# OT-Security
# Von der Norm ins Leitsystem

Sarah Fluchs · Heiko Rudolph

admeritia GmbH
{sarah.fluchs | heiko.rudolph}@admeritia.de

## Zusammenfassung

Wenn es um Security für Prozessleit- und Automatisierungssysteme geht – im Folgenden auch mit Operational Technology Security oder OT-Security abgekürzt – stellt die internationale Normenreihe IEC 62443 klare Anforderungen. Das Interesse an der Implementierung der Norm in der Praxis steigt, stellt Anwender jedoch vor einige Fragen. Dieses Paper greift Fragen auf, die erfahrungsgemäß bei der Umsetzung der IEC 62443 auftreten und skizziert einen Weg, wie OT-Security nach den Vorgaben der Norm machbar wird. Dabei werden auch besondere Anforderungen für Safety-Systeme berücksichtigt. „Machbar“ soll in diesem Zusammenhang vor allem bedeuten: Pragmatisch am Alltag der PLT-Ingenieure, SPS-Programmierer, Leitsystemadministratoren und Leitstandsfahrer ausgerichtet, für die eben nicht OT-Security, sondern der reibungslose Betrieb ihrer Anlagen im Vordergrund steht. Dazu wird das in der Norm geforderte Managementsystem als Prozess statt als Papierstapel interpretiert. Für seine Kernprozesse werden sinnvolle Risikomanagementmethoden und dafür notwendige Kompetenzen identifiziert und ein Weg skizziert, wie Risikomanagement aufgabenteilig in das bestehende Betriebsregime integriert werden kann. Der Fokus liegt dabei stets auf einer technisch wirksamen Umsetzung der IEC 62443. Dabei hilft die Modellierung in vierschichtigen Architektur-Blueprints, um Normanforderungen in konkrete Umsetzungspläne zu übersetzen und die zentrale Frage zu beantworten, die Automatisierer beim Blick in die Norm umtreibt: „Und was heißt das jetzt für mein Leitsystem?“

# 1 Rahmen: Managementsystem

Die IEC 62443-2-1:2010 fordert den Aufbau eines Managementsystems für OT-Security – der Standard selbst nennt dies ein IACS-SMS oder „Industrial Automation and Control System Security Management System“ [IEC10a] [Kobe17]. Wie auch für die internationalen Normen ISO/IEC 27001:2013 für Informationssicherheitsmanagement und ISO 9001:2015 für Qualitätsmanagement basiert das Managementsystem zu diesem Zweck auf einem PDCA-Zyklus nach Deming [Demi94], wobei PDCA für Plan, Do, Check und Act steht (siehe Abbildung 1) [Kerst13]. Auch wenn es paradox klingt, weil zusätzliche Strukturen aufgebaut werden: Ein Managementsystem reduziert Komplexität. Es bietet einen Rahmen, um OT-Security-Ziele zu identifizieren und gezielt und nachhaltig zu erreichen. Gezielt, weil genau die Maßnahmen identifiziert werden, die der Zielerreichung am meisten dienen; nachhaltig, weil die Zielerreichung kontinuierlich überprüft und nachgesteuert wird.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 276-286.

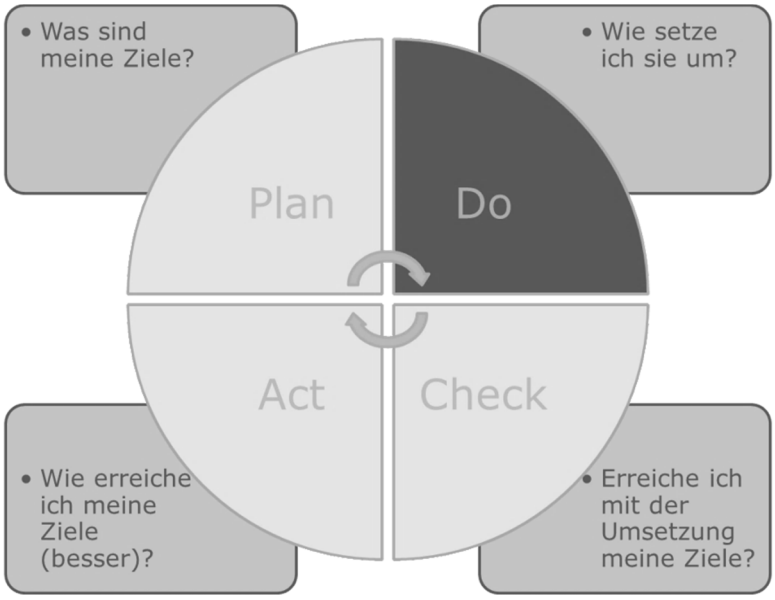


**Abb. 1:** PDCA-Zyklus

Die Alternative – und auf den ersten Blick einfachere Lösung – ist ein reines „Do“: Umsetzung eines (standardisierten) Katalogs von Security-Anforderungen, wie z. B. der Annex der ISO/IEC 27001:2013 oder passende Teile der IEC 62443, z.B. IEC 62443-2-1:2018 [IEC18a] oder IEC 62443-3:2013 [IEC13] (für weitere Beispiele siehe auch Abschnitt 5.1). Dies hat zwei Nachteile:

1. Der Katalog ist nicht an das individuelle System und die realen Gefährdungen des Systems angepasst.
2. Der Katalog kann nicht auf veränderte Gegebenheiten der Umgebung (technische Neuigkeiten, entdeckte Schwachstellen) reagieren.

Die Konsequenz dieser Nachteile sind Anforderungen, die sehr wahrscheinlich entweder zu umfangreich für das betrachtete System oder für die vorgegebenen Ziele nicht ausreichend sind. Ein Managementsystem wird keine Auskunft darüber geben, welche Firewall sinnvollerweise anzuschaffen ist. Aber es gibt dem Anwender alle Werkzeuge an die Hand, dies selbst herauszufinden – und auch zu merken, wann die bisherige Firewall nicht mehr ausreicht. Es bettet das „Do“ (Umsetzen) in einen Rahmen aus „Plan“ (Nachdenken), „Check“ (Erfolgskontrolle) und „Act“ (Verbesserung), um die in „Do“ identifizierten Anforderungen an das individuelle System und die veränderliche Umgebung anzupassen.

# 2 Dokumentenstruktur: Wo fange ich bloß an?

Gerade wenn technisch wirksame Security-Lösungen das Ziel sind, ist der erste Schritt zur Umsetzung der IEC 62443-2-1:2010 frustrierend. Die Liste der Anforderungen ist lang: Änderungsmanagement, Risikomanagement, Lieferantenmanagement, Zutrittskontrolle, Organisationsstruktur: Anwender haben oft den Eindruck, einen zusammenhanglosen Papierstapel zu produzieren. Das Bild wird klarer, sobald der Papierstapel prozessorientiert nach seinem Zweck hinsichtlich der PDCA-Phasen strukturiert wird (siehe Abbildung 2).

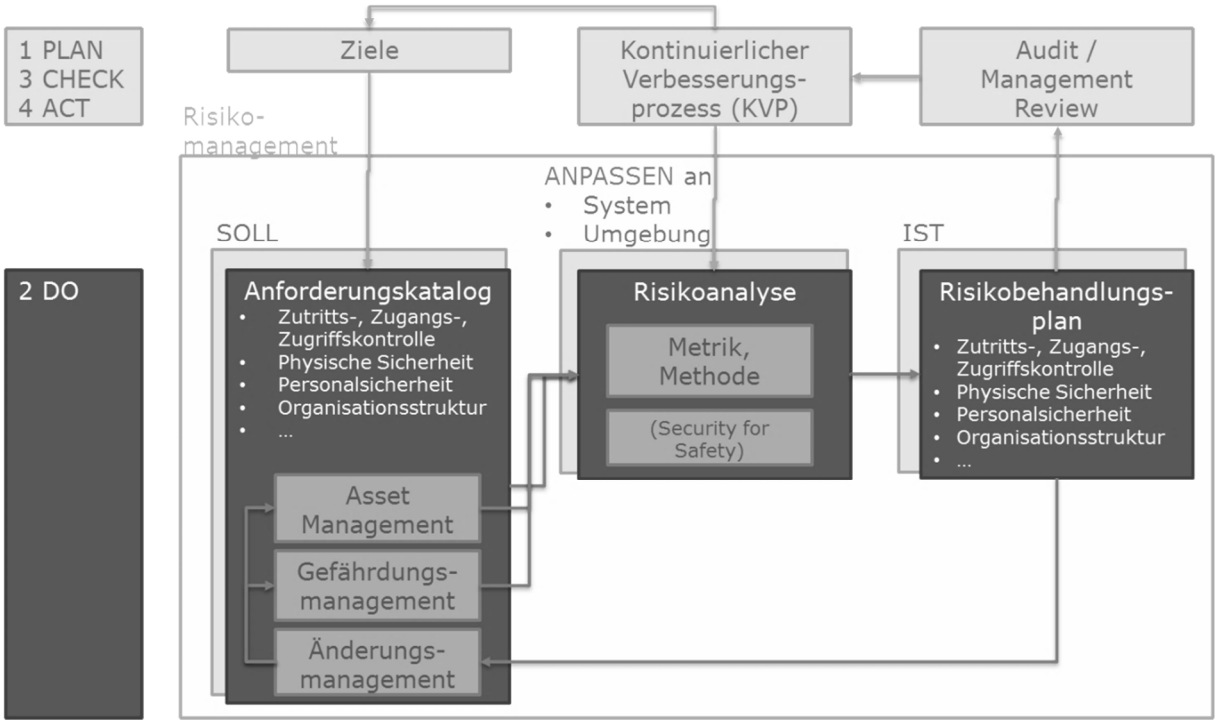


**Abb. 2:** Dokumentenstruktur Security-Managementsystems nach PDCA-Zyklus aus Prozesssicht

Für den Plan-Check-Act-Rahmen des Managementsystems (heller Hintergrund) sind die Definition von Zielen etwa in einer Leitlinie, die Anpassung dieser Ziele an das individuelle System und die veränderliche Umgebung sowie das Überprüfen des Ist-Zustands wesentlich. Für die Do-Phase (dunkler Hintergrund) muss dieser Rahmen mit Inhalten gefüllt werden: Die Ziele werden in einen Anforderungskatalog übersetzt und ein Risikobehandlungsplan, also ein angepasster Anforderungskatalog für ein konkretes System, erstellt. Das Bindeglied zwischen Anforderungskatalog und Risikobehandlungsplan ist die Risikoanalyse: Sie ist das Werkzeug für die individuelle und laufende Anpassung von Anforderungen an das betreffende System und seine Umgebung. Somit können der Anforderungskatalog mitsamt Asset-, Gefährdungs- und Änderungsmanagement sowie der Risikobehandlungsplan als Ein- beziehungsweise Ausgänge für die Risikoanalyse verstanden werden. Gemeinsam bilden sie das kontinuierliche Risikomanagement. Mit dieser prozessualen Struktur im Hinterkopf ist der Startpunkt für den Aufbau eines OT-Security-Managementsystems klar bestimmt: Das Risikomanagement, oder genauer: Die Risikoanalyse. Alle weiteren Elemente dienen als Eingänge oder Ausgänge der Risikoanalyse oder stellen den Plan-Check-Act-Rahmen.

# 3 Risikoanalyse: Nur der Blick in die Glaskugel?

Risikomanagement wird häufig als aufwendiger Prozess mit fragwürdigem Output wahrgenommen. Gerade die Denkweise der klassischen Risikoanalyse mit ihrer Einschätzung von Eintrittswahrscheinlichkeiten und Auswirkungen von Bedrohungsszenarien mittels einer Risikomatrix ist für PLT-Ingenieure ungewohnt – vor allem die nicht messbare Eintrittswahrscheinlichkeit erscheint Ingenieuren oft in etwa so hilfreich wie ein Blick in die Glaskugel.

## 1.1 Teilschritte und Ziele

Dabei besteht ein Risikomanagement nach IEC 62443-3-2 [IEC18b] mitnichten nur aus der „Glaskugel“ Risikomatrix, sondern aus mehreren Teilschritten mit unterschiedlichen Zielen und Methoden (siehe Abbildung 3).

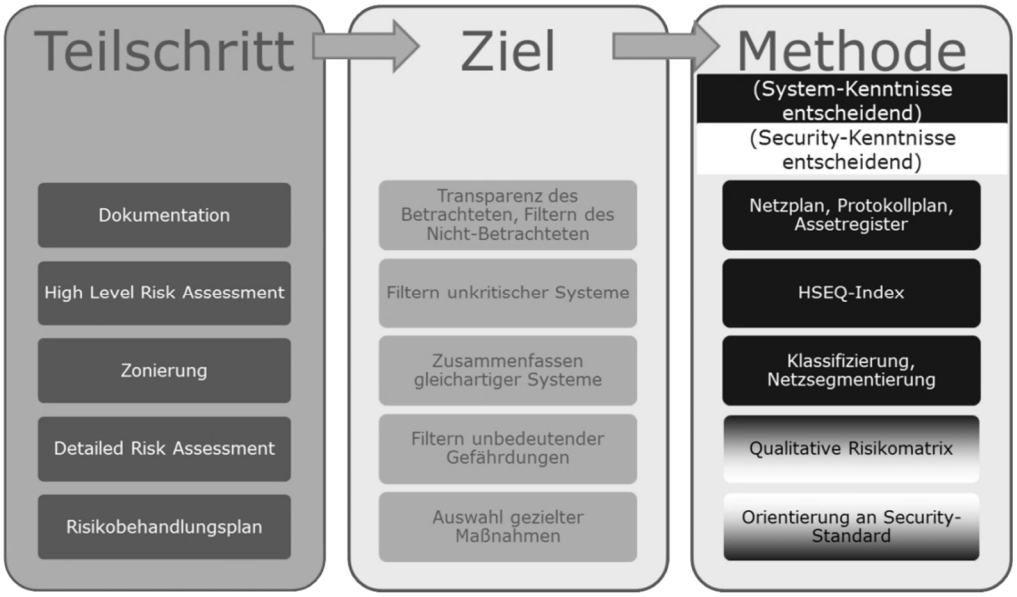


**Abb. 3:** Teilschritte, Ziele, Methoden der Risikoanalyse und notwendige Kenntnisse für Methoden

Als erster Schritt erfolgt die Dokumentation von System und Umgebung. Im nächsten Schritt dient ein High Level Risk Assessment dem Filtern von Systemen nach Schutzbedarf und hilft, im nächsten Schritt gleichartige Systeme zu Zonen zusammenzufassen. Detailed Risk Assessment und Risikobehandlungsplan schließlich dienen der Identifikation bedeutender (und Filterung unbedeutender!) Gefährdungen und Auswahl gezielter Maßnahmen. Mit dem Risikomanagement ist es wie mit dem Managementsystem: Sein Zweck ist kein Aufbau zusätzlicher Komplexität, sondern Komplexitätsreduktion. Systeme, Schutzbedarf und Systemumgebung werden transparent gemacht und durch Filtern nicht relevanter und Zusammenfassen ähnlicher Systeme strukturiert, um die individuell wirksamsten OT-Security-Anforderungen zu identifizieren.

## 1.2 Methoden

Für eine pragmatische Umsetzung der Teilschritte sollte sich die Methodenauswahl strikt an den folgenden Fragen orientieren:

1. Was muss die Methode liefern, um das identifizierte Ziel zu erreichen (und nur dieses!)?
2. Sind bereits Prozesse oder Datengrundlagen vorhanden, die für die Methode verwendet werden können?

In Abbildung 3 werden beispielhaft geeignete Methoden für die einzelnen Teilschritte aufgeführt:

Die Systemdokumentation als Fundament des Risikomanagements erfolgt durch sinnvolle tabellarische und visuelle Aufbereitung von Systemen, Komponenten, Kommunikationsverbindungen und verwendeten Kommunikationsprotokollen – in Assetregistern, Netzplänen und Protokollplänen.

Für das High Level Risk Assessment ist eine valide Methode die Identifikation kritischer Systeme anhand des Health, Safety, Environment and Quality (HSEQ)-Indizes. Zonierung, also das Zusammenfassen von Systemen ähnlichen Schutzbedarfs kann aus dem High Level Risk Assessment resultieren und gleichzeitig Grundlage für den Aufbau einer sinnvoll segmentierten Netzarchitektur sein [KnLa15]. Erst für das Detailed Risk Assessment wird dann die „Glaskugel“ Risikomatrix herangezogen – allerdings in der Regel mit einer qualitativen, nicht quantitativen Metrik. Für die Erstellung des Risikobehandlungsplans hilft die Orientierung an bestehenden Standards, etwa der IEC 62443-3-3 [IEC13].

# 4 Aufgabenverteilung: Wer soll das alles machen?!

Auch wenn das Risikomanagement der Komplexitätsreduktion und damit letztlich der zeiteffizienten Umsetzung von OT-Security dient: OT-Security, auch mit sinnvoll gewählten Risikomanagementmethoden, bedeutet immer einen Mehraufwand. Ingenieure und Anlagenfahrer sind jedoch in der Regel mit ihrem Tagesgeschäft – dem Anlagenbetrieb – ausreichend ausgelastet. Risikomanagement wird nur dann dauerhaft funktionieren, wenn es sich ins Tagesgeschäft eingliedert. Dabei helfen zwei Ansätze: Kompetenzbündelung und Standardisierung.

## 4.1 Kompetenzbündelung

In Abbildung 3 ist für jeden Teilschritt des Risikomanagements eine weitere Information enthalten: Welche Kenntnisse sind für die Durchführung eines Teilschritts relevant? Sind es Kenntnisse über Aufbau, Funktion und Betrieb von Prozessleit- und Automatisierungssystemen (Systemkenntnisse, schwarz) oder Kenntnisse über Gefährdungen, also Bedrohungsszenarien und Schwachstellen, dieser Systeme und wirksame Gegenmaßnahmen (Security-Kenntnisse, weiß)?

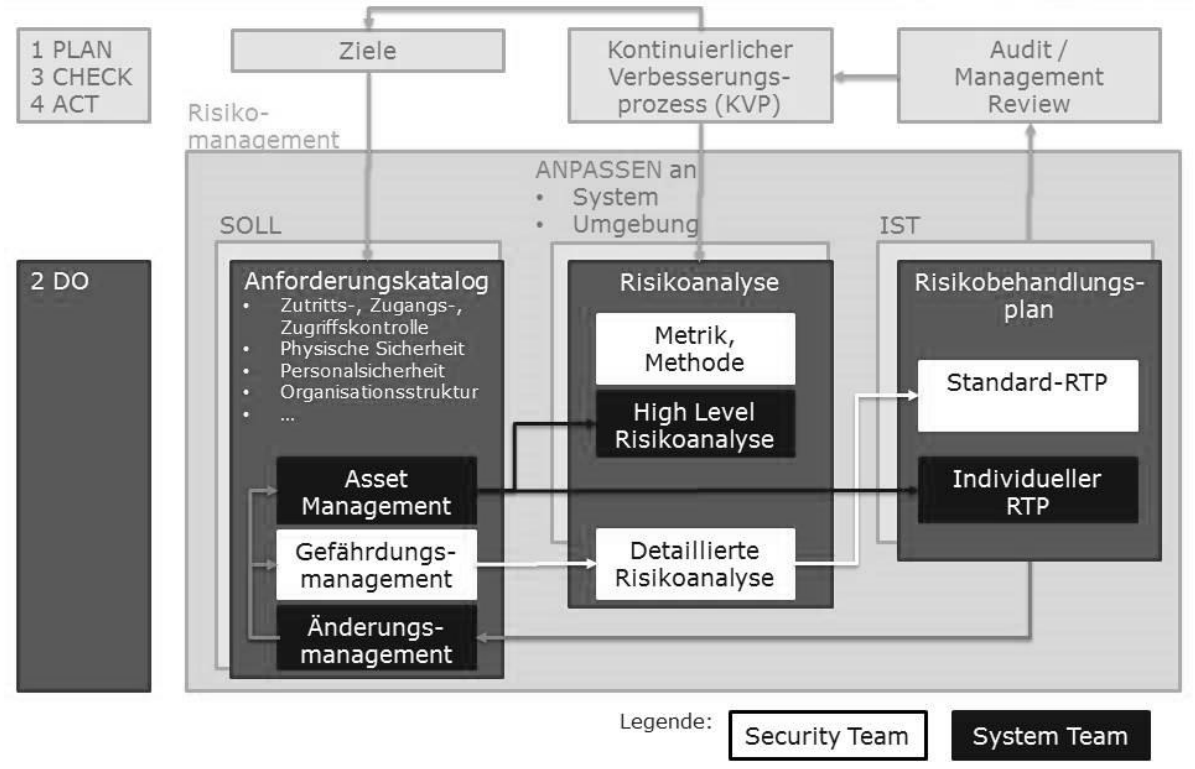


**Abb. 4:** Integration der Risikoanalyse in den betrieblichen Alltag durch Kompetenzbündelung

Für alle Schritte bis zum Detailed Risk Assessment ist vor allem eine profunde Systemkenntnis entscheidend. Erst für das Detailed Risk Assessment und die Identifikation und Priorisierung passender Anforderungen müssen Systemkenntnisse durch Security-Kenntnisse ergänzt werden. Für die operative Umsetzung der konkreten Maßnahmen zur Anforderungserfüllung sind wieder primär Systemkenntnisse relevant. Gerade bei größeren Unternehmen, die viele von unterschiedlichen Betreibern betreute Prozessleit- und Automatisierungssysteme betreiben, ist eine Bündelung der Security-Kompetenz in einem „Security-Team“ sinnvoll. Dieses kann alle Teilschritte des Risikomanagements übernehmen bzw. unterstützen, die Security-Kenntnisse erfordern (weiß markiert in Abbildung 4). Dies umfasst in jedem Fall die Schritte, die eine klassische Risikoanalyse („Glaskugel“) erfordert: Das Gefährdungsmanagement, also die kontinuierliche Beobachtung und Einschätzung neuer Bedrohungen und Schwachstellen und die detaillierte Risikoanalyse sowie die Erarbeitung sinnvoller Methoden und Metriken für die Risikoanalysen. Die grobe Risikoanalyse, also die Kritikalitätseinschätzung der Systeme, sowie das Asset- und Änderungsmanagement inklusive Erstellung und Pflege der Systemdokumentation als Eingang für die Risikoanalyse (schwarz markiert in Abbildung 4) kann das „System-Team“, zusammengesetzt beispielsweise aus PLT-Ingenieuren, Leitsystemadministratoren und Leitstandsfahrern, mit seinen Erfahrungen aus dem Tagesgeschäft gut durchführen – oft tut es dies ohnehin schon aus betrieblichen Gründen.

## 4.2 Standardisierung

Die Risikobehandlung erfordert eine Zusammenarbeit der beiden Kompetenzbereiche „System“ und „Security“. Sie umfasst:

- die Erstellung des generischen Anforderungskatalogs und
- die Erstellung der an individuelle Systeme angepassten Risikobehandlungspläne (Risk Treatment Plans, RTP), indem der Anforderungskatalog auf Basis der Ergebnisse des Detailed Risk Assessments angepasst wird.

Das Security Team kann den Anforderungskatalog auf Basis relevanter Standards ebenso ohne Zutun der Ingenieure pflegen wie das systemübergreifende Gefährdungsmanagement. Zusätzlich hat sich die Einführung von Standard-Umsetzungsplänen bewährt, die das Security-Team mittels detaillierter Risikoanalysen für bestimmte Systemtypen erstellen kann. Systemtypen können hersteller-, modell- oder einsatzzweckbasiert unterschieden werden. Die Verwendung von Standard-Umsetzungsplänen hat – wie zuvor PDCA-Zyklus und Risikomanagement – den Zweck der Komplexitätsreduktion. Gleichartige Systeme werden zusammengefasst, die Pläne sind wiederverwendbar und skalierbar. Zudem ermöglichen sie eine Aufgabenteilung zwischen den Kompetenzbereichen durch Trennen von Problemstellungen: Das System-Team schätzt die Kritikalität seiner Systeme ein und liefert Informationen zu Aufbau und Funktion, muss aber keine Schwachstellen und Bedrohungen sondieren und einschätzen und keine Anforderungen auswählen – der „Glaskugel“-Teil bleibt komplett beim Security-Team. Das System-Team kann seine Systemkenntnisse abschließend wieder einbringen, indem es die Standard-Umsetzungspläne so individualisiert und konkretisiert, dass sie für seine realen Systeme operativ umsetzbar und machbar sind.

# 5 Risikobehandlung: Auswirkungen aufs Leitsystem

Die Aufteilung der Risikobehandlung durch die Erstellung von Anforderungskatalog und Standard-Umsetzungsplänen durch das Security-Team und die Erstellung individueller Umsetzungspläne durch das System-Team misst Struktur und Formulierung des Anforderungskatalogs eine hohe Bedeutung bei: Er stellt die Schnittstelle zwischen Security- und System-Team dar. Aufgrund dieser Schnittstellenfunktion ist es elementar, für den Anforderungskatalog eine Kategorisierung, Detailtiefe und Formulierungsgrundlage zu finden, mit der sowohl das Security-Team als auch die Systembetreiber und -administratoren möglichst intuitiv arbeiten können.

## 5.1 Gemeinsame Sprache finden

Auch bei Implementierung eines IACS-SMS nach IEC 62443-2-1:2018 [IEC18a] [IEC10a] müssen für die Anforderungen nicht zwingend Wortwahl und Kategorisierung der IEC-Normen verwendet werden. Den Vorrang bei der Auswahl sollte die für das eigene Unternehmen verständliche inhaltliche Formulierung und Detailtiefe der technischen und organisatorischen Anforderungen haben. Als mögliche Basis können neben IEC 62443-2-1] und IEC 62443-3-3 [IEC13] auch die Anforderungskataloge aus IT-Grundschutz [BSI17], NIST Special Publication 800-53 [NIST13] oder ISO 27001 [ISO17] dienen. Die intuitiv verständliche Strukturierung des Anforderungskatalogs ist ein unterschätztes Kriterium. Es ist dabei durchaus denkbar, nach der Auswahl eines inhaltlich geeigneten Anforderungskatalogs die inhaltlichen Anforderungen in eine passendere Struktur zu überführen – sozusagen eine individuelle „Maske“ über die bestehende Struktur legen. Das NIST Cybersecurity Framework [NIST18] bietet eine Basis, mit der gerade Systembetreiber und -administratoren oft gut zurechtkommen. Auch die IEC 62443 wird gerade um einen Teil ergänzt, der eine einheitliche Strukturierung – sogenannte Security Control Classes – der Anforderungen aus unterschiedlichen Teilen des Standards anstrebt [IEC18c]. Dabei ist explizit auch die Möglichkeit einer IEC-fremden oder komplett individuellen Strukturierung benannt.

## 5.2 Blueprint-Schichten

Auch ein gut formulierter und strukturierter Anforderungskatalog bleibt: Eine Liste von Anforderungen. Um die technische Wirksamkeit des Security-Managementsystems sicherzustellen, empfiehlt sich deswegen die direkte Übersetzung der Erkenntnisse aus dem Risikomanagementprozess in für das Leitsystem verwertbare Ergebnisse. Dies kann die Modellierung von Blueprints in vier Schichten leisten, die parallel zum Risikomanagementprozess erarbeitet werden (siehe Abbildung 5).

Die erste Schicht, der Funktions-Blueprint, beinhaltet alle funktionalen Anforderungen an das betrachtete System und deren Visualisierung in einer Netzarchitektur. Er definiert, welche Funktionalität je Systemkomponente zwingend erforderlich ist und dient somit der strukturierten Erfassung von Schutzzielen. Die nächste Schicht, der Risiko-Blueprint stellt die Ergebnisse der High Level und Detailed Risk Assessments in verdichteter Form dar, indem er den Funktions-Blueprint um die identifizierten Risiken und Angriffsvektoren ergänzt. Die dritte Schicht, der Security-Blueprint, leitet aus den funktionalen Anforderungen, Schutzzielen und identifizierten Risiken Security-Anforderungen ab. Dabei stützt er sich auf die Standards, die für die Erarbeitung des Risikobehandlungsplans herangezogen wurden. Der Umsetzungs-Blueprint

bildet den Abschluss innerhalb der Blueprint-Schichten. Er beinhaltet basierend auf den Anforderungen des Security-Blueprints konkrete Pläne, wie die Anforderungen erfüllt werden können. Dies können spezielle Produkttypen oder sogar spezifische Produkte definierter Hersteller sein. Um den Überblick bei einer großen Anzahl von Maßnahmen nicht zu verlieren, empfiehlt sich auch bei der Maßnahmenumsetzung eine Priorisierung der Maßnahmen, die den bewährten Strategien zur Komplexitätsreduktion dienen:

1. Transparenz: Maßnahmen, die Systemverständnis und -dokumentation fördern: Änderungsmanagement, Logging, Asset Management, Inventarisierung
2. Struktur: Maßnahmen, die die grundlegende Architektur verbessern: Klassifizierung, Zonierung, Netzsegmentierung, Einschränkung der Kommunikation
3. Standardisierung: Maßnahmen, die Security in den Alltag integrieren helfen: Standardkonfigurationