# 5 Konzepte der IEC 62443

Die Norm IEC 62443 basiert auf einigen übergeordneten Grundkonzepten. In der ersten Edition des Teils IEC 62443-1-1 [3], der 2010 veröffentlicht wurde, sind einige dieser Konzepte beschrieben. Eine Aktualisierung des Dokuments ist in Arbeit, dass die folgenden Konzepte detaillierter beschreiben wird.

## 5.1 Tiefgestaffelte Verteidigung (Defense-in-Depth)

Defense in Depth – dieses wichtige Konzept basiert auf der Erkenntnis, dass beim Schutz der industriellen Anlagen gegen Cyberangriffe der Beitrag aller Protagonisten erforderlich ist: Betreiber, Systemintegratoren, Wartungsdienstleister sowie Produkthersteller. Eine einzige Maßnahme ist im Allgemein nicht ausreichend, um einen angemessenen Schutz zu erreichen. Vielmehr müssen mehrere, untereinander abgestimmte und koordinierte Securitymaßnahmen 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 und werden von dem Dokument IEC 62443-2-1 [5] adressiert. Sie bestehen weitgehend aus organisatorischen und aus Objektsicherungsmaßnahmen. Eine Grundvoraussetzung jedes Schutzkonzepts beginnt mit der Sensibilisierung der Mitarbeiter für die Gefahren von Cyberangriffen. Die Norm fordert definierte Richtlinien und Prozesse zum Betrieb der Automatisierungslösung aber auch Kompetenzaufbau durch Informationsveranstaltungen oder Schulungen und klare Verantwortlichkeitsstrukturen in der Organisation. Zum Beispiel ist es sehr wichtig, die Zugriffsrechte aller Nutzer der Automatisierungslösung zu definieren und auf das minimal Notwendige einzugrenzen. Zu nennen ist auch, im Voraus Maßnahmen festzulegen, um das Aufrechterhalten des Betriebs im Fall eines erfolgreichen Cyberangriffs sicherstellen sollen, (*Business Continuity Plan*). Der Betreiber muss auch dafür sorgen, dass Korrekturen (*Patches*) unter Berücksichtigung der anlagenspezifischen Betriebskonditionen eingespielt werden (siehe IEC 62443-2-3 [7]) über den Patchmanagement-Prozess.

Weitere Verteidigungslinien sind in der Verantwortung des Systemintegrators und werden von den Dokumenten IEC 62443-3-2 [10] und 3-3 [11] adressiert. Im Vordergrund steht die Auslegung von Securitymaßnahmen für die Automatisierungslösung. Beispiele sind Segmentierung des Kommunikationsnetzwerks in Firewall-geschützten Zellen oder Zugriffsschutz mit Passwörtern. Zur Unterstützung der vom Betreiber festgelegten Nutzerrollen, sollte die Automatisierungslösung so konfiguriert werden, dass ein zugelassener Nutzer nur solche Aktionen durchführen kann, die für seine Aufgabe notwendig sind (*least privilege*). Solche Maßnahmen werden in der Regel bei der Auslegung der Automatisierungslösung durch den Systemintegrator umgesetzt. 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 z. B. das gezielte Deaktivieren aller temporären Accounts, der Schutz der System- und Default-Accounts durch strenge Passwörter oder die systematische Aktualisierung aller Daten der Anti-Malware Maßnahmen. IEC 62443-2-4 [8] beinhaltet jeweilige Anforderungen zu diesen Aktivitäten.

Die inneren Verteidigungslinien werden durch Security-Fähigkeiten der Geräte und Komponenten der Automatisierungslösung bzw. der Maschine realisiert. Sie liegen in der Verantwortung der Produkthersteller und werden durch die Dokumente IEC 62443-3-3 [11] und -4-2 [13] adressiert. 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, (*password guessing*), werden durch Verzögerungen zwischen nacheinander folgenden Anmeldeversuchen abgewehrt. Ein stringenter Entwicklungsprozess nach den Anforderungen der IEC 62443-4-1 [12] unterstützt die Vermeidung möglicher Angriffsmöglichkeiten.

