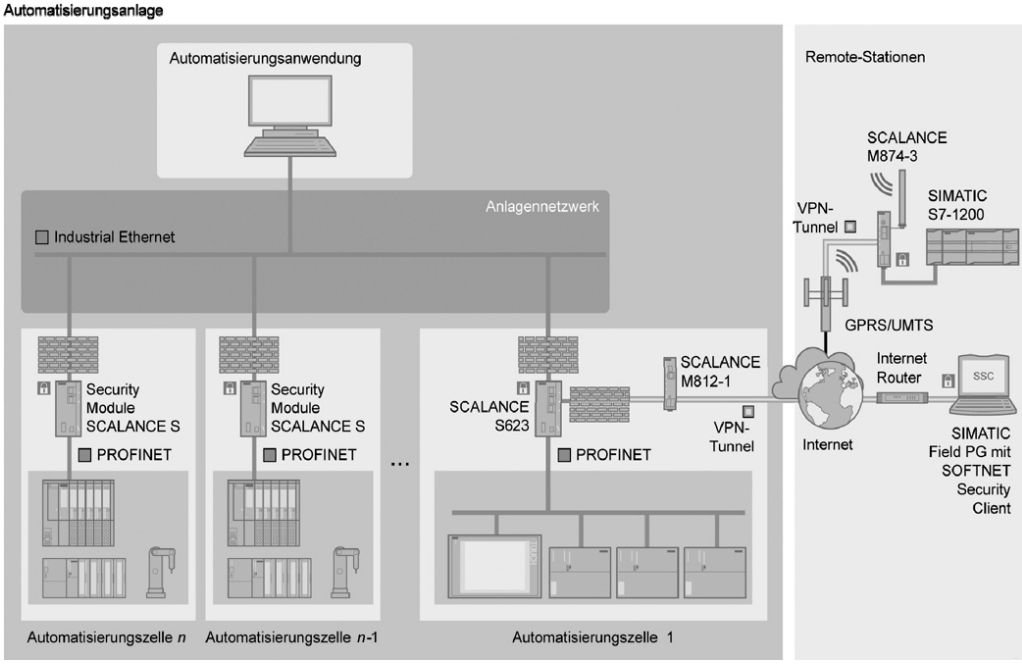

Bild 18 Sicherer Fernzugriff auf Anlagenteile ohne direkten Zugang zum Anlagennetzwerk mit 3-Port-Firewall

6.4 Systemintegrität

Als dritte tragende Säule eines ausgewogenen Schutzkonzepts ist die Sicherung der Systemintegrität zu sehen. Sie ist im Wesentlichen durch den Hersteller in den Eigenschaften der Produkte sicherzustellen. Hierbei sind Automatisierungssysteme und Steuerungskomponenten,

SCADA- und HMI-Systeme gemeint, die gegen unbefugte Zugriffe und Malware geschützt werden oder spezielle Anforderungen wie Know-how-Schutz erfüllen müssen.

Schutz PC-basierter Systeme im Anlagennetz

Ebenso wie PC-Systeme in Büros gegen Schadsoftware geschützt werden und entdeckte Schwachstellen im Betriebssystem oder in der Anwendersoftware durch Updates mit Patches geschlossen werden müssen, bedürfen auch industrielle PCs und PC-basierte Steuerungssysteme im Anlagennetz entsprechender Schutzmaßnahmen. Viele der im Büroumfeld bewährten Schutzsysteme können hier genauso eingesetzt werden, z. B. Virenscanner. Da Virenscanner nicht alle Viren erkennen können und gegen neue bis zur Aktualisierung der Pattern machtlos sind, sollten ggf. Alternativen überlegt werden – insbesondere da im Automatisierungsumfeld Software nicht immer zeitnah aktualisiert werden kann, wenn gerade kein Wartungsfenster zur Verfügung steht, z. B. bei 24/7-Betrieb.

Der Einsatz von sogenannter Whitelisting-Software ist eine Alternative zu Virenscannern. Whitelisting arbeitet mit Positivlisten, in denen der Benutzer festlegen kann, welche Prozesse bzw. Programme auf dem Rechner laufen dürfen. Versucht dann ein Benutzer oder eine Schadsoftware ein neues Programm zu installieren, so wird dies unterbunden und der Schaden verhindert. Siemens als Hersteller von Industriesoftware unterstützt hierbei den Anwender, indem Siemens die Software auf Verträglichkeit mit Virenscannern oder Whitelisting-Software testet.

Schutz der Steuerungsebene

Dass PCs und Netzwerke gegen Bedrohungen geschützt werden müssen, ist hinlänglich bekannt. Doch welche Maßnahmen kann man zum Schutz meist herstellerspezifischer, proprietärer Systeme ergreifen? Wie schützt man speicherprogrammierbare Steuerungen (SPS) und Bedienstationen, die entweder kein kommerzielles Betriebssystem oder eine ältere Version nutzen, da sie über viele Jahre und sogar Jahrzehnte im Einsatz sind? Sicherheitssoftware Dritter stellt hierfür in den meisten Fällen keine Lösung dar.

Der Zugriff auf die Systemfunktionen der Geräte ist meist gar nicht oder nur eingeschränkt möglich. Bei Sicherheitslösungen zum Schutz der Steuerungsebene sind die Hersteller von Automatisierungshardware gefragt, entsprechende Sicherheitsmechanismen zu implementieren und den Anwendern anlagenspezifische Einstellmöglichkeiten zur Verfügung zu stellen. Gleichzeitig sind die Anwender dazu aufgefordert, das Vorhandensein solcher Mechanismen bei den Herstellern zu hinterfragen und diese auch zu aktivieren, sofern dazu Einstellungsmöglichkeiten angeboten werden.

Der Schutz der Steuerungsebene richtet sich im Kern darauf, die Verfügbarkeit der Steuerungen im Feld zu gewährleisten, zielt aber auch darauf, geistiges Eigentum zu schützen, denn das Entwicklungs-Know-how bezüglich der Maschine stellt für jeden Maschinenbauer eine große Investition dar. Mit zunehmender Vernetzung und der Integration der IT-Welt in die Automatisierungstechnik verändern sich jedoch die Anforderungen an Zugriffsschutz und Manipulationssicherheit von Produktionsanlagen. Dieser ist für moderne Steuerungssysteme unumgänglich und beispielsweise in der neuen Steuerungsgeneration SIMATIC S7-1500 von Siemens bereits integriert. Werden z. B. die von Siemens-Steuerungen zur Verfügung gestellten

Funktionen wie Passwortschutz, Bausteinschutz oder Kopierschutz genutzt, ist ein weiterer essenzieller Baustein zur Absicherung des Anlagennetzwerks gelegt.

Hierbei können einzelne Funktionsbausteine geschützt werden, sodass Unbefugte keinen Zugriff auf deren Inhalt haben und somit Algorithmen nicht kopieren oder verändern können. Mit einem Kopierschutz, d. h. Verknüpfung von Programmteilen mit der Seriennummer der Speicherkarte, wird gleichzeitig die Vervielfältigung der Maschinen verhindert, sodass geschützte Programme nur in zulässigen Maschinen eingesetzt werden können. Diese Funktionen helfen jedem Maschinenbauer, seine Investition zu sichern und seinen technologischen Vorsprung zu behalten. Das in Bild 18 beschriebene Zellenschutzkonzept, welches bislang nur von speziellen Security Appliances realisiert werden konnte, wird von Siemens nun erweitert. Die Security-Funktionen Stateful Inspection Firewall und VPN werden in bestehende Hardware, den Kommunikationsprozessoren für S7-Steuerungen integriert. Verschlüsselte HTML-Seiten über Secure Sockets Layer (SSL), abhörsichere Übertragung von Netzwerkanalyseinformationen an das Netzwerkmanagementsystem (SNMP V3) komplettieren die Security-Funktionen der Kommunikationsprozessoren und stellen einen echten Mehrwert für die Anwender dar.

Die Kommunikationsprozessoren CP343-1 Advanced für die speicherprogrammierbaren Steuerungen Simatic S7-300 bzw. CP443-1 Advanced für die Simatic S7-400 und CP1543-1 für die S7-1500 werden dadurch zur „sicheren Schnittstelle“ hin zum gesamten Anlagennetzwerk und schützen die jeweils angebundenen Steuerungen, sowie die unterlagerten Netze und bei Bedarf auch die Kommunikation zwischen ihnen und ergänzen bzw. erweitern damit das Zellenschutzkonzept in einer Anlage.

Für den Schutz von PCs kommt die Ethernet-Karte CP1628 zum Einsatz, die ebenfalls mittels VPN und Firewall Industrie-PCs und die Kommunikation dahin schützen kann. Alle diese „Security Integrated“-Produkte sind kompatibel zueinander und können sichere VPN-Verbindungen zueinander aufbauen, sodass praktisch jeder Anlagenteil und alle Arten von Automatisierungskomponenten damit geschützt werden können.

6.5 Rollen- und Rechtekonzepte

Wir haben gesehen, dass zur Abwehr der unterschiedlichen Bedrohungen und auch um einen angemessenen Schutz erreichen zu können ein Verteidigungskonzept erforderlich ist, das mehrere Hürden für Angreifer aufbaut (Defense-in-Depth-Konzept). Das bedeutet aber gleichzeitig, dass auch berechtigte Personen diese Hürden überwinden müssen. In der Praxis gibt es normalerweise verschiedene Zugangsberechtigungen bzw. Klassen von Rechten. Bestimmte Anwender dürfen beispielsweise nur auf bestimmte Anlagenteile, Geräte oder Applikationen zugreifen, manche haben Administratorrechte, andere nur Lese- oder auch Schreibrechte.

Die Umsetzung eines Schutzkonzeptes dient also nicht nur der Abwehr von Angriffen, sondern auch der Umsetzung eines Rechte-Konzepts, d. h. sicherzustellen, dass ausschließlich berechtigte Personen und auch nur gemäß ihren jeweils zugeordneten Rechten zugreifen können. Üblicherweise wird nicht für jede Person ein eigenes Rechteprofil erstellt, sondern Rollen definiert, die bestimmte Rechte haben. Den Rollen werden nun Anwender bzw. Gruppen von Anwendern zugeteilt und somit ihre jeweils entsprechenden Zugriffsrechte zugewiesen. Ein wichtiger Aspekt im Zusammenhang mit Security ist daher auch die Anwender- oder Userverwaltung.

Eine durchgängige Projektierung für alle Automatisierungskomponenten erleichtert hier die Userverwaltung, da von zentraler Stelle aus Rollen und Rechte verschiedener Personen anlagenweit festgelegt und gepflegt werden können. Werkzeuge sollten dem Betreiber das Anlegen und die Pflege aller berechtigten Anwender der Automatisierungslösung erleichtern, beispielsweise die Userverwaltung im Engineering Framework TIA-Portal von Siemens.

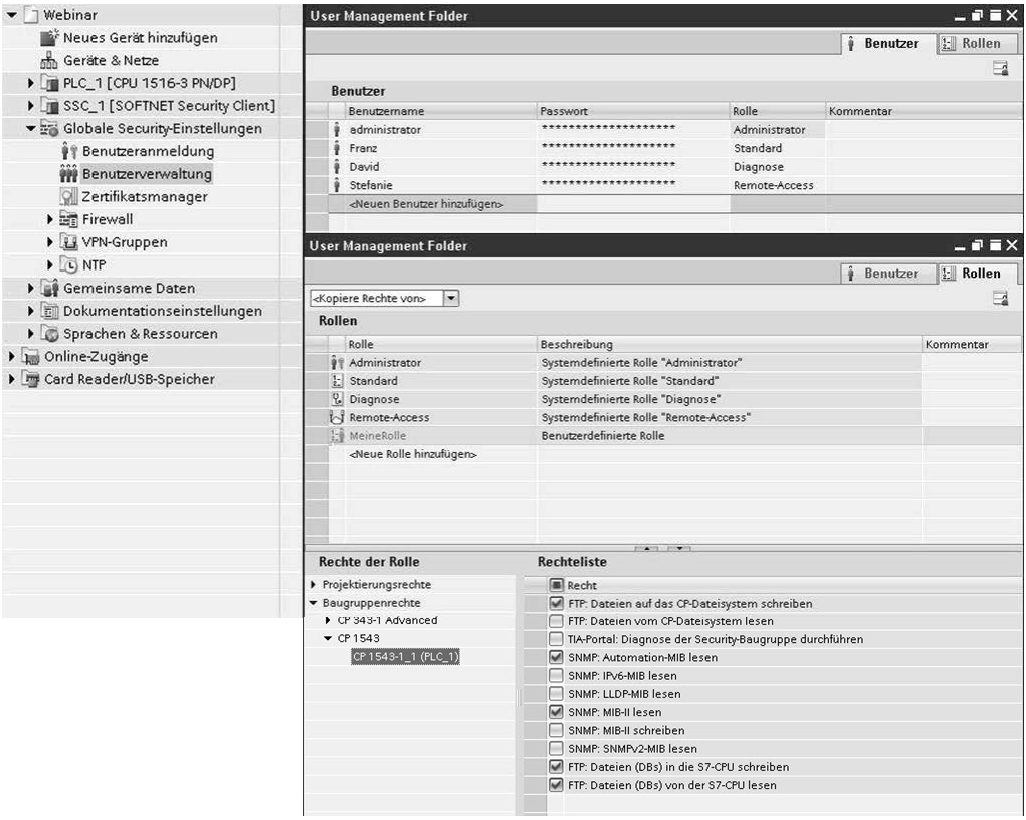

Bild 19 Usermanagement im TIA Portal mit Rollen- und Rechte-Vergabe

Anhang: Die IEC-62443-Dokumente im Einzelnen

In diesem Abschnitt sollen die Inhalte der verschiedenen Teile des Standards erklärt werden. Für jedes Dokument wird ein Überblick über Ziel, Struktur und wesentliche Inhalte gegeben.

A Wesentliche Dokumente zur Erstellung und Pflege eines Schutzkonzepts

A.1 IEC 62443-2-1 / ISO/IEC 27001

Das Dokument IEC 62443-2-1 spezifiziert die Anforderungen an die organisatorischen Maßnahmen zum sicheren Betrieb einer Automatisierungslösung. Man spricht hier von einem IACS Security Managementsystem (*IACS-SMS, IACS-Security Management System*). Die Elemente eines Security-Managementsystems sind Richtlinien, Prozesse und Anweisungen für das Personal, das für den Betrieb der Anlage und den Umgang mit der Automatisierungslösung zuständig ist. Das Dokument unterstützt den Betreiber in der Erarbeitung aller relevanten Maßnahmen, die die Aufrechterhaltung des Betriebs im Falle eines Cyberangriffs sicherstellen. PDCA-Zyklen bilden die Grundlage der Erstellung eines Security-Managementsystems (siehe Abschnitt 4.4).

Die Edition 1 wurde im Jahr 2010 mit dem Titel „Establishing an industrial automation and control system security program“ veröffentlicht [4]. Eine erste Version der 2. Edition wurde als CD (Committee Draft) im Jahr 2012 veröffentlicht. Sie berücksichtigt die Kommentare, die eine Überarbeitung des Dokuments als Profil der breit etablierten Norm ISO 27001 [1] gefordert haben. Die zukünftige Norm wird die Struktur der ISO/IEC 27001 übernehmen und nur die Unterschiede spezifizieren, die für den Einsatz im industriellen Umfeld relevant sind. Um auf die zu erwartende Edition 2 vorzugreifen, basiert die folgende Zusammenfassung auf der Beschreibung der Norm ISO/IEC 27001, in der der Begriff „Informationssicherheitsmanagementsystem, ISMS“ (*Information Security Management System*) durch den Begriff „IACS Security Managementsystem, IACS-SMS“ (*Industrial Automation and Control System Security Management System*) ersetzt wurde. Allgemein wurde der Begriff „Informationssicherheit“ durch den Begriff „IACS Security“ ersetzt.

Die Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines IACS Security Managementsystems (IACS-SMS) festzulegen. Die Einführung eines IACS Security Managementsystems stellt für eine Organisation eine strategische Entscheidung dar. Die Erstellung und Umsetzung eines IACS Security Managementsystems innerhalb einer Organisation richtet sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern.

Das IACS Security Managementsystem unterstützt die Verfügbarkeit, Integrität und Vertraulichkeit aller Assets einer Automatisierungslösung unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Es ist wichtig, dass das IACS Security Managementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Security bereits bei der Konzeption von Prozessen, Automatisierungslösungen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines IACS Security Managementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Die Norm beschreibt, die Vorgehensweise und Prozesse zur Erstellung eines IACS Security Managementsystems und beinhaltet Anforderungen für die Beurteilung und Behandlung von Security-Risiken entsprechend den individuellen Bedürfnissen der Organisation. Die Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar sein. Im Folgenden werden die Inhalte der einzelnen Abschnitte kurz zusammengefasst.

- *Kontext der Organisation:* Verstehen der Organisation und ihres Kontextes, Verstehen der Erfordernisse und Erwartungen interessierter Parteien, Festlegen des Anwendungsbereichs des IACS Security Managementsystems;
- *Führung:* Führung und Verpflichtung der obersten Leitung in Bezug auf das IACS Security Managementsystem festlegen, Definition der Security-Politik, Festlegung der Rollen, Verantwortlichkeiten und Befugnisse in der Organisation;
- *Planung:* Festlegung von Maßnahmen zum Umgang mit Risiken und Chancen insbesondere Bewertung und Behandlung von Security-Risiken, Bestimmung von Security-Zielen und Planung zu deren Erreichung;
- *Unterstützung:* Ressourcen und Kompetenz zur Verfügung stellen, Bewusstsein sicherstellen, interne und externe Kommunikation in Bezug auf das IACS Security Managementsystem bestimmen, Bereitstellung einer dokumentierten Information, welche die Organisation als notwendig für die Wirksamkeit des Managementsystems bestimmt hat;
- *Betrieb:* Prozesse zur Erfüllung der Anforderungen und zur Durchführung der Maßnahmen planen, verwirklichen und steuern, in geplanten Abständen Beurteilung und ggf. Behandlung der Security-Risiken;
- *Bewertung der Leistung:* Security-Leistung und die Wirksamkeit des IACS Security Managementsystems bewerten, interne Audits in geplanten Abständen durchführen und Bewertung in geplanten Abständen des IACS Security Managementsystems durch die oberste Leitung;
- *Verbesserung:* Reagieren wenn eine Nichtkonformität auftritt, Korrekturmaßnahmen vornehmen, Eignung, Angemessenheit und Wirksamkeit des IACS Security Managementsystems fortlaufend verbessern.

In dem Dokument werden eine Liste von Maßnahmenzielen und Maßnahmen aufgeführt, die im Kontext des festgelegten Anwendungsbereichs des IACS Security Managementsystems auszuwählen und anzuwenden sind. Als Überblick werden im Folgenden Ziel und Überschriften der Maßnahmen gegeben. Als Vorgriff auf die Edition 2 des Teils 2-1 entspricht in unserer Beschreibung die Nummerierung der Norm IEC / ISO 27001 [1], wobei der Begriff „Informationssicherheit“ durch den Begriff „IACS Security“ ersetzt wurde.

- A.5 Richtlinien zu IACS Security
  - A.5.1 Vorgaben der Leitung für IACS Security

Ziel: Vorgaben und Unterstützung für die IACS Security sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.

Themen der Maßnahmen:

- Richtlinien zu IACS Security
- Überprüfung der Richtlinien zu IACS Security

- A.6 Organisation der IACS Security
  - A.6.1 Interne Organisation

    Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der IACS Security in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.

    Themen der Maßnahmen:

    - Rollen und Verantwortlichkeiten der IACS Security
    - Aufgabentrennung
    - Kontakt mit Behörden
    - Kontakt mit speziellen Interessensgruppen
    - IACS Security im Projektmanagement
  - A.6.2 Mobilgeräte und Telearbeit

    Ziel: Die IACS Security bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt. Mobilgeräte umfassen mobile Endgeräte jeder Art (Smartphones, Tablets, Laptops, Netbooks etc.).

    Themen der Maßnahmen:

    - Richtlinie zu Mobilgeräten
    - Telearbeit
- A.7 Personalsicherheit
  - A.7.1 Vor der Beschäftigung

    Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Rollen geeignet sind.

    Themen der Maßnahmen:

    - Sicherheitsüberprüfung
    - Beschäftigungs- und Vertragsbedingungen
  - A.7.2 Während der Beschäftigung

    Ziel: Es ist sichergestellt, dass Beschäftigte und Auftragnehmer sich ihrer Verantwortlichkeiten bezüglich der IACS Security bewusst sind und diesen nachkommen.

    Themen der Maßnahmen:

    - Verantwortlichkeiten der Leitung
    - Bewusstsein, Ausbildung und Schulung zu IACS Security
    - Maßregelungsprozess

  - A.7.3 Beendigung und Änderung der Beschäftigung

    Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

    Themen der Maßnahmen:

    - Inventarisierung der Werte
    - Zuständigkeit für Werte
    - Zulässiger Gebrauch von Werten
    - Rückgabe von Werten

- A.8 Verwaltung der Werte
  - A.8.1 Verantwortlichkeit für Werte

    Ziel: Die Werte der Organisation sind identifiziert und angemessene Verantwortlichkeiten zu ihrem Schutz sind festgelegt.

    Themen der Maßnahmen:

    - Inventarisierung der Werte
    - Zuständigkeit für Werte
    - Zulässiger Gebrauch von Werten
    - Rückgabe von Werten
  - A.8.2 Informationsklassifizierung

    Ziel: Es ist sichergestellt, dass Informationen ein angemessenes Schutzniveau entsprechend ihrer Bedeutung für die Organisation erhalten.

    Themen der Maßnahmen:

    - Klassifizierung von Informationen
    - Kennzeichnung von Informationen
    - Handhabung von Werten
  - A.8.3 Handhabung von Datenträgern

    Ziel: Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Informationen, die auf Datenträgern gespeichert ist, wird unterbunden.

    Themen der Maßnahmen:

    - Handhabung von Wechseldatenträgern
    - Entsorgung von Datenträgern
    - Transport von Datenträgern

- A.9 Zugangssteuerung
  - A.9.1 Geschäftsanforderungen an die Zugangssteuerung

    Ziel: Der Zugang zu Informationen und informationsverarbeitenden Einrichtungen ist eingeschränkt.

    Themen der Maßnahmen:

    - Zugangssteuerungsrichtlinie
    - Zugang zu Netzwerken und Netzwerkdiensten

- A.9.2 Benutzerzugangsverwaltung

  Ziel: Es ist sichergestellt, dass befugte Benutzer Zugang zu Systemen und Diensten haben und unbefugter Zugang unterbunden wird.

  Themen der Maßnahmen:

  - Registrierung und De-Registrierung von Benutzern
  - Zuteilung von Benutzerzugängen
  - Verwaltung privilegierter Zugangsrechte
  - Verwaltung geheimer Authentisierungsinformationen von Benutzern
  - Entzug oder Anpassung von Zugangsrechten
- A.9.3 Benutzerverantwortlichkeiten

  Ziel: Benutzer sind für den Schutz ihrer Authentisierungsinformationen verantwortlich gemacht.

  Themen der Maßnahmen:

  - Gebrauch geheimer Authentisierungsinformationen
- A.9.4 Zugangssteuerung für Systeme und Anwendungen

  Ziel: Unbefugter Zugang zu Systemen und Anwendungen ist unterbunden.

  Themen der Maßnahmen:

  - Informationszugangsbeschränkung
  - Sichere Anmeldeverfahren
  - System zur Verwaltung von Kennwörtern
  - Gebrauch von Hilfsprogrammen mit privilegierten Rechten
  - Zugangssteuerung für Quellcode von Programmen

- A.10 Kryptographie
  - A.10.1 Kryptographische Maßnahmen

    Ziel: Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Informationen ist sichergestellt.

    Themen der Maßnahmen:

    - Richtlinie zum Gebrauch von kryptographischen Maßnahmen
    - Schlüsselverwaltung
- A.11 Physische und umgebungsbezogene Sicherheit
  - A.11.1 Sicherheitsbereiche

    Ziel: Unbefugter Zutritt, die Beschädigung und die Beeinträchtigung von Informationen und informationsverarbeitenden Einrichtungen der Organisation sind verhindert.

    Themen der Maßnahmen:

    - Physischer Sicherheitsperimeter
    - Physische Zutrittssteuerung
    - Sichern von Büros, Räumen und Einrichtungen
    - Schutz vor externen und umweltbedingten Bedrohungen

  - Arbeiten in Sicherheitsbereichen
  - Anlieferungs- und Ladebereiche
- A.11.2 Geräte und Betriebsmittel

  Ziel: Verlust, Beschädigung, Diebstahl oder Gefährdung von Werten und die Unterbrechung von Organisationstätigkeiten sind unterbunden.

  Themen der Maßnahmen:
  - Platzierung und Schutz von Geräten und Betriebsmitteln
  - Versorgungseinrichtungen
  - Sicherheit der Verkabelung
  - Instandhalten von Geräten und Betriebsmitteln
  - Entfernen von Werten
  - Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten
  - Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
  - Unbeaufsichtigte Benutzergeräte
  - Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

- A.12 Betriebssicherheit
  - A.12.1 Betriebsabläufe und -verantwortlichkeiten

    Ziel: Der ordnungsgemäße und sichere Betrieb von informationsverarbeitenden Einrichtungen ist sichergestellt.

    Themen der Maßnahmen:
    - Dokumentierte Bedienabläufe
    - Änderungssteuerung
    - Kapazitätssteuerung
    - Trennung von Entwicklungs-, Test- und Betriebsumgebungen
  - A.12.2 Schutz vor Schadsoftware

    Ziel: Informationen und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.

    Themen der Maßnahmen:
    - Maßnahmen gegen Schadsoftware
  - A.12.3 Datensicherung

    Ziel: Daten sind vor Verlust geschützt.

    Themen der Maßnahmen:
    - Sicherung von Informationen
  - A.12.4 Protokollierung und Überwachung

    Ziel: Ereignisse sind aufgezeichnet und Nachweise sind erzeugt.

    Themen der Maßnahmen:
    - Ereignisprotokollierung
    - Schutz der Protokollinformation

  - Administratoren- und Bedienerprotokolle
  - Uhrensynchronisation
- A.12.5 Steuerung von Software im Betrieb

  Ziel: Die Integrität von Systemen im Betrieb ist sichergestellt.

  Themen der Maßnahmen:
  - Installation von Software auf Systemen im Betrieb
- A.12.6 Handhabung technischer Schwachstellen

  Ziel: Die Ausnutzung technischer Schwachstellen ist verhindert.

  Themen der Maßnahmen:
  - Handhabung von technischen Schwachstellen
  - Einschränkung von Softwareinstallation
- A.12.7 Audit von Informationssystemen

  Ziel: Die Auswirkung von Audittätigkeiten auf Systeme im Betrieb ist minimiert.

  Themen der Maßnahmen:
  - Maßnahmen für Audits von Informationssystemen

- A.13 Kommunikationssicherheit
  - A.13.1 Netzwerksicherheitsmanagement

    Ziel: Der Schutz von Informationen in Netzwerken und den unterstützenden informationsverarbeitenden Einrichtungen ist sichergestellt.

    Themen der Maßnahmen:
    - Netzwerksteuerungsmaßnahmen
    - Sicherheit von Netzwerkdiensten
    - Trennung in Netzwerken
  - A.13.2 Informationsübertragung

    Ziel: Die Sicherheit von übertragener Information, sowohl innerhalb einer Organisation als auch mit jeglicher externen Stelle, ist aufrechterhalten.

    Themen der Maßnahmen:
    - Richtlinien und Verfahren zur Informationsübertragung
    - Vereinbarungen zur Informationsübertragung
    - Elektronische Nachrichtenübermittlung
    - Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
  - A.14.1 Sicherheitsanforderungen an Informationssysteme

    Ziel: Es ist sichergestellt, dass IACS Security ein fester Bestandteil über den gesamten Lebenszyklus von Informationssystemen ist. Dies beinhaltet auch die Anforderungen an Informationssysteme, die Dienste über öffentliche Netze bereitstellen.

    Themen der Maßnahmen:
    - Analyse und Spezifikation von Anforderungen der IACS Security

  - Sicherung von Anwendungsdiensten in öffentlichen Netzwerken
  - Schutz der Transaktionen bei Anwendungsdiensten
- A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

  Ziel: Es ist sichergestellt, dass IACS Security im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist.

  Themen der Maßnahmen:
  - Richtlinie für sichere Entwicklung
  - Verfahren zur Verwaltung von Systemänderungen
  - Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform
  - Beschränkung von Änderungen an Softwarepaketen
  - Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme
  - Sichere Entwicklungsumgebung
  - Ausgegliederte Entwicklung
  - Testen der Systemsicherheit
  - Systemabnahmetest
- A.14.3 Testdaten

  Ziel: Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.

  Themen der Maßnahmen:
  - Schutz von Testdaten

- A.15 Lieferantenbeziehungen
  - A.15.1 IACS Security in Lieferantenbeziehungen

    Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.

    Themen der Maßnahmen:
    - Richtlinie zu IACS Security für Lieferantenbeziehungen
    - Behandlung von Sicherheit in Lieferantenvereinbarungen
    - Lieferkette für Informations- und Kommunikationstechnologie
  - A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten

    Ziel: Ein vereinbartes Niveau der IACS Security und der Dienstleistungserbringung ist im Einklang mit Lieferantenverträgen aufrechterhalten.

    Themen der Maßnahmen:
    - Überwachung und Überprüfung von Lieferantendienstleistungen
    - Handhabung der Änderungen von Lieferantendienstleistungen
- A.16 Handhabung von IACS Security-Vorfällen
  - A.16.1 Handhabung von IACS Security-Vorfällen und Verbesserungen

    Ziel: Eine konsistente und wirksame Herangehensweise für die Handhabung von IACS Security-Vorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwächen ist sichergestellt.

Themen der Maßnahmen:

- Verantwortlichkeiten und Verfahren
- Meldung von IACS Security-Ereignissen
- Meldung von Schwächen in der IACS Security
- Beurteilung von und Entscheidung über IACS Security-Ereignisse
- Reaktion auf IACS Security-Vorfälle
- Erkenntnisse aus Informationssicherheitsvorfällen
- Sammeln von Beweismaterial

- A.17 IACS Security-Aspekte beim Business Continuity Management
  - A.17.1 Aufrechterhalten der IACS Security

    Ziel: Die Aufrechterhaltung der IACS Security ist in das Business Continuity Managementsystem der Organisation eingebettet.

    Themen der Maßnahmen:

    - Planung zur Aufrechterhaltung der IACS Security
    - Umsetzen der Aufrechterhaltung der IACS Security
    - Überprüfen und Bewerten der Aufrechterhaltung der IACS Security
  - A.17.2 Redundanzen

    Ziel: Die Verfügbarkeit von informationsverarbeitenden Einrichtungen ist sichergestellt.

    Themen der Maßnahmen:

    - Verfügbarkeit von informationsverarbeitenden Einrichtungen
- A.18 Compliance
  - A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

    Ziel: Verstöße gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Verpflichtungen mit Bezug auf IACS Security und gegen jegliche Sicherheitsanforderungen sind vermieden.

    Themen der Maßnahmen:

    - Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen
    - Geistige Eigentumsrechte
    - Schutz von Aufzeichnungen
    - Privatsphäre und Schutz von personenbezogener Information
    - Regelungen bezüglich kryptographischer Maßnahmen
  - A.18.2 Überprüfungen der IACS Security

    Ziel: IACS Security ist in Übereinstimmung mit den Richtlinien und Verfahren der Organisation umgesetzt und wird entsprechend angewendet.

    Themen der Maßnahmen:

    - Unabhängige Überprüfung der IACS Security
    - Einhaltung von Richtlinien und Standards bei der IACS Security
    - Überprüfung der Einhaltung von technischen Vorgaben

A.2 IEC 62443-2-4

Das Dokument IEC 62443-2-4 [6] richtet sich an Anbietern für Integrationsleistungen oder Wartungsleistungen. Die Anforderungen spezifizieren organisatorische Vorgaben an Prozesse, Praktiken und Personal des Dienstleisters. Die Anforderungen richten sich an die Fähigkeiten des Dienstleisters, um eine allgemeine Bewertung des Leistungsangebots vornehmen zu können. Im Rahmen eines Projekts können die Inhalte auch dazu dienen, die umgesetzten Leistungen und Prozesse bezüglich Integration und Wartung zu bewerten.

Dienstleister können auch die Teile IEC 62443-3-3 und IEC 62443-4-2 in Zusammenhang mit diesem Teil verwenden, um mit Herstellern von Automatisierungssystemen oder Komponenten zusammenzuarbeiten. Damit können sie Leistungen und Prozesse entwickeln, die auf den Fähigkeiten des Automatisierungssystems oder der Komponente aufsetzen. Zum Beispiel Datensicherung und Wiederherstellung auf Basis der Empfehlungen des Herstellers und der Fähigkeiten des Automatisierungssystems oder der Komponente.

Der Betreiber kann IEC 62443-2-4 verwenden, um die Fähigkeiten des Dienstleisters zu bewerten. Er kann prüfen, ob bei einer Ausschreibung das Leistungsangebot des Dienstleisters die Fähigkeiten, die für ein gegebenes Projekt benötigt werden, abdeckt. In der Integrationsphase kann der Betreiber bewerten, ob die geforderten Anforderungen auch umgesetzt wurden. Schließlich kann der Betreiber während der Betriebsphase das Dokument als Vorgabe für die Wartungsprozesse verwenden.

Das Dokument erlaubt die Festlegung sogenannter Profile, um der Tatsache gerecht zu werden, dass nicht alle Anforderungen für alle Industriesektoren und Umgebungen anwendbar sind. Solche Profile können von Industriegruppen oder Organisationen als sog. „IEC Technical Reports, IEC TR“ erstellt werden, um die Untermenge der anwendbaren Anforderungen zu definieren und ggf. zu beschreiben, wie die Anforderungen in der spezifischen Umgebung anzupassen oder zu interpretieren sind.

Die Anforderungen wurden in einer Tabelle aufgelistet, die auch als separate Excel-Datei erhältlich ist, um dem Anwender die Sortierung und das Filtern zu erleichtern.

Die Anforderungen wurden weitgehend abstrakt formuliert, um den Dienstleistern eine gewisse Freiheit für ihre Umsetzung zu lassen. Weitergehende Anforderungen beschreiben Restriktionen oder Spezialisierungen mit dem Ziel, die Security durch strengere Umsetzungen der Anforderungen zu erhöhen.

Um dem Leser einen Überblick über inhaltliche Abdeckung der Anforderungen zu geben, werden in den folgenden Tabellen die funktionalen Bereiche sowie die Haupt- und Unterthemen beschrieben.

Tabelle 2 Anforderungstabelle

Spalte	Beschreibung
Req ID	Kennung
BR/RE	Indikator für Anforderung / weitergehende Anforderung
Functional area	Funktionaler Bereich
Topic	Schlüsselwort für das Hauptthema der Anforderung. Das gleiche Thema kann für mehrere funktionale Gebiete oder Aktivitäten relevant sein.
Subtopic	Schlüsselwort für das Unterthema der Anforderung. Das gleiche Thema kann für mehrere funktionale Gebiete oder Aktivitäten relevant sein.
Doc?	Ist dem Betreiber eine Dokumentation als Ergebnis zur Verfügung zu stellen? Anmerkung: Manche Anforderungen können erfordern, dass der Dienstleister eine Dokumentation pflegt, die nicht als Ergebnis zu betrachten ist. Der Betreiber kann aber mit dem Dienstleister vereinbaren, dass er diese Dokumentation sichten kann oder zur Verfügung gestellt bekommt.
Requirement description	Text der Anforderung, die eine Fähigkeit des Dienstleisters definiert. Ob der Betreiber diese Anforderung verlangt, ist nicht Bestandteil des Dokuments.
Rationale	Text über den Hintergrund, die Begründung oder andere Aspekte, die für den Leser für das Verständnis der Anforderung hilfreich sind.

Tabelle 3 Funktionale Bereiche

Funktionaler Bereich	Req ID	Beschreibung
Solution staffing	SP.01.xx	Anforderungen zu der Zuordnung von Personal zu Aktivitäten des Dienstleisters bezüglich der Automatisierungslösung
Assurance	SP.02.xx	Anforderungen, die das Vertrauen betreffen, dass die Security in der Automatisierungslösung durchgesetzt wird
Architecture	SP.03.xx	Anforderungen, die das Design der Automatisierungslösung betreffen
Wireless	SP.04.xx	Anforderungen, die den Einsatz drahtloser Kommunikation in der Automatisierungslösung betreffen
SIS	SP.05.xx	Anforderungen, die die Integration von PLT-Sicherheitseinrichtungen in der Automatisierungslösung betreffen
Configuration management	SP.06.xx	Anforderungen, die die Beherrschung der Konfiguration der Automatisierungslösung betreffen
Remote access	SP.07.xx	Anforderungen, die den Fernzugriff zu der Automatisierungslösung betreffen
Event management	SP.08.xx	Anforderungen, die die Behandlung von Ereignissen in der Automatisierungslösung betreffen
Account management	SP.09.xx	Anforderungen, die die Verwaltung von Nutzerkonten der Automatisierungslösung betreffen
Malware protection	SP.10.xx	Anforderungen, die die Nutzung von Anti-Malware Software in der Automatisierungslösung betreffen
Patch Management	SP.11.xx	Anforderungen, die die Security-Aspekte bei dem Bereitstellen und dem Einspielen von Software-Aktualisierungen betreffen
Backup/Restore	SP.12.xx	Anforderungen, die die Datensicherung und die Wiederherstellung von Daten betreffen

Tabelle 4 Hauptthemen.

Hauptthema	Beschreibung
Accounts – ...	Anforderungen, die verschiedene Arten von Nutzerkonten betreffen
Security tools and software	Anforderungen, die die Anwendung von Softwarewerkzeugen für die Security in der Automatisierungslösung betreffen
Background checks	Anforderungen, die die Überprüfung der Vergangenheit (eines) Mitarbeiters betreffen
Backup	Anforderungen, die die Sicherung und Wiederherstellung der Daten der Automatisierungslösung betreffen
Data protection	Anforderungen, die den Schutz der Daten betreffen
Devices – ...	Anforderungen, die verschiedene Arten von in der Automatisierungslösung eingesetzten Komponenten betreffen
Events – ...	Anforderungen, die verschiedene Arten von Ereignissen in der Automatisierungslösung betreffen
Hardening guidelines	Anforderungen, die Richtlinien zur Härtung der Automatisierungslösung betreffen
Manual process	Anforderungen, die manuelle Prozesse zur Benutzung von Security-Fähigkeiten der Automatisierungslösung (z. B. Patch-Management, Datensicherung und Wiederherstellung) betreffen
Network design	Anforderungen, die das Auslegen der Netzwerkarchitektur der Automatisierungslösung betreffen
Passwords	Anforderungen, die die Passwörter der Nutzerkonten betreffen
Patch list	Anforderungen, die eine Liste von Kennungen und Eigenschaften von Security-Patchen betreffen, die für die Automatisierungslösung anwendbar sind
Personnel assignments	Anforderungen zu der Zuordnung von Personal zu Aktivitäten des Dienstleisters bezüglich der Automatisierungslösung
Portable media	Anforderungen, die den Einsatz von tragbaren Medien in der Automatisierungslösung betreffen
Restore	Anforderungen, die die Wiederherstellung von Daten in der Automatisierungslösung betreffen
Risk assessment	Anforderungen, die die Durchführung von Risiko-Bewertungen bezüglich der Automatisierungslösung und ihrer Komponenten betreffen
Security tools and software	Anforderungen, die die Verwendung von Softwarewerkzeugen für die Implementierung und die Verwaltung der Security der Automatisierungslösung betreffen
Solution components	Anforderungen, die den Einsatz von Komponenten der Automatisierungslösung betreffen
Training	Anforderungen, die die Schulung des Personals betreffen, das in Aktivitäten des Dienstleisters bezüglich der Automatisierungslösung eingebunden ist
User interface	Anforderungen, die die Anwenderschnittstellen der Automatisierungslösung betreffen
Vulnerabilities	Anforderungen, die die Behandlung von Schwachstellen in der Automatisierungslösung betreffen

Tabelle 5 Unterthemen.

Unterthema	Beschreibung
Access control	Anforderungen, die Authentisierung und/oder Autorisierung betreffen
Administration	Anforderungen, die Administration und Verwaltung, z. B. die Geräte-Administration und die Benutzerverwaltung betreffen
Approval	Anforderungen, die die Genehmigung durch den Betreiber betreffen
Change	Anforderungen, die die Änderung von Passwörtern betreffen
Communications	Anforderungen, die interne und externe Kommunikation der Automatisierungslösung betreffen
Composition	Anforderungen, die die Zusammensetzung von Passwörtern betreffen
Configuration mode	Anforderungen, die den Zustand einer konfigurierbaren Komponente betreffen
Connectivity	Anforderungen, die Anschlussfähigkeit von Komponenten und/oder Netzwerksegmenten betreffen
Cryptography	Anforderungen, die den Einsatz von kryptographischen Verfahren (z. B. Verschlüsselung, digitale Signaturen) betreffen
Data/event retention	Anforderungen, die das Archivieren von Daten und Ereignissen betreffen
Delivery	Anforderungen, die die Bereitstellung von Security-Patchen betreffen
Detection	Anforderungen, die die Erkennung von Ereignissen betreffen
Disaster recovery	Anforderungen, die die Erholung von Krisen betreffen
Expiration	Anforderungen, die das Ablaufen von Passwörtern und Nutzerkonten betreffen
Installation	Anforderungen, die die Installation von Security-Werkzeugen und Software betreffen
Inventory register	Anforderungen, die die Dokumentation der eingesetzten Geräte und deren Software-Komponenten in der Automatisierungslösung betreffen
Least functionality	Anforderungen, die die Unterstützung des Konzepts der minimalen Funktionalität betreffen (z. B. Abschalten von unnötigen Diensten oder Entfernen von temporären Nutzerkonten). Siehe dazu die IEC 62443-3-3 für weitere Details.
Logging	Anforderungen, die die Protokollierung von Ereignissen betreffen
Malware definition files	Anforderungen, die die Genehmigung und den Einsatz von Malware-Definitionsdateien betreffen
Malware protection mechanism	Anforderungen, die den Einsatz von Schutzmechanismen gegen Malware betreffen (z. B. Antivirus-Software, Whitelisting)
Network time	Anforderungen, die Verteilung und Synchronisierung einer Uhr über das Netzwerk betreffen
Patch qualification	Anforderungen, die die Bewertung und Genehmigung von Patchen für den Einsatz in der Automatisierungslösung betreffen
Perform	Anforderungen, die die Umsetzung einer Fähigkeit in der Automatisierungslösung betreffen
Reporting	Anforderungen, die das Berichtswesen der Ereignisse betreffen (z. B. Meldungen)
Responding	Anforderungen, die Behandlung und Beantwortung von Ereignissen betreffen
Reuse	Anforderungen, die die Wiederverwendung von Passwörtern betreffen
Robustness	Anforderungen, die Widerstandsfähigkeit der Automatisierungslösung bei unnormalen Daten, unnormalen Sequenzen oder unnormal hohem Netzwerkverkehr betreffen (z. B. bei Alarmsturmen oder Netzwerk-Scans)
Sanitizing	Anforderungen, die die Bereinigung von Geräten und tragbaren Datenmedien von sensiblen Daten und/oder Malware betreffen

Unterthema	Beschreibung
Security contact	Anforderungen, die eine Kontaktrolle für Security fordern und definieren
Security lead	Anforderungen, die eine Führungsrolle für Security fordern und definieren
Security requirements – ...	Anforderungen, die Security-Anforderungen betreffen, die in diesem Dokument enthalten sind oder vom Betreiber definiert werden
Sensitive data	Anforderungen, die Daten mit einem Bedarf einer sicheren Aufbewahrung betreffen,
Service provider	Anforderungen, die das Personal oder die Fähigkeit des Dienstleisters betreffen
Session lock	Anforderungen, die die Sperrung von Tastauren und Bildschirmen der Arbeitsstationen betreffen
Shared	Anforderungen, die die gemeinsame Benutzung von Passwörtern betreffen
Subcontractor	Anforderungen, die das Personal oder der Fähigkeit von Unterauftragnehmern, Beratern oder Vertretern des Dienstleisters betreffen
Technical description	Anforderungen, die Beschreibungen von technischen Aspekten der Automatisierungslösung betreffen
Usage	Anforderungen, die den Einsatz oder die Umsetzung einer geforderten Fähigkeit betreffen
Verification	Anforderungen, die die Prüfung einer Fähigkeit betreffen (z. B. mittels eines Demonstrators oder durch visuelle Kontrolle)
Wireless network identifiers	Anforderungen, die die Kennungen von drahtlosen Netzwerken betreffen

A.3 IEC 62443-3-3

Dieses Dokument [9] richtet sich in erster Linie an Produktlieferanten und Systemintegratoren. Auf der einen Seite können die funktionalen Fähigkeiten von Automatisierungssystemen an den in Dokument gelisteten Anforderungen gespiegelt werden, auf der anderen Seite können die in einer Automatisierungslösung realisierten Funktionalitäten gegenüber diesen Anforderungen bewertet werden. Das Dokument ist auch relevant für die auf dem Gebiet der industriellen Automatisierungstechnik tätigen Betreiber, Dienstleister und gegebenenfalls Zulassungsstellen. Zu letzteren gehören auch Behörden und Regulierer, deren Zuständigkeit es ist, die Einhaltung von Gesetzen und Vorschriften durch Prüfungen zu überwachen.

Systemintegratoren, Produktlieferanten und Dienstleister werden mit Hilfe dieser Norm bewerten, inwieweit ihre Produkte und Dienstleistungen die funktionalen IT-Sicherheitsfähigkeiten erbringen, um die Anforderungen des Betreibers, ausgedrückt als SL-T (zu erreichender SL), zu erreichen. Ebenso wie die Zuweisung von SL-Ts müssen auch die einzelnen Systemanforderungen auf den IT-Sicherheitsleitlinien, den Vorgehensweisen und der Risikobewertung des Betreibers im Zusammenhang mit der jeweiligen Anlage beruhen. Dabei ist zu beachten, dass manche Systemanforderungen Voraussetzungen für zulässige Ausnahmen enthalten, etwa wenn ihr Einhalten zur Verletzung fundamentaler betrieblicher Anforderungen einer Automatisierungslösung führen sollte (was Ausgleichsmaßnahmen notwendig machen könnte).

Beim Entwurf einer Automatisierungslösung, die eine Anzahl von Systemanforderungen zum jeweiligen SL-T einhalten soll, ist es nicht erforderlich, dass jede Komponente des vorgeschlagenen Automatisierungssystems auch jede Systemanforderung auf der in dieser Norm

angegebenen Stufe einhalten muss. So können auch Ausgleichsmaßnahmen ergriffen werden, um die von anderen Subsystemen benötigte Funktionalität bereitzustellen und auf der Ebene der Automatisierungslösung dennoch die SL-T-Anforderungen einzuhalten. Die Einbeziehung von Ausgleichsmaßnahmen während der Entwurfsphase der Automatisierungslösung sollte durch eine umfassende Dokumentation begleitet werden, so dass der erreichte Security-Level der Automatisierungslösung (SL-A) die beabsichtigten, sich aus dem Entwurf ergebenden Security-Fähigkeiten vollständig widerspiegelt.

Der Detaillierungsrad dieser Norm reicht nicht aus, um ein ganzheitliches Schutzkonzept zu entwerfen und aufzubauen. Hierzu sind zusätzliche und tiefergehende Analysen in der Systemebene und die Ausarbeitung abgeleiteter Anforderungen notwendig, die Gegenstand weiterer Normen der Reihe IEC 62443 sind. Man beachte, dass eine für den Aufbau einer IT-Sicherheitsarchitektur ausreichend detaillierte Spezifikation nicht das Ziel dieses Dokuments ist. Dieses ist vielmehr die Festlegung einer gemeinsamen kleinsten Menge von Anforderungen, um fortschreitend strengere Security-Levels erreichen zu können. Der Entwurf einer diese Anforderungen einhaltenden Architektur obliegt den Systemintegratoren und Produktlieferanten. Sie sind bei diesen Arbeiten frei, individuelle Auswahlen zu treffen und können sich somit dem Wettbewerb stellen und Innovationen vorantreiben. Das Dokument beschränkt sich ganz bewusst auf die Festlegung funktionaler Anforderungen und legt nicht fest, wie diese erfüllt werden sollten.

Das Dokument legt anhand der sieben grundlegenden Anforderungen (FR) nach IEC 62443-1-1 detaillierte technische Systemanforderungen (SR) an industrielle Automatisierungssysteme fest, einschließlich der Festlegung der Anforderungen zu erreichbaren Security Levels, SL-C (Automatisierungssystem). Diese Anforderungen werden von verschiedenen Personen im Bereich der industriellen Automatisierungstechnik angewendet, indem sie, anhand der festgelegten Zonen und Conduits einer zu betrachtenden Automatisierungslösung, einen angemessenen, zu erreichenden Security-Level SL-T für das zu schützende Asset entwickeln. Jede Systemanforderung besteht aus einer Hauptanforderung und gegebenenfalls weitergehenden Anforderungen (RE), die die Security potenziell verstärken. Die Hauptforderung und etwaige vorhandene weitergehende Anforderungen werden dann auf die erreichbaren Security-Levels SL-C des Automatisierungssystems 1 bis 4 abgebildet.

Nach IEC 62443-1-1 gibt es insgesamt sieben grundlegende Anforderungen:

- FR 1 – Identifizierung und Authentifizierung (*IAC, identification and authentication control*)
- FR 2 – Nutzungskontrolle (*UC, use control*)
- FR 3 – Systemintegrität (*SI, system integrity*)
- FR 4 – Vertraulichkeit der Daten (*DC, data confidentiality*)
- FR 5 – Eingeschränkter Datenfluss (*RDF, restricted data flow*)
- FR 6 – Rechtzeitige Reaktion auf Ereignisse (*TRE, timely response to events*)
- FR 7 – Verfügbarkeit der Ressourcen (*RA, resource availability*)

Alle sieben grundlegenden Anforderungen haben eine festgelegte Menge von vier SL, siehe die Beschreibung im Abschnitt 4.5. SL 0 als erreichbares SL eines Automatisierungssystems für eine gegebene grundlegende Anforderung (FR) bedeutet keine Anforderung.

FR 1 – Identifizierung und Authentifizierung

Die Betreiber werden eine Liste aller Nutzer (Menschen, Softwareprozesse und Geräte) erstellen und müssen für jede Komponente des Automatisierungssystems die erforderliche Schutzstufe durch Identifizierung und Authentifizierung bestimmen. Das Ziel der Identifizierung und Authentifizierung ist es, das Automatisierungssystem dadurch zu schützen, dass die Identität eines jeden Nutzers geprüft wird, der Zugriff zum Automatisierungssystem anfordert, bevor die Kommunikation aktiviert wird. Zu den Empfehlungen und Leitlinien sollten solche Verfahren gehören, die im gemischten Modus arbeiten. So erfordern manche Komponenten eines Automatisierungssystems beispielsweise eine starke Identifizierung und Authentifizierung, wie etwa starke Authentifizierungsverfahren, und andere nicht.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, alle Nutzer (Menschen, Softwareprozesse und Geräte) zu identifizieren und authentifizieren, bevor ihnen der Zugang zum Automatisierungssystem gewährt wird.

- SL 1 – Identifizieren und Authentifizieren aller Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen gelegentlichen oder zufälligen Zugang von nicht authentifizierten Personen oder Stellen schützen.
- SL 2 – Identifizieren und Authentifizieren aller Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Personen oder Stellen, die mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fertigkeiten und geringer Motivation vorgehen, schützen.
- SL 3 – Identifizieren und Authentifizieren aller Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Personen oder Stellen, die mit raffinierten Mitteln, mittleren Ressourcen, automatisierungstechnischen Fertigkeiten und mittlerer Motivation vorgehen, schützen.
- SL 4 – Identifizieren und Authentifizieren aller Nutzer (Menschen, Softwareprozesse und Geräte) durch Verfahren, die gegen einen absichtlichen, nicht authentifizierten Zugang von Personen oder Stellen, die mit raffinierten Mitteln, erheblichen Ressourcen, automatisierungstechnischen Fertigkeiten und hoher Motivation vorgehen, schützen.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für Identifizierung und Authentifizierung zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identifizierung und Authentifizierung (IAC)				
SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern	✓	✓	✓	✓
SR 1.1 RE 1 – Eindeutige Identifizierung und Authentifizierung		✓	✓	✓
SR 1.1 RE 3 – Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze			✓	✓
SR 1.1 RE 3 – Multifaktor-Authentifizierung über alle Netze				✓
SR 1.2 – Identifizierung und Authentifizierung von Softwareprozessen und Geräten		✓	✓	✓
SR 1.2 RE 1 – Eindeutige Identifizierung und Authentifizierung			✓	✓
SR 1.3 – Nutzerkontenverwaltung	✓	✓	✓	✓
SR 1.3 RE 1 – Einheitliche Nutzerkontenverwaltung			✓	✓
SR 1.4 – Verwaltung der Kennungen	✓	✓	✓	✓
SR 1.5 – Verwaltung der Authentifikatoren	✓	✓	✓	✓
SR 1.5 RE 1 – Beglaubigung der Identität von Softwareprozessen durch Hardwaremaßnahmen			✓	✓
SR 1.6 – Management drahtloser Zugriffsverfahren	✓	✓	✓	✓
SR 1.6 RE 1 – Eindeutige Identifizierung und Authentifizierung		✓	✓	✓
SR 1.7 – Stärke der Authentifizierung durch Passwörter	✓	✓	✓	✓
SR 1.7 RE 1 – Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Nutzer			✓	✓
SR 1.7 RE 2 – Lebensdauerbeschränkungen von Passwörtern für alle Nutzer				✓
SR 1.8 – PKI-Zertifikate		✓	✓	✓
SR 1.9 – Stärke der Authentifizierung durch öffentliche Schlüssel		✓	✓	✓
SR 1.9 RE 1 – Beglaubigung öffentlicher Schlüssel durch Hardwaremaßnahmen			✓	✓
SR 1.10 – Rückmeldung vom Authentifikator	✓	✓	✓	✓
SR 1.11 – Erfolglose Anmeldeversuche	✓	✓	✓	✓
SR 1.12 – Nutzungshinweis	✓	✓	✓	✓
SR 1.13 – Zugriff über nicht vertrauenswürdige Netze	✓	✓	✓	✓
SR 1.13 RE 1 – Genehmigung ausdrücklicher Anmeldebegehren		✓	✓	✓

FR 2 – Nutzungskontrolle

Nach erfolgter Identifizierung und Authentifizierung eines Nutzers muss das Automatisierungssystem die erlaubten Aktionen auf die autorisierte Nutzung des Automatisierungssystems einschränken. Betreiber und Systemintegratoren müssen jedem Nutzer (menschlichem Nutzer, Softwareprozess oder Gerät), jeder Gruppe, Rolle usw. (siehe 5.6, SR 1.4 – Verwaltung der Kennungen) die Berechtigungen zuweisen, die die autorisierte Nutzung des Automatisierungssystem definieren. Das Ziel der Nutzungskontrolle ist der Schutz vor nicht autorisierten Handlungen an den Ressourcen des Automatisierungssystems durch Verifikation, dass die erforderlichen Berechtigungen erteilt worden sind, bevor dem Nutzer erlaubt wird, die Aktionen durchzuführen. Beispiele solcher Handlungen sind Daten auslesen oder schreiben, Programme herunterladen und Konfigurationen verändern. Empfehlungen und Leitlinien sollten Verfahren enthalten, die im gemischten Modus arbeiten. Beispielsweise erfordern einige Ressourcen des Automatisierungssystems eine strenge Nutzungskontrolle, wie restriktive Berechtigungen, andere dagegen nicht. Die Nutzungskontrolle muss auch auf Daten bei der Speicherung ausgedehnt werden. Nutzerberechtigungen können nach Tageszeit/Datum, Ort und Zugangsmedium variieren.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, die einem authentifizierten Nutzer (menschlicher Nutzer, Softwareprozess oder Gerät) zugewiesenen Berechtigungen durchzuführen, durchzusetzen sowie die Verwendung dieser Berechtigungen zu überwachen.

- SL 1 – Beschränkung der Nutzung des Automatisierungssystems entsprechend den festgelegten Berechtigungen, um vor gelegentlichem oder zufälligem Missbrauch zu schützen.
- SL 2 – Beschränkung der Nutzung des Automatisierungssystems entsprechend den festgelegten Berechtigungen, um vor Missbrauch durch Personen oder Stellen, die mit einfachen Mitteln bei geringen Ressourcen, allgemeinen Fertigkeiten und geringer Motivation vorgehen, zu schützen.
- SL 3 – Beschränkung der Nutzung des Automatisierungssystems entsprechend den festgelegten Berechtigungen, um vor Missbrauch durch Personen oder Stellen, die mit raffinierten Mitteln und mittleren Ressourcen, automatisierungstechnischen Fertigkeiten und mittlerer Motivation vorgehen, zu schützen.
- SL 4 – Beschränkung der Nutzung des Automatisierungssystems entsprechend den festgelegten Berechtigungen, um vor Missbrauch durch Personen oder Stellen, die mit raffinierten Mitteln und erheblichen Ressourcen, automatisierungstechnischen Fertigkeiten und hoher Motivation vorgehen, zu schützen.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die Nutzungskontrolle zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 2 – Nutzungskontrolle (UC)				
SR 2.1 – Durchsetzung der Autorisierung	✓	✓	✓	✓
SR 2.1 RE 1 – Durchsetzung der Autorisierung für alle Nutzer		✓	✓	✓
SR 2.1 RE 2 – Abbildung der Berechtigung auf Rollen		✓	✓	✓
SR 2.1 RE 3 – Eingriffe des Aufsichtspersonals			✓	✓
SR 2.1 RE 4 – Doppelte Zustimmung				✓
SR 2.2 –Nutzungskontrolle von Funkverbindungen	✓	✓	✓	✓
SR 2.2 RE 1 – Nicht genehmigte drahtlose Geräte erkennen und anzeigen			✓	✓
SR 2.3 – Nutzungskontrolle von tragbaren und mobilen Geräten	✓	✓	✓	✓
SR 2.3 RE 1 – Security-Status tragbarer und mobiler Geräte durchsetzen			✓	✓
SR 2.4 – Mobiler Code	✓	✓	✓	✓
SR 2.4 RE 1 – Prüfung der Integrität mobilen Codes			✓	✓
SR 2.5 – Sitzungssperrung	✓	✓	✓	✓
SR 2.6 – Beendigung einer Fernzugriffssitzung		✓	✓	✓
SR 2.7 – Begrenzung der Anzahl gleichzeitiger Sitzungen			✓	✓
SR 2.8 –Prüfbare Ereignisse und deren Aufzeichnung	✓	✓	✓	✓
SR 2.8 RE 1 – Zentral verwaltete systemweite Ereignisaufzeichnung			✓	✓
SR 2.9 – Speicherkapazität für Aufzeichnungen	✓	✓	✓	✓
SR 2.9 RE 1 – Warnung, wenn die Kapazitätsgrenze zur Speicherung von Ereignisdatensätzen erreicht ist			✓	✓
SR 2.10 – Reaktion auf ausgefallene Ereignisdatenverarbeitung	✓	✓	✓	✓
SR 2.11 – Zeitstempel		✓	✓	✓
SR 2.11 RE 1 – Interne Systemtakte			✓	✓
SR 2.11 RE 2 – Schutz und Integrität der Zeitquelle				✓
SR 2-12 – Nicht-Abstreitbarkeit			✓	✓
SR 2.12 RE 1 – Nicht-Abstreitbarkeit für alle Nutzer				✓

FR 3 – Systemintegrität

Industrielle Automatisierungssysteme werden meist mehreren Prüfphasen unterzogen, um noch vor Produktionsaufnahme festzustellen, dass sich die Systeme bestimmungsgemäß verhalten. Nach Betriebsbeginn sind die Betreiber für die Aufrechterhaltung der Integrität des industriellen Automatisierungssystems verantwortlich. Mittels ihrer Risikobewertung können sie unterschiedlichen Systemen, Kommunikationskanälen und Informationen in ihrem industriellen Automatisierungssystem unterschiedliche Stufen des Integritätsschutzes zuweisen. Die Integrität des zu schützende Assets sollte sowohl im Betriebszustand als auch in Nicht-Betriebszuständen aufrechterhalten werden, beispielsweise während der Produktion, im Lager oder wenn die Anlage zum Zwecke der Instandhaltung heruntergefahren wurde. Die Integrität der logischen Vermögenswerte sollte bei deren Übertragung und Speicherung aufrechterhalten werden, beispielsweise bei der Übertragung über ein Kommunikationsnetz oder bei der Ablage in einem Datenbestand.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, die Integrität des industriellen Automatisierungssystems sicherzustellen und nicht autorisierte Manipulation zu verhindern.

- SL 1 – Schutz der Integrität des industriellen Automatisierungssystems gegen gelegentliche oder zufällige Manipulation.
- SL 2 – Schutz der Integrität des industriellen Automatisierungssystems gegen Manipulation durch Personen oder Stellen, die mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fertigkeiten und geringer Motivation vorgehen.
- SL 3 – Schutz der Integrität des industriellen Automatisierungssystems gegen Manipulation durch Personen oder Stellen, die mit raffinierten Mitteln, mittleren Ressourcen, automatisierungstechnischen Fertigkeiten und mittlerer Motivation vorgehen.
- SL 4 – Schutz der Integrität des industriellen Automatisierungssystems gegen Manipulation durch Personen oder Stellen, die mit raffinierten Mitteln, erheblichen Ressourcen, automatisierungstechnischen Fertigkeiten und hoher Motivation vorgehen.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die Systemintegrität zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 3 – Systemintegrität (SI)				
SR 3.1 – Kommunikationsintegrität	✓	✓	✓	✓
SR 3.1 RE 1 – Kryptographische Schutzmaßnahmen zur Bewahrung der Integrität			✓	✓
SR 3.2 – Schutz vor Schadcode	✓	✓	✓	✓
SR 3.2 RE 1 – Schutz vor Schadcode an Eingangs- und Ausgangspunkten		✓	✓	✓
SR 3.2 RE 2 – Zentrales Management und Meldewesen zum Schutz vor Schadcode			✓	✓
SR 3.3 – Verifikation der IT-Sicherheitsfunktionalität	✓	✓	✓	✓
SR 3.3 RE 1 – Automatisierte Mechanismen zur Verifikation der IT-Sicherheitsfunktionalität			✓	✓
SR 3.3 RE 2 – Verifikation der IT-Sicherheitsfunktionalität im laufenden Betrieb				✓
SR 3.4 – Software- und Informationsintegrität	✓	✓	✓	✓
SR 3.4 RE 1 – Automatisierte Hinweise auf IT-Sicherheitsverstöße			✓	✓
SR 3.5 – Eingabevalidierung	✓	✓	✓	✓
SR 3.6 – Vorbestimmte Zustände der Ausgänge	✓	✓	✓	✓
SR 3.7 – Fehlerbehandlung		✓	✓	✓
SR 3.8 – Sitzungsintegrität		✓	✓	✓
SR 3.8 RE 1 – Annullierung der Sitzungskennungen nach Sitzungsbeendigung			✓	✓
SR 3.8 RE 2 – Erzeugung einer eindeutigen Sitzungskennung			✓	✓
SR 3.8 RE 3 – Zufälligkeit der Sitzungskennungen				✓
SR 3.9 – Schutz von Prüfinformationen		✓	✓	✓
SR 3.9 RE 1 – Ereignisdatensätze auf nur einmal beschreibbaren Speichermedien				✓

FR 4 – Vertraulichkeit der Daten

Einige vom Automatisierungssystem erzeugte Informationen, sowohl bei der Übertragung als auch bei der Speicherung, sind von vertraulicher oder sensibler Natur. Dies hat zur Folge, dass einige Kommunikationskanäle und Datenbestände Schutz gegen Abhören und nicht autorisierten Zugriff benötigen.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, die Vertraulichkeit von Daten in Kommunikationskanälen und Datenbeständen sicherzustellen, um deren nicht autorisierte Offenlegung zu verhindern.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die Vertraulichkeit der Daten zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 4 – Vertraulichkeit der Daten (DC)				
SR 4.1 – Vertraulichkeit von Informationen	✓	✓	✓	✓
SR 4.1 RE 1 – Schutz der Vertraulichkeit bei der Speicherung oder Übertragung über nicht vertrauenswürdige Netze		✓	✓	✓
SR 4.1 RE 2 – Schutz der Vertraulichkeit über Zonengrenzen hinweg				✓
SR 4.2 – Dauerhaftigkeit von Informationen		✓	✓	✓
SR 4.2 RE 1 – Säuberung gemeinsam genutzter Speicher			✓	✓
SR 4.3 – Verwendung von Verschlüsselung	✓	✓	✓	✓

FR 5 – Eingeschränkter Datenfluss

Anhand einer Risikoeinschätzung müssen die Betreiber die notwendigen Einschränkungen des Informationsflusses bestimmen und damit folglich auch die Einrichtung der zur Übermittlung dieser Informationen benutzten Conduits festlegen. Hieraus abgeleitete Empfehlungen und Leitlinien sollten Mechanismen enthalten, die von der Trennung der Automatisierungssysteme von kommerziellen oder öffentlichen Netzen bis zur Verwendung unidirektionaler Gateways, Firewalls mit stateful-packet-Inspection und DMZs reichen, um so den Informationsfluss lenken zu können.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, das Automatisierungssystem in Zonen und Conduits aufzuteilen, um einen unnötigen Datenfluss zu verhindern.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die Vertraulichkeit der Daten zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Eingeschränkter Datenfluss (RDF)				
SR 5.1 – Netzaufteilung	✓	✓	✓	✓
SR 5.1 RE 1 – Physikalische Netzaufteilung		✓	✓	✓
SR 5.1 RE 2 – Unabhängigkeit von nicht-automatisierungstechnischen Netzen			✓	✓
SR 5.1 RE 3 – Logische und physikalische Isolierung kritischer Netze				✓
SR 5.2 – Schutz der Zonengrenze	✓	✓	✓	✓
SR 5.2 RE 1 – Deny by default, allow by exception		✓	✓	✓
SR 5.2 RE 2 – Inselmodus			✓	✓
SR 5.2 RE 3 – Fail close			✓	✓
SR 5.3 – Beschränkung der Verwendung der persönlichen Kommunikation	✓	✓	✓	✓
SR 5.3 RE 1 – Verbot der Verwendung der persönlichen Kommunikation			✓	✓
SR 5.4 – Partitionierung von Anwendungen	✓	✓	✓	✓

FR 6 – Rechtzeitige Reaktion auf Ereignisse

Anhand einer Risikoeinschätzung sollten die Betreiber Leitlinien und Vorgehensweisen sowie eindeutige Kommunikations- und Eingriffswege, die zur Reaktion auf Verstöße gegen die Security benötigt werden, festlegen. Daraus abgeleitete vorschriftenartige Empfehlungen und Leitlinien sollten Mechanismen zur Erfassung, Weiterleitung, Aufbewahrung und automatischen Korrelation forensischer Beweise einschließen, um zeitnahe Maßnahmen sicherzustellen. Der Einsatz von Überwachungswerkzeugen und -techniken sollte die Leistung des Automatisierungssystems nicht nachteilig beeinflussen.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, auf Verstöße gegen die Security durch Benachrichtigen der richtigen Stelle, Beibringen von Beweisen der Verletzung und Veranlassen rechtzeitiger Maßnahmen zu reagieren, sobald Vorfälle entdeckt worden sind.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die rechtzeitige Reaktion auf Ereignisse zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 6 – Rechtzeitige Reaktion auf Ereignisse (TRE)				
SR 6.1 – Zugriffsmöglichkeit auf Ereignisprotokolle	✓	✓	✓	✓
SR 6.1 RE 1 – Programmgesteuerter Zugriff auf Ereignisprotokolle			✓	✓
SR 6.2 – Kontinuierliche Überwachung		✓	✓	✓

FR 7 – Ressourcenverfügbarkeit

Das Ziel dieser Reihe von SR ist es, sicherzustellen, dass das Automatisierungssystem gegen verschiedene Arten von DoS-Ereignissen widerstandsfähig ist. Dieses schließt die teilweise oder vollständige Nicht-verfügbarkeit von Systemfunktionen auf verschiedenen Ebenen ein. Insbesondere sollten Security-Vorfälle in der Automatisierungslösung keine sicherheitstechnischen Systeme oder andere sicherheitsbezogene Funktionen beeinträchtigen.

Die allgemeine Beschreibung der erreichbaren Security Levels nach 4.5 wird in dieser grundlegenden Anforderung angepasst mit dem Ziel, die Verfügbarkeit des Automatisierungssystems sicherzustellen, um der Verschlechterung oder Ablehnung wesentlicher Dienste entgegenzuwirken (Denial of service: DoS).

- SL 1 – Sicherstellen, dass das Automatisierungssystem unter normalen Produktionsbedingungen zuverlässig arbeitet und DoS-Situationen verhindert, die eine Person oder Stelle durch gelegentliche oder zufällige Handlungen verursacht hat.
- SL 2 – Sicherstellen, dass das Automatisierungssystem unter normalen und außergewöhnlichen Produktionsbedingungen zuverlässig arbeitet und DoS-Situationen durch Personen oder Stellen verhindert, die mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fertigkeiten und geringer Motivation vorgehen.

- SL 3 – Sicherstellen, dass das Automatisierungssystem unter normalen und außergewöhnlichen und extremen Produktionsbedingungen zuverlässig arbeitet und DoS-Situationen durch Personen oder Stellen verhindert, die mit raffinierten Mitteln, mittleren Ressourcen, automatisierungstechnischen Fertigkeiten und mittlerer Motivation vorgehen.
- SL 4 – Sicherstellen, dass das Automatisierungssystem unter normalen und außergewöhnlichen und extremen Produktionsbedingungen zuverlässig arbeitet und DoS-Situationen durch Personen oder Stellen verhindert, die mit raffinierten Mitteln, erheblichen Ressourcen, automatisierungstechnischen Fertigkeiten und hoher Motivation vorgehen.

Die folgende Tabelle zeigt auf, welche SR und RE bei einem zu erreichenden Security Level SL-C für die Ressourcenverfügbarkeit zutreffen.

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 7 – Ressourcenverfügbarkeit (RA)				
SR 7.1 – Schutz gegen DoS-Ereignisse	✓	✓	✓	✓
SR 7.1 RE 1 – Netzbelastung steuern		✓	✓	✓
SR 7.1 RE 2 – DoS-Auswirkungen auf andere Systeme oder Netze begrenzen			✓	✓
SR 7.2 – Ressourcenmanagement	✓	✓	✓	✓
SR 7.3 – Datensicherung im Automatisierungssystem	✓	✓	✓	✓
SR 7.3 RE 1 – Verifikation der Datensicherung		✓	✓	✓
SR 7.3 RE 2 – Automatisierung der Datensicherung			✓	✓
SR 7.4 – Wiederherstellung des Automatisierungssystems	✓	✓	✓	✓
SR 7.5 – Notstromversorgung	✓	✓	✓	✓
SR 7.6 – Netzwerk- und IT-Sicherheitseinstellungen	✓	✓	✓	✓
SR 7.6 RE 1 – Maschinen-lesbare Meldungen der momentanen IT-Sicherheitseinstellungen			✓	✓
SR 7.7 – Geringste Funktionalität	✓	✓	✓	✓
SR 7.8 – Verzeichnis der Komponenten eines Automatisierungssystems		✓	✓	✓

A.4 IEC 62443-4-1

Der letzte Stand wurde als *„Draft for Comments (DC)“* am 02.03.2015 veröffentlicht [10]. Die folgende Beschreibung bezieht sich auf die dem Autor letzte bekannte Arbeitsversion des Dokuments. Kommentare zum DC wurden zum Teil eingearbeitet.

Der Teil IEC 62443-4-1 spezifiziert die Prozessanforderungen für die Integration von Security in der Entwicklung von Produkten, die in Automatisierungslösungen eingesetzt werden. Es wird ein Security Entwicklungslebenszyklus („Secure Development Lifecycle, SDL“) definiert, der von der Definition der Security-Anforderungen über Security by Design, Sichere Implementierung (einschließlich Codierungsrichtlinien), Verifikation und Validierung, Security-Mängelbehandlung, Security-Patch-Management bis zum Zurückziehen des Produkts geht.

Die Anforderungen können für neue oder bestehende Prozesse angewendet werden, für die Entwicklung, Pflege und das Zurückziehen von Hardware, Software oder Firmware von neuen oder bestehenden Produkten. Die Adressaten dieses Dokuments sind die Verantwortlichen für die Entwicklung und Pflege der Produkte. Die Anforderungen adressieren nicht die Anwender der Produkte, die für das Design, Inbetriebnahme und Betrieb von Automatisierungslösungen verantwortlich sind; es geht um die Produkte, die in einer Automatisierungslösung eingesetzt werden.

Das Hauptziel ist, ein Rahmenwerk zu schaffen, um einen Ansatz für die Integration der Security in das Design der Produkte („Security by Design“) zu definieren, der auf einer Defense-in-Depth-Strategie basiert. Damit kann das Vertrauen gesteigert werden, dass die Security-Risiken, die mit dem Einsatz der Komponente oder des Automatisierungssystems verbunden sind, im Rahmen des akzeptablen Restrisikos entlang des Lebenszyklus bleiben. Ein weiteres Ziel der Anforderungen ist, den Entwicklungsprozess an den erhöhten Sicherheits-Bedürfnissen der Anwender auszurichten (Betreiber, Integratoren, Dienstleister für Wartung). Insbesondere müssen aus dem Prozess gut dokumentierte Richtlinien für die Security-Konfiguration, das Patch-Management und der Härtung entstehen sowie klare und kurze Kommunikationen über die Schwachstellen, die ggf. im Produkte entdeckt werden.

Im folgenden Bild werden die Beiträge der Design-Prinzipien im Rahmen einer Defense-in-Depth-Strategie für das Produkt dargestellt. Nicht dargestellt sind die Mängelbehandlung und das Patch-Management, die als Beitrag zur sicheren Implementierung zu sehen sind. Ein Schlüsselkonzept des Dokuments ist die Modellierung der Bedrohungen und die Durchführung von Analysen, um Gegenmaßnahmen in dem Produkt zu implementieren, siehe dazu auch Abschnitt 4.4. Auch in diesem Dokument ist das Reifegradmodell des Kapitels 5 relevant.

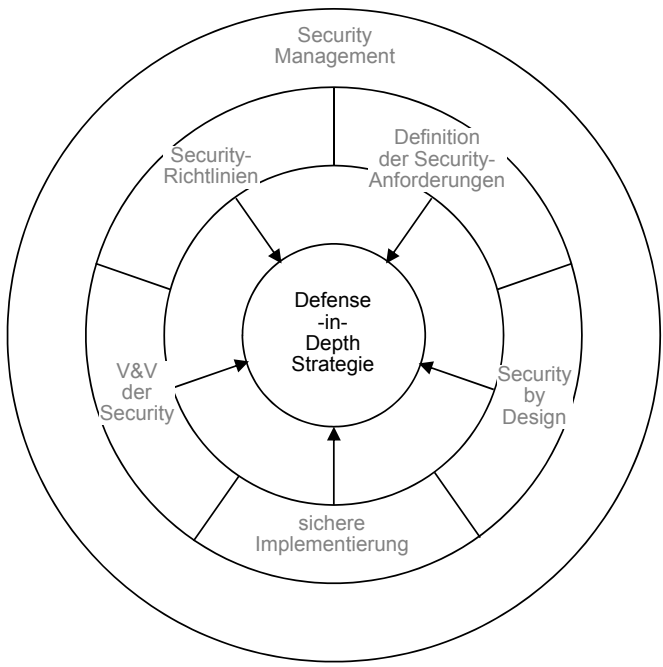

Bild 20 Die Defense-in-Depth-Strategie ist ein Schlüsselprinzip für Security im Produkt-Lebenszyklus.

Die Anforderungen werden in acht Tätigkeitsbereiche, sog. *„Practices“* gegliedert, die sich an dem dargestellten Zyklus orientieren. Die Tabelle in den Abschnitten gibt einen Überblick über den aktuellen Stand der Anforderungen. Da das Dokument noch vorläufig ist, wurde die englische Bezeichnung beibehalten.

Practice 1 – Security-Management (*Security Management, SM*)

Das Ziel des Security-Managements ist es, sicherzustellen, dass die Security-Aktivitäten geplant, dokumentiert und entlang des Lebenszyklus umgesetzt werden, um deren Effizienz sicherzustellen. Wichtig ist z. B. eine ausreichende Ressourcenplanung oder ein an die geforderte Security des Produkts angepasstes Lieferantenmanagement.

SM-1 – Development process	BR
SM-2 – Identification of responsibilities	BR
SM-3 – Identification of applicability	BR
SM-4 – Security expertise	BR
SM-5 – Process tailoring	BR
SM-6 – Code signing	BR
SM-7 – Development environment security	BR
RE (1) Controls for private keys	RE
SM-8 – Third party embedded component security	BR
SM-9 – Special purpose third party components	BR
SM-10 – Addressing of security-related issues	BR
SM-11 – Process verification	BR

Practice 2 – Definition der Security-Anforderungen (*Specification of security requirements, SR*)

Die Prozesse in diesem Abschnitt haben zum Ziel, die Security-Fähigkeiten zu dokumentieren, die vom Produkt in Rahmen seiner geplanten Einsatzumgebung erfüllt werden sollen. Die geplante Einsatzumgebung kann zum Beispiel den physischen Zugangs oder den Schutz durch eine externe Firewall einschließen. Die Teile IEC 62443-3-3 und IEC 62443-4-2 sind Kataloge möglicher Security-Fähigkeiten, die für das Produkt selbst oder für ergänzende Anforderungen an die Produktumgebung herangezogen werden können.

SR-1 – Product security context	BR
SR-2 – Threat model	BR
RE (1) Threat model updates	RE
SR-3 – Product security requirements	BR
SR-4 – Product security requirements content	BR
SR-5 – Security requirements review	BR

Practice 3 – Security by design (*Secure by design, SD*)

Die Prozesse in diesem Abschnitt sollen sicherstellen, dass das Produkt in seinem Design die Security integriert. Die Prozesse sollen in allen Phasen des Designs angewendet werden, von

der Konzeptphase bis zum detaillierten Design und über alle Ebenen des Produkt-Designs von der Architektur bis zum Auslegen der einzelnen Komponenten.

SD-1 – Secure design principles	BR
SD-2 – Defense in depth design	BR
SD-3 – Security design review	BR
SD-5 – Addressing security-related issues	BR
SD-6 – Secure design industry recommended practices	BR
RE (1) Industry recommended practices	RE

Practice 4 – Sichere Implementierung (*Secure implementation, SI*)

Die Prozesse in diesem Abschnitt sollen sicherstellen, dass die Produkt-Fähigkeiten sicher implementiert werden.

SI-1 – Security implementation review	BR
RE (1) Static code analysis scope	RE
SI-2 – Assessing security-related implementation issues	BR
SI-3 – Addressing security-related issues	BR
SI-4 – Secure Implementation recommended practices	BR

Practice 5 – Verifikation und Validierung der Security (*Security verification and validation testing, SV*)

Die Prozesse in diesem Abschnitt haben zum Ziel, das Testen zu dokumentieren, um zum Ersten sicherzustellen, dass alle Security-Anforderungen erfüllt werden. Ein zweites Ziel ist sicherzustellen, dass die Security des Produkts ausreichend gepflegt wird, wenn das Produkt in der geplanten Umgebung eingesetzt wird und für eine Defense-in-Depth-Strategie konfiguriert wird.

Das Testen der Security kann zu verschiedenen Zeitpunkten und von unterschiedlichem Personal entlang des Entwicklungs-Lebenszyklus durchgeführt werden, je nach Art des Testens und des Entwicklungsmodells des Herstellers. Zum Beispiel kann das sog. *„fuzzing testing“* während der Software-Entwicklung durch das Entwicklungsteam und später durch das Testteam durchgeführt werden.

Vier Arten von Testen werden in diesem Abschnitt angesprochen:

a) Testen der Security-Anforderungen: Dieses Testen fokussiert auf die Verifikation, dass alle Anforderungen des Security-Lastenhefts erfüllt werden.

b) Testen der Gegenmaßnahmen gegen Bedrohungen: Dieses Testen wird von Bedrohungsbäumen abgeleitet, die bei der Identifikation und der Modellierung der Bedrohungen erzeugt werden, und stellt sicher, dass die Gegenmaßnahmen effizient gegen die betrachteten Bedrohungen sind.

c) Allgemeines Testen von Schwachstellen: Dieses Testen fokussiert auf den Einsatz von Werkzeugen oder veröffentlichten Anleitungen, um potenzielle Schwachstellen zu entdecken.

d) Eindringungstests: Dieses Testen fokussiert auf den Missbrauch der Verfügbarkeit, Integrität und Vertraulichkeit des Produkts.

SV-1 – Security requirements testing	BR
SV-2 – Threat mitigation testing	BR
SV-3 – Vulnerability testing	BR
RE (1) Use of multiple tools	RE
RE (2) Development of tools when no tools available	RE
SV-4 – Penetration testing	BR
RE (1) Third party penetration testing	RE
SV-5 – Independence of testers	BR

Practice 6 – Security-Mängelbehebung (*Security defect management, DM*)

Diese Prozesse finden ihren Einsatz in der Behandlung von Security-Vorfällen von Produkten, die konfiguriert wurden, um eine Defense-in-Depth-Strategie (Practice 3) in der geplanten Einsatzumgebung umzusetzen (Practice 2).

DM-1 – Receiving notifications of security-related issues	BR
DM-2 – Reviewing security-related issues	BR
DM-3 – Assessing security-related issues	BR
DM-4 – Addressing security-related issues	BR
RE (1) Informing third parties of problems	RE
DM-5 – Disclosing security-related issues	BR
DM-6 – Periodic review of security defect management practice	BR

Practice 7 – Security-Patch-Management (*Security update management, PM*)

Die Prozesse in diesem Abschnitt werden verwendet, um sicherzustellen, dass Security-Aktualisierungen des Produkts auf Regression getestet werden und für die Anwender in einem angemessen Zeitraum zur Verfügung gestellt werden.

PM-1 – Security update qualification	BR
PM-2 – Security update documentation	BR
PM-3 – Dependent component or operating system security update documentation	BR
PM-4 – Security update delivery	BR
PM-5 – Timely delivery of security patches	BR

Practice 8 – Security-Richtlinien (*Security guidelines, SG*)

Diese Prozesse sollen sicherstellen, dass eine Dokumentation zur Verfügung gestellt wird, die beschreibt, wie das Produkt für die Defense-in-Depth-Strategie des Produkts im Rahmen seiner geplanten Einsatzumgebung (Practice 2) zu integrieren, konfigurieren und warten ist.

Der Teil IEC 62443-2-4 beschreibt zusätzliche Härtungsanforderungen für den Einsatz dieser Dokumentation durch Dienstleister für industrielle Automatisierungssysteme.

Die Umsetzung und die Aufrechterhaltung einer Defense-in-Depth-Strategie muss typischerweise Folgendes adressieren:

a) Prozesse und Richtlinien, die mit der Einsatzumgebung verbunden sind, wie in Practice 1 beschrieben,

b) Konzept der Netzwerkarchitektur, z. B. das Platzieren von Firewalls und den Einsatz von kompensierenden Security-Maßnahmen, siehe Practice 3,

c) Konfiguration der Security-Einstellungen und -Optionen, z. B. die Konfiguration der Firewall-Regeln und die Verwaltung der Nutzerkonten mit ihren Rechten,

d) die Verwendung von Werkzeugen, um die Härtung zu unterstützen.

In dem Abschnitt ist das Patchen nicht enthalten, weil dieses bereits in Practice 7 enthalten ist.

Der Abschnitt beschreibt auch Anforderungen für die Entwicklung und die Pflege der Dokumentation, insbesondere die Erzeugung, Pflege und Bereitstellung der Härtungsbeschreibung. Die Härtung des Produkts in einer Anlage erfolgt in der Regel auf Basis einer Risikobewertung, siehe dazu auch IEC 62443-3-2.

SG-1 – Product	BR
SG-2 – Defense in depth measures expected in the environment	BR
SG-3 – Security hardening guidelines	BR
SG-4 – Secure disposal guidelines	BR
SG-5 – Secure operation guidelines	BR
SG-6 – Account management guidelines	BR
SG-7 – Documentation review	BR

A.5 IEC 62443-4-2

Der letzte Stand wurde als *„Draft for Comments (DC)“* am 20.07.2015 veröffentlicht [11]. Die folgende Beschreibung bezieht sich auf die dem Autor letzte bekannte Arbeitsversion des Dokuments. Kommentare zum DC wurden zum Teil in der hier dargestellten Arbeitsversion eingearbeitet.

Dieser Teil der Norm erweitert die Systemanforderungen und weitergehenden Anforderungen (SR und RE) der IEC 62443-3-3 in einer Liste von Anforderungen (*CR, Component Requirement*) und weitergehenden Anforderungen (*RE, Requirement Enhancement*) an die Komponenten, die in einer Automatisierungslösung eingesetzt werden. Es werden vier Klassen unterschieden:

- Software Applikationen (*Applications*), z. B. Software für Archivierung oder Dokumentation,
- PC-basierte Stationen (*Host Devices*), z. B. Operator oder Engineering-Stationen,

- eingebettete Geräte (*Embedded Devices*), z. B. Speicherprogrammierbare Steuerungen oder Intelligente Elektronische Einheiten,
- Netzwerkkomponenten (*Network Devices*), z. B. Firewalls, Switches oder Gateways.

Um den Leser zu unterstützen, wird jede Anforderung mit einer Begründung und zusätzlichen Informationen ergänzt. Wie in IEC 62443-3-3 werden die CRs und REs auf erreichbare Levels der Komponenten abgebildet (*Component Capability Level*). Die Levels werden von den erreichbaren Levels der entsprechenden Systemanforderungen des Teils IEC 62443-3-3 abgeleitet. Auch die thematische Unterteilung entspricht den grundlegenden Anforderungen FR 1 bis FR 7 nach IEC 62443-1-1.

Viele Anforderungen sind gemeinsam zu allen vier Arten von Komponenten und werden als Komponentenanforderung CR aufgelistet. Gibt es abhängig von der Komponentenklasse Besonderheiten, so werden diese als Anforderungen an Applikationen (*ACR, Application Component Requirement*), PC-basierte Stationen (*HCR, Host Device Requirement*), Netzwerkkomponenten (*NCR, Network Component Requirement*) oder eingebettete Geräte (*ECR, Embedded Component Requirement*) unterschieden.

Die folgende Tabelle gibt einen Überblick, ob für jede Systemanforderung bzw. weitergehende Anforderung (SR / RE) eine gemeinsame Anforderung an alle Komponenten (Markierung bei CR) oder je nach Art der Komponente eine unterschiedliche Anforderung (Markierung bei ACR, HCR, ECR bzw. NCR) daraus abgeleitet wird.

SRs und REs	CR	ACR	HCR	ECR	NCR
SR 1.1 – Identifizierung und Authentifizierung von menschlichen Nutzern	✓				
SR 1.1 RE 1 – Eindeutige Identifizierung und Authentifizierung	✓				
SR 1.1 RE 3 – Multifaktor-Authentifizierung über nicht vertrauenswürdige Netze	✓				
SR 1.1 RE 3 – Multifaktor-Authentifizierung über alle Netze	✓				
SR 1.2 – Identifizierung und Authentifizierung von Softwareprozessen und Geräten	✓				
SR 1.2 RE 1 – Eindeutige Identifizierung und Authentifizierung	✓				
SR 1.3 – Nutzerkontenverwaltung	✓				
SR 1.3 RE 1 – Einheitliche Nutzerkontenverwaltung	✓				
SR 1.4 – Verwaltung der Kennungen	✓				
SR 1.5 – Verwaltung der Authentifikatoren	✓				
SR 1.5 RE 1 – Beglaubigung der Identität von Softwareprozessen durch Hardwaremaßnahmen	✓				
SR 1.6 – Management drahtloser Zugriffsverfahren					✓
SR 1.6 RE 1 – Eindeutige Identifizierung und Authentifizierung					✓

SRs und REs	CR	ACR	HCR	ECR	NCR
SR 1.7 – Stärke der Authentifizierung durch Passwörter	✓				
SR 1.7 RE 1 – Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Nutzer	✓				
SR 1.7 RE 2 – Lebensdauerbeschränkungen von Passwörtern für alle Nutzer	✓				
SR 1.8 – PKI-Zertifikate	✓				
SR 1.9 – Stärke der Authentifizierung durch öffentliche Schlüssel	✓				
SR 1.9 RE 1 – Beglaubigung öffentlicher Schlüssel durch Hardwaremaßnahmen	✓				
SR 1.10 – Rückmeldung vom Authentifikator	✓				
SR 1.11 – Erfolglose Anmeldeversuche	✓				
SR 1.12 – Nutzungshinweis	✓				
SR 1.13 – Zugriff über nicht vertrauenswürdige Netze					✓
SR 1.13 RE 1 – Genehmigung ausdrücklicher Anmelde-begehren					✓
CR 1.14 – Strength of symmetric key authentication	✓				
CR 1.14 RE1 – ISO/IEC 19790 Level 3 security for symmetric keys	✓				
CR 1.14 RE2 – ISO/IEC 19790 Level 4 security for symmetric keys	✓				
SR 2.1 – Durchsetzung der Autorisierung	✓				
SR 2.1 RE 1 – Durchsetzung der Autorisierung für alle Nutzer	✓				
SR 2.1 RE 2 – Abbildung der Berechtigung auf Rollen	✓				
SR 2.1 RE 3 – Eingriffe des Aufsichtspersonals	✓				
SR 2.1 RE 4 – Doppelte Zustimmung	✓				
SR 2.2 – Nutzungskontrolle von Funkverbindungen	✓				
SR 2.2 RE 1 – Nicht genehmigte drahtlose Geräte erkennen und anzeigen	keine				
SR 2.3 – Nutzungskontrolle von tragbaren und mobilen Geräten	✓				
SR 2.3 RE 1 – Security-Status tragbarer und mobiler Geräte durchsetzen	keine				
SR 2.4 – Mobiler Code		✓	✓	✓	✓
SR 2.4 RE 1 – Prüfung der Integrität mobilen Codes		✓	✓	✓	
SR 2.5 – Sitzungssperrung	✓				
SR 2.6 – Beendigung einer Fernzugriffssitzung	✓				
SR 2.7 – Begrenzung der Anzahl gleichzeitiger Sitzungen	✓				
SR 2.8 –Prüfbare Ereignisse und deren Aufzeichnung	✓				
SR 2.8 RE 1 – Zentral verwaltete systemweite Ereignis-aufzeichnung	✓				

SRs und REs	CR	ACR	HCR	ECR	NCR
SR 2.9 – Speicherkapazität für Aufzeichnungen	✓				
SR 2.9 RE 1 – Warnung, wenn die Kapazitätsgrenze zur Speicherung von Ereignisdatensätzen erreicht ist	✓				
SR 2.10 – Reaktion auf ausgefallene Ereignisdatenverarbeitung	✓				
SR 2.11 – Zeitstempel	✓				
SR 2.11 RE 1 – Interne Systemtakte	✓				
SR 2.11 RE 2 – Schutz und Integrität der Zeitquelle	✓				
SR 2-12 – Nicht-Abstreitbarkeit	✓				
SR 2.12 RE 1 – Nicht-Abstreitbarkeit für alle Nutzer	✓				
SR 3.1 – Kommunikationsintegrität	✓				
SR 3.1 RE 1 – Kryptographische Schutzmaßnahmen zur Bewahrung der Integrität	✓				
SR 3.2 – Schutz vor Schadcode		✓	✓	✓	✓
SR 3.2 RE 1 – Schutz vor Schadcode an Eingangs- und Ausgangspunkten		✓			
SR 3.2 RE 2 – Zentrales Management und Meldewesen zum Schutz vor Schadcode	keine				
SR 3.3 – Verifikation der IT-Sicherheitsfunktionalität	✓				
SR 3.3 RE 1 – Automatisierte Mechanismen zur Verifikation der IT-Sicherheitsfunktionalität	✓				
SR 3.3 RE 2 – Verifikation der IT-Sicherheitsfunktionalität im laufenden Betrieb	✓				
SR 3.4 – Software- und Informationsintegrität	✓				
SR 3.4 RE 1 – Automatisierte Hinweise auf IT-Sicherheits-verstöße	✓				
SR 3.5 – Eingabevalidierung	✓				
SR 3.6 – Vorbestimmte Zustände der Ausgänge	✓				
SR 3.7 – Fehlerbehandlung	✓				
SR 3.8 – Sitzungsintegrität	✓				
SR 3.8 RE 1 – Annullierung der Sitzungskennungen nach Sitzungsbeendigung	✓				
SR 3.8 RE 2 – Erzeugung einer eindeutigen Sitzungskennung	✓				
SR 3.8 RE 3 – Zufälligkeit der Sitzungskennungen	✓				
SR 3.9 – Schutz von Prüfinformationen	✓				
SR 3.9 RE 1 – Ereignisdatensätze auf nur einmal beschreib-baren Speichermedien	✓				
CR 3.10 – Beweis der Originalität		✓	✓	✓	✓
CR 3.10 RE 1 – Nicht-klonbarer Beweis der Originalität			✓		✓
SR 4.1 – Vertraulichkeit von Informationen	✓				

SRs und REs	CR	ACR	HCR	ECR	NCR
SR 4.1 RE 1 – Schutz der Vertraulichkeit bei der Speicherung oder Übertragung über nicht vertrauenswürdige Netze	✓				
SR 4.1 RE 2 – Schutz der Vertraulichkeit über Zonengrenzen hinweg	✓				
SR 4.2 – Dauerhaftigkeit von Informationen	✓				
SR 4.2 RE 1 – Säuberung gemeinsam genutzter Speicher	✓				
SR 4.3 – Verwendung von Verschlüsselung	✓				
SR 5.1 – Netzaufteilung	✓				
SR 5.1 RE 1 – Physikalische Netzaufteilung	keine				
SR 5.1 RE 2 – Unabhängigkeit von nicht-automatisierungstechnischen Netzen	keine				
SR 5.1 RE 3 – Logische und physikalische Isolierung kritischer Netze	keine				
SR 5.2 – Schutz der Zonengrenze					✓
SR 5.2 RE 1 – Deny by default, allow by exception					✓
SR 5.2 RE 2 – Inselmodus					✓
SR 5.2 RE 3 – Fail close					✓
SR 5.3 – Beschränkung der Verwendung der persönlichen Kommunikation					✓
SR 5.3 RE 1 – Verbot der Verwendung der persönlichen Kommunikation	✓				
SR 5.4 – Partitionierung von Anwenungen	✓				
SR 6.1 – Zugriffsmöglichkeit auf Ereignisprotokolle	✓				
SR 6.1 RE 1 – Programmgesteuerter Zugriff auf Ereignisprotokolle	✓				
SR 6.2 – Kontinuierliche Überwachung	✓				
SR 7.1 – Schutz gegen DoS-Ereignisse	✓				
SR 7.1 RE 1 – Netzbelastung steuern	✓				
SR 7.1 RE 2 – DoS-Auswirkungen auf andere Systeme oder Netze begrenzen	✓				
SR 7.2 – Ressourcenmanagement	✓				
SR 7.3 – Datensicherung im Automatisierungssystem	✓				
SR 7.3 RE 1 – Verifikation der Datensicherung	✓				
SR 7.3 RE 2 – Automatisierung der Datensicherung	✓				
SR 7.4 – Wiederherstellung des Automatisierungssystems	✓				
SR 7.5 – Notstromversorgung	✓				
SR 7.6 – Netzwerk- und IT-Sicherheitseinstellungen	✓				
SR 7.6 RE 1 – Maschinen-lesbare Meldungen der momentanen IT-Sicherheitseinstellungen	✓				
SR 7.7 – Geringste Funktionalität	✓				
SR 7.8 – Verzeichnis der Komponenten eines Automatisierungssystems	✓				

B Weitere Dokumente der IEC 62443

B.1 IEC 62443-1-1

Die Edition 1 dieses Teils [2] wurde im Jahr 2009 als technische Spezifikation („*TS, Technisal Specification*“) veröffentlicht. Die Edition 2 ist in Bearbeitung.

Das Dokument definiert die Begriffe, Konzepte und Methoden, die übergeordnet die Grundsätze und Basis für die anderen Teile der Reihe IEC 62443 bilden. Insbesondere werden in der Edition 2 die im Abschnitt 4 beschriebenen Konzepte detailliert dargestellt werden.

Das Dokument beschreibt den Anwendungsbereich, des Standards. Man kann diesen aus verschiedenen Geschichtspunkten beschreiben:

- Abgedeckte Funktionalitäten: Der Standard fokussiert hauptsächlich auf IACS, die als Referenzmodelle beschrieben werden.
- Systeme und Schnittstellen: Der Standard schließt alle Bestandteile, die den sicheren und verlässlichen Betrieb des gesamten IACS betreffen, ein.
- Aktivitäten: Ein System fällt in den Anwendungsbereich des Standards, wenn es den vorhersagbaren und sicheren Betrieb der Produktion, den Schutz des Personals und der Produktion, die Verfügbarkeit, Effizienz und Qualität der Produktion, den Schutz der Umwelt oder die Gesetzeskonformität zum Ziel hat.
- Betriebsmittel: Der Standard deckt die Betriebsmittel ab, die einen wirtschaftlichen Wert für den Betrieb oder die Produktion haben und erforderlich für den sicheren Betrieb des Prozesses und den Schutz von Personal und Umgebung, sowie für den Schutz des geistigen Eigentums des Produktions- oder Betriebsprozesses sind.

B.2 IEC 62443-1-2

Es ist vorgesehen, ein Wörterbuch mit den Bezeichnungen und Abkürzungen zu veröffentlichen, wenn alle Dokumente als Standard angenommen sind. Zum Zeitpunkt der Entstehung dieses Buch wird ein elektronisches Wörterbuch von der ISA-99 entwickelt und gepflegt.

B.3 IEC 62443-1-3

Das Dokument [3] soll die wesentlichen Metriken für die Verwaltung eines Security-Programms während des Lebenszyklus eines IACS definieren. Die Ziele des Dokuments schließen Folgendes ein:

- Beschreibung eines Prozesses zur Spezifikation der Konformität zu relevanten Anforderungen einschließlich eines Mindestsatzes an Metriken, um die Konformität zu messen,
- Belegung, dass der Mindestsatz an Metriken die Konformität nachprüfbar, vollständig und präzise nachweist,
- folgende Kriterien müssen von den Konformitätsmetriken erfüllt werden:
  - messbar im Sinne, dass sie konsistent mit objektive Kriterien gemessen werden,
  - kontextspezifisch im Sinne, dass sie für den jeweiligen Anwender relevant sind,
  - dargestellt als eine Zahl oder ein Prozentsatz, nicht als qualitative Aussage wie niedrig, mittel, hoch,
  - dargestellt als mindestens eine Maßeinheit,
- Darstellung, dass die Metriken helfen können, um Leistungs-, Reife- und Risiko-Bewertung vorzunehmen,
- Darstellung, dass die Metriken helfen können, die Widerstandsfähigkeit von industriellen Automatisierungssystemen gegen Cyberattacken zu bewerten.

Dieses Dokument wurde Anfang 2014 als Entwurf einer technischen Spezifikation („*DTS; Draft Technical Specification*“) veröffentlicht, der abgelehnt wurde. Der Inhalt entsprach nicht dem Anwendungsbereich und den Zielen, die hier beschrieben sind. Ein neuer Anlauf wurde im Jahr 2016 als neuer Vorschlag („*NP, New Proposal*“) vorgenommen, der ebenfalls dem Ziel nicht entspricht. Es ist zu erwarten, dass auch dieser Vorschlag abgelehnt wird.

Die Ablehnung der Inhalte beruht wahrscheinlich auf der Tatsache, dass die gesteckten Ziele eine Messbarkeit der Security annehmen. Die in diesem Buch beschriebenen Inhalte verdeutlichen jedoch, dass man die Security auf der Basis von Expertenwissen zwar bewerten kann, jedoch eine Messung, wie sie die Physik kennt, weder sinnvoll noch aussagekräftig ist.

B.4 IEC 62443-2-3

Dieser Teil der IEC 62443 [5] ist ein technischer Bericht (“TR, Technical Report“), der die Anforderungen für alle Stakeholder eines IACS, die an der Erstellung und Pflege eines Patch-Management-Programms beteiligt sind, beschreibt.

Es wird ein Format für die Verteilung von Informationen über Security Patches empfohlen. Das Dokument beinhaltet eine Beschreibung von einigen Aktivitäten zur Entwicklung der Patch-Information durch die Hersteller sowie zur Auslegung und Installation von Patches durch die Betreiber. Das Austauschformat kann auch für nicht Security-relevante Patches und Aktualisierungen verwendet werden.

Der technische Bericht gibt eine Orientierung für alle Arten von Patches, sei es zur Korrektur von Fehlern, Zuverlässigkeitsproblemen oder Security-Schwachstellen. Es wird nicht unterschieden zwischen Patches, die für Betriebssysteme, Applikationen oder Geräte relevant sind, oder ob die Patches von Herstellern von Infrastruktur-Komponenten oder weiteren IACS-Komponenten oder Applikationen herausgegeben werden.

Der Patch-Zustand entlang seines Lebenszyklus wird in der folgenden Tabelle dargestellt. Der Begriff IACS-Hersteller schließt hier sowohl Produkt-Hersteller, dessen Produkte in der Auto-

matisierungslösung integriert sind, als auch Dienstleister für Integration oder Wartung ein. Je nach Gegebenheiten kann die eine oder andere dieser Rolle die beschriebenen Aufgaben erfüllen.

Patch-Zustand	Definition	verwaltet durch
verfügbar	Der Patch wurde von einer Drittstelle oder von einem IACS-Hersteller zur Verfügung gestellt, wurde aber noch nicht getestet.	Betreiber IACS-Hersteller
in Test	Der Patch wird von einem IACS-Hersteller getestet.	IACS-Hersteller
nicht genehmigt	Der Patch ist beim Test durch einen ICAS-Hersteller durchgefallen und sollte nicht eingesetzt werden bis der IACS-Hersteller bestätigt, dass der Patch genehmigt wurde.	IACS-Hersteller
nicht anwendbar	Der Patch wurde getestet, ist jedoch nicht relevant für die spezifische IACS-Umgebung.	IACS-Hersteller
genehmigt	Der Patch wurde erfolgreich durch den IACS-Hersteller getestet.	IACS-Hersteller
freigegeben	Der Patch wurde für den Einsatz vom IACS-Hersteller oder von einer Drittstelle freigegeben oder der Patch kann direkt vom Betreiber für das eigenentwickelte System eingesetzt werden.	Betreiber IACS-Hersteller
im internen Test	Der Patch wird durch das Testteam des Betreibers getestet.	Betreiber
nicht erlaubt	Der Patch hat den internen Test nicht bestanden oder ist nicht anwendbar.	Betreiber
erlaubt	Der Patch wurde vom Betreiber freigegeben und erfüllt die Organisationsstandards für die Aktualisierung von Geräten oder durch Überprüfung wurde festgelegt, dass kein Test erforderlich ist.	Betreiber
wirksam	Der Patch wurde vom Betreiber zum Einsatz veröffentlicht.	Betreiber
installiert	Der Patch wurde in der Automatisierungslösung installiert.	Betreiber

Das Patch-Management ist eine wesentliche proaktive Maßnahme zur Reduzierung der Wahrscheinlichkeit, dass eine Anlage in Betrieb kompromittiert wird. Der IACS-Hersteller hat hier die wichtige Verantwortung festzulegen, welcher Patch für das Produkt relevant ist und getestet werden sollte.

IACS-Hersteller sollten:

- Die Prozedur zum Patchen der Software für ihre Produkte und Systeme dokumentieren;
- alle Patches qualifizieren, d. h. Anwendbarkeit und Kompatibilität analysieren und verifizieren, einschließlich gegebenenfalls der Patches der Hersteller des Betriebssystems oder der Fremdsoftware, die im Produkt verwendet werden;
- eine Liste aller Patches mit deren Genehmigungsstatus zur Verfügung stellen;
- regelmäßig die Betreiber informieren und die Liste aktualisieren, idealerweise innerhalb von 30 Tagen nach der Herausgabe eines Patches vom Hersteller des Betriebssystems oder der Fremdsoftware;
- eine geeignete Warnung (mindestens zwei Jahre im Voraus) über Komponenten, die das Ende ihrer Lebenszeit erreichen haben und für die kein weiterer Patch mehr erstellt wird;
- die Betreiber über die Richtlinien für den Support der Produkte informieren.

Betreiber haben die Verantwortung, die Sicherheit, Zuverlässigkeit, Funktionsfähigkeit, Security und Qualität ihres Betriebs aufrecht zu halten. Ein wichtiger Teil hierzu ist die Zusicherung der Security mit dem Patchen der Betriebsmittel des IACS.

Betreiber sollten:

- ein Inventar über alle elektronischen Betriebsmittel des IACS erstellen und pflegen, die durch Veränderung ihrer Funktionalität, Konfiguration, Betrieb, Software, Firmware usw. aktualisiert werden können. Diese Geräte sollten als „aktualisierbare Geräte“ gekennzeichnet werden;
- eine genaue Aufzeichnung der aktuell installierten Versionen jedes Geräts, sog. „installierte Versionen“, erstellen und pflegen;
- regelmäßig bestimmen, welche Aktualisierung für jedes Gerät, sog. „letzte Versionen“, verfügbar sind;
- regelmäßig die „freigegebenen Versionen“ der Aktualisierungen bestimmen, die vom IACS-Hersteller als kompatibel gekennzeichnet sind und der Richtlinie des Betreibers für „aktualisierbare Geräte“ entsprechen;
- das Einspielen des Patches in einer Art testen, die genau der Produktionsumgebung entspricht, um sicherzustellen, dass die Zuverlässigkeit und Funktionalität des IACS nicht negativ beeinflusst wird, wenn die Patches in der aktuellen Produktionsumgebung installiert werden. Patches, die den Test bestanden haben, werden als „erlaubte Patches“ bezeichnet;
- das Patchen des IACS mit erlaubten, wirksamen Patches zu der nächstmöglichen Gelegenheit innerhalb der Randbedingungen des Designs (z. B. Redundanz, Fehlertoleranz, funktionale Sicherheit) und der Betriebsanforderungen (z. B. ungeplanter Stillstand, geplanter Stillstand, während des Betriebs) einplanen;
- die Aufzeichnungen regelmäßig für jedes aktualisierbare Gerät bezüglich installierter, genehmigter und wirksamer Versionen aktualisieren;
- einen geplanten Zeitabstand für das Einspielen von Patches identifizieren (z. B. wann Patches zur Verfügung stehen; maximal jährlich);
- Patches einspielen und/oder Gegenmaßnahmen umsetzen, um Security-Schwachstellen zu kompensieren.

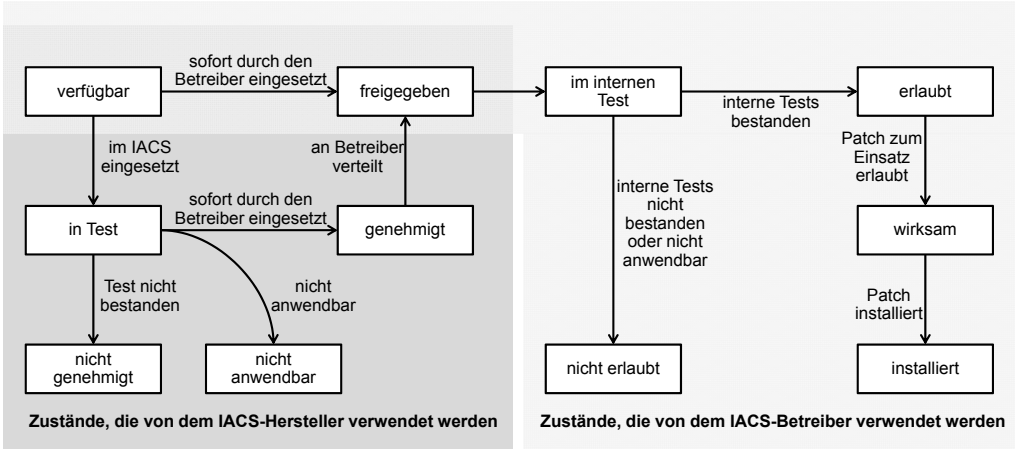

Bild 21 Patch-Zustandsmodell

B.5 IEC 62443-3-1

Dieser technische Bericht der IEC-62443-Serie [7] stellt eine Bewertung von verschiedenen Werkzeugen, Gegenmaßnahmen und Technologien dar, die zum Schutz von Netzwerk-basierten elektronischen UACS eingesetzt werden können. Es werden mehrere Kategorien auf Automatisierungssysteme fokussierter Technologien beschrieben. In jeder Kategorie werden die Produkttypen, die in der Kategorie verfügbar sind, die Vor- und Nachteile bezüglich der erwarteten Bedrohungen und bekannten Schwachstellen beim Einsatz dieser Produkte in IACS-Umgebungen und die Empfehlungen und Leitfäden beim Einsatz der Produkte und/oder Gegenmaßnahmen behandelt.

Die Defense-in-Depth-Strategie liegt auch diesem Dokument zugrunde und schließt folgende Auswahl von Technologien ein:

- Authentifikation und Autorisierung,
- Filtern, Blockieren und Zugangskotrolle,
- Verschlüsselung,
- Datenvalidierung,
- Messung,
- Überwachungs- und Detektionswerkzeuge,
- Betriebssysteme.

Zusätzlich ist eine Nicht-Security-Technologie äußerst wichtig und wird in dem technischen Bericht behandelt: der physische Zugangsschutz.

Das Ziel des Dokuments ist, die Security-Technologien, -Werkzeuge und -Maßnahmen zu definieren und kategorisieren, um eine gemeinsame Basis für weitere Berichte und Normen zu liefern. Jede Technologie wird bezüglich der folgenden Gesichtspunkte diskutiert:

- Security-Schwachstelle, die von der Technologie, dem Werkzeug oder der Maßnahme adressiert wird,
- typische Auslegung,
- bekannte Fehler und Schwächen,
- Bewertung des Einsatzes in einer IACS-Umgebung,
- zukünftige Weiterentwicklungen,
- Empfehlungen und Leitfaden,
- Informationsquellen und Referenzmaterial.

Der technische Bericht soll den aktuellen Kenntnisstand der Security-Technologien, -Werkzeuge und -Maßnahmen dokumentieren, die in einer IACS-Umgebung einsetzbar sind, klar definieren, welche Technologien heute angemessen eingesetzt werden können, und Bereiche definieren, in denen weitere Forschungsarbeiten erforderlich sind.

B.6 IEC 62443-3-2

Dieser Teil [8] definiert die Vorgehensweise und die Anforderungen, um ein IACS als zu betrachtendes System zu definieren, dieses in Zonen und Conduits aufzuteilen, Risiken zu bewerten, die zu erreichenden Security-Levels festzulegen und die Security-Anforderungen zu dokumentieren.

Der Betreiber und der Systemintegrator sollten eng zusammenarbeiten, um folgende Schritte durchzuführen:

- Identifikation des zu betrachtenden Systems, einschließlich der Festlegung des Security-Perimeters und die Identifikation aller Zugangspunkte zum zu betrachtenden System;
- Durchführung einer groben Risikobewertung, um das Risiko zu identifizieren, das das zu bewertende System unter ungünstigsten Randbedingungen für die Organisation bildet;
- Zonen und Conduits bilden, in dem IACS- und zugehörige Assets auf Basis der groben Risikobewertung eingeteilt werden. Die Einteilung kann auch auf Basis von Kriterien, z. B. die Kritikalität der Betriebsmittel, Betriebsfunktionen, physische oder logische Lage, Zugriffsbedarf (z. B. nach dem Prinzip der Mindestrechte) oder verantwortliche Organisation, erfolgen;
- Trennung der in Zonen und Conduits eingeteilten Betriebsmittel von den anderen Betriebsmitteln der Organisation;
- Erstellung einer Darstellung aller Zonen und Conduits des zu betrachtenden Systems. Alle Betriebsmittel müssen einer Zone oder einem Conduit zugeteilt werden. Die Darstellung sollte für jede Zone mit den dazugehörigen Conduits folgende Informationen enthalten:
  - Name und/oder Kennung,
  - logische Begrenzung,
  - ggf. physische Begrenzung,
  - Liste aller physischen und logischen Zugangspunkte und der zugehörigen Begrenzungsgeräte,
  - für jeden Zugangspunkt eine Liste der Datenflüsse,
  - relevante Security-Anforderungen,
  - zu erreichender Security-Level,
  - relevante Security-Richtlinien,
  - Annahmen und externe Randbedingungen;
- Erstellung eines Security-Lastenhefts, um die verbindlichen Security-Funktionen des zu betrachtenden Systems zu dokumentieren. Die Basis dafür sind die detaillierte Risikobewertung und die übergeordneten Security-Anforderungen aus Richtlinien der Organisation oder des Standorts, Normen oder relevanten Gesetzgebungen. Das Security-Lastenheft sollte mindestens folgende Beschreibungen beinhalten:
  - eine grobe Beschreibung des zu betrachtenden Systems,
  - die physische und logische Umgebung des zu betrachtenden Systems,
  - die Bedrohungslage, die auf das zu betrachtende System Einfluss haben kann,

– die verbindlichen Security-Funktionen,
– das akzeptable Restrisiko,
– die Gesetzesanforderungen, die für das zu betrachtende System relevant sind.

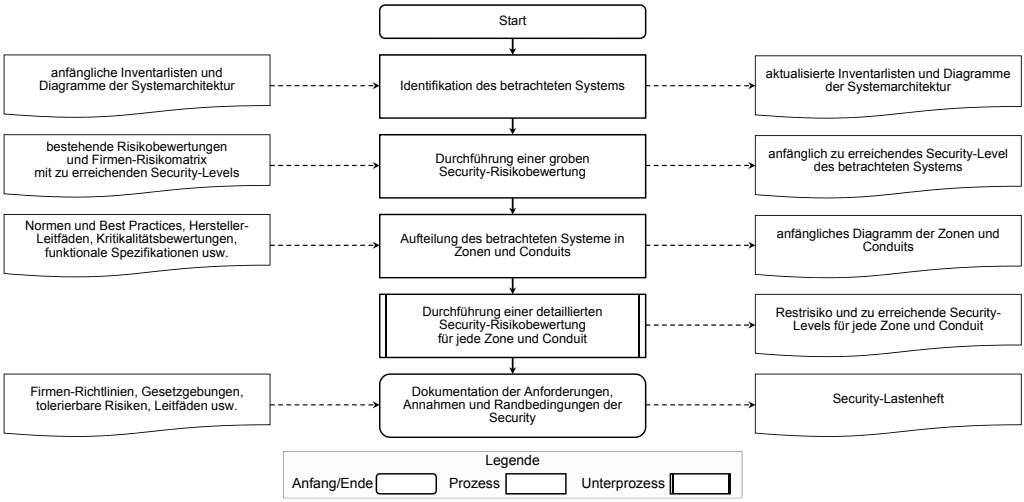

Bild 22 Ablaufplan für die Bestimmung von Zonen und Conduits

Literaturverzeichnis

[1] DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
(ISO/IEC 27001:2013 + Cor. 1:2014)

[2] IEC 62443-1-1: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
(IEC/TS 62443-1-1:2009)

[3] IEC 62443-1-3: Security for industrial automation and control systems – Part 1-3: Cyber security system conformance metrics
(Draft for Comments: 05.10.2015)

[4] IEC 62443-2-1 (Ed. 2.0): Security for industrial automation and control systems – Part 2 1: Requirements for an IACS security management system
(Draft for Comments: 26.09.2012)

[5] IEC 62443-2-3: Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment
(IEC TR 62443-2-3:2015)

[6] IEC 62443-2-4: Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
(IEC 62443-2-4:2015)

[7] IEC 62443-3-1: Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems
(IEC/TR 62443-3-1:2009)

[8] IEC 62443-3-2 (Ed. 1): Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design
(New Proposal: 13.10.2015)

[9] DIN IEC 62443-3-3: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme – Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level
(IEC 62443-3-3:2013 + Cor.:2014)

[10] IEC 62443-4-1 (Ed. 1): Security for industrial automation and control systems – Part 4-1: Secure Product Development Lifecycle Requirements
(Draft for Comments: 02.03.2015)

[11] IEC 62443-4-2 (Ed. 1): Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components
(Draft for Comments: 20.07.2015)

[12] VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung – Blatt 1: Allgemeines Vorgehensmodell
(VDI/VDE-Richtlinien, Januar 2011)

[13] Siemens AG – Industry White Paper V1.0 Industrial Security – Security-Konzept zum Schutz industrieller Anlagen, August 2013

Stichwortverzeichnis

SIEMENS

DFFA-A0105-00

Produktivität umfassend schützen

Industrial Security

Mit zunehmender Digitalisierung wird umfassende Sicherheit in der Automatisierung immer wichtiger. Deshalb ist Industrial Security ein Kernelement von Digital Enterprise, dem Lösungsansatz von Siemens auf dem Weg zu Industrie 4.0.

Mit Defense in Depth bietet Siemens ein vielschichtiges Konzept, das Ihre Anlage sowohl rundum als auch in die Tiefe schützt. Das Konzept basiert auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität nach den Empfehlungen der ISA 99/IEC 62443.

Anlagensicherheit

Sicherer physischer Zugang von Personen zu kritischen Komponenten und Einsatz von Plant Security Services

Netzwerksicherheit

Schutz von Automatisierungsnetzen gegen unbefugte Zugriffe durch Netzzugangsschutz, Netzsegmentierung und verschlüsselte Kommunikation

Systemintegrität

Sicherung der Systemintegrität durch systemeigene Schutzfunktionen

Defense in Depth
Industrial Security berücksichtigt Anlagensicherheit, Netzwerksicherheit und Systemintegrität

siemens.de/industrial-security

VDE VERLAG

LESER

Dieser Leitfaden wendet sich an alle, die mit Planung und Umsetzung von geeigneten Security-Maßnahmen im industriellen Umfeld befasst sind, seien es **Entscheider, technische Leiter, Geschäftsführer** oder **Ingenieure** und **Techniker**, sowie **Studierende.**

INHALT

Zu wenig Sicherheit ist fahrlässig, zu viel Sicherheit ist unwirtschaftlich.

Erstmals rückt die Angst vor Cyberangriffen bei einer aktuellen Umfrage unter die drei größten Unternehmensrisiken auf. Cloud, Datenschutz, Mobile oder das Internet der Dinge sind wichtige Faktoren für anstehende Veränderungen in IT-Sicherheitsfragen. Ein IT-Experte formulierte es so: „Ohne IT-Sicherheit wird Industrie 4.0 nicht akzeptiert."

Im Zuge der zunehmenden Zugriffe von außen, wächst die Bedeutung von Schutzkonzepten, was die deutsche Regierung durch die Verabschiedung des IT-Sicherheitsgesetzes erkannt hat. Betreiber kritischer Infrastrukturen müssen IT-Security-Mindeststandards einhalten und ihre Anlagen gegen Cyberangriffe schützen. Wirksame Schutzkonzepte lassen sich nur mit einem Bündel abgestimmter organisatorischer und technischer Maßnahmen umsetzen. Dabei sind alle Beteiligten gefordert, die Produkthersteller, die Integratoren und die Betreiber müssen Hand in Hand ganzheitliche Lösungen erarbeiten.

Die Normenreihe IEC 62443 adressiert die Belange ganzheitlicher Lösungen zum Schutz von industriellen Anlagen und richtet sich an alle Akteure, die an deren Erstellung beteiligt sind. Sie ist dementsprechend umfangreich und komplex. Dieser kurze Leitfaden gibt einen Überblick über die Normenreihe, fasst die wesentlichen Konzepte und Ideen zusammen und zeigt konkrete Umsetzungsmöglichkeiten auf.

AUTOR

Dr. Pierre Kobes ist Product and Solution Security Officer bei der Siemens AG. Er ist verantwortlich für Normen, Regulierungen und Zertifizierungen für die Divisionen Digital Factory und Process Industries and Drives. Er hat den Standard IEC 62443 miterarbeitet und ist in verschiedenen Standardisierungsgremien in Deutschland und international tätig.

www.vde-verlag.de