Zusammenfassend, alle Protagonisten müssen zur Realisierung einer effizienten tiefgestaffelten Verteidigungsstrategie beitragen:

- Die Produkthersteller müssen Komponenten mit adäquaten Securityfunktionen entwickeln, um die Auslegung der Securitymaßnahmen der Automatisierungslösung zu unterstützen. Der Entwicklungsprozess muss möglichst die Entstehung von Angriffsmöglichkeiten während der Entwicklungstätigkeiten vermeiden.
- Der Systemintegrator muss die Fähigkeiten der Komponenten und System nutzen, um möglichst sichere Automatisierungslösungen auszulegen. Durch Verfolgung von strikten Prozessen sollen die Entstehung weiteren Angriffsmöglichkeiten in den Automatisierungslösungen möglichst vermieden werden.
- Der Betreiber muss ein Security-Programm aufstellen, mit dem Zweck der Reduzierung der Cyberrisiken des IACS während des Betriebs. Ein wesentlicher Bestandteil dabei ist eine kontinuierliche Analyse der Cyberrisiken und die Erstellung eines Plans zur Aufrechterhaltung des Betriebs.

Folgende Beispiele verdeutlichen Angriffsmöglichkeiten, die von den jeweiligen Protagonisten im Bereich der Nutzerverwaltung und Zugriffssteuerung (*User Management and Access Control, UMAC*) generiert werden können. 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 Angriffsmöglichkeit ist die Möglichkeit, Privilegien zu erhöhen und sich z. B. durch Überwinden der Nutzerverwaltung als Administrator anzumelden. Damit stehen dem Angreifer alle Mittel zum Missbrauch zur Verfügung. Die Produkthersteller können solche Angriffsmöglichkeiten durch klare Regeln für die Programmerstellung im Entwicklungsprozess vermeiden.

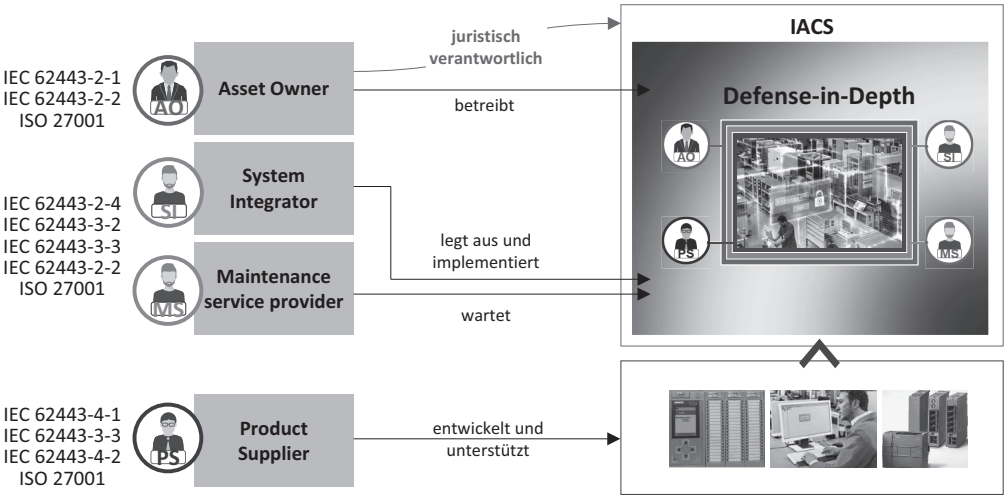


**Bild 5.1** Tiefgestaffelte Verteidigung (Defense-in-Depth)

In der Verantwortung des Integrators liegt 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 der Entwickler nicht aufwendig bei jedem Einloggen ein langes, komplexes Passwort eingeben müssen. Eine häufig anzutreffende Angriffsmöglichkeit 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 Angriffsmöglichkeiten leicht vermieden werden.

Schließlich muss der Betreiber die Namen der Personen, die den definierten Nutzerrollen zugewiesen sind, während der Betriebsphase pflegen. Da diese oft viele Jahre dauert, ist die Verantwortung des Betreibers besonders groß. Wenn beispielsweise 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 Richtlinien und Prozesse für den Betrieb und die Wartung gefragt.

Aus dem genannten Beispiel wird ersichtlich, dass jeder Protagonist seinen Teil der Securitymaßnahmen umsetzen muss, um einen gewissen Schutz zu erreichen. Eine Schwachstelle reicht aus, um die gesamte Kette zu schwächen und die Anlage anfällig zu machen.

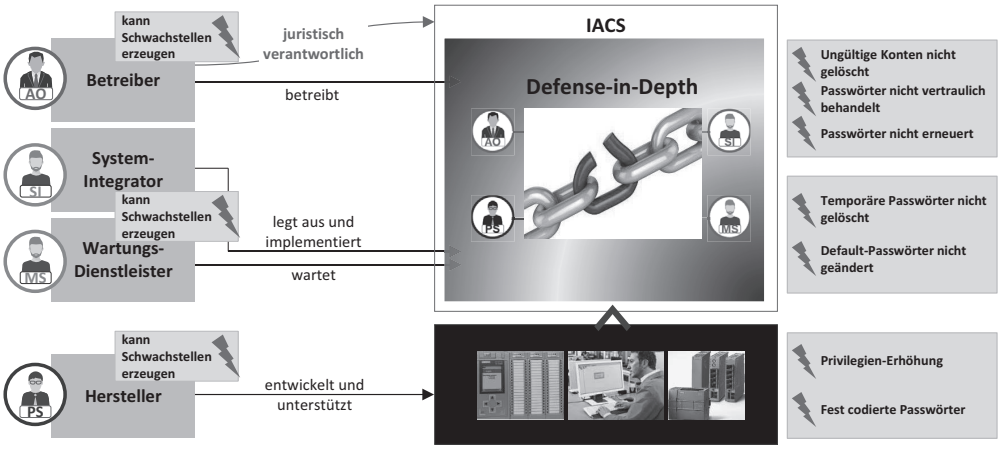


**Bild 5.2** Jeder Protagonist kann Angriffsmöglichkeiten erzeugen; das schwächste Glied definiert die Stärke der Kette.

## 5.2 Die Norm IEC 62443 in Produkt- und IACS-Lebenszyklen

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 Produktlebenszyklen

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

Um möglichst die Erzeugung von Angriffsmöglichkeiten während der Entstehung des Produkts zu vermeiden, sollte der Produkthersteller einen stringenten Entwicklungsprozess einhalten, der in allen Phasen die Security als nichtfunktionale Anforderungen integriert. In der Norm IEC 62443 wurde dies IEC 62443-4-1 [12] behandelt. Das Dokument deckt den gesamten Entwicklungsprozess ab, von der Spezifikation bis zur Testphase. Darüber hinaus werden Anforderungen an der Behandlung von eventuellen Angriffsmöglichkeiten spezifiziert, die während der Vermarktung auftreten könnten.

Die Anforderungen an Securityfunktionen von Produkten befinden sich in den Dokumenten IEC 62443-3-3 [11] und IEC 62443-4-2 [13]. Der Produkthersteller sollte in seinen Produkten die Securityfunktionen integrieren, die zur Unterstützung der allgemeinen Anforderungen des Zielmarkts benötigt werden. Die Securityfunktionen werden vom Systemintegrator in der Automatisierungslösung eingesetzt und entsprechend den Projektanforderungen konfiguriert. Ggf. müssen zusätzliche Securitymaßnahmen und Produkte hinzugefügt werden, um den gewünschten Schutz-Level zu erreichen. Der Teil IEC 62443-3-3 spezifiziert die Anforderungen an ein Leit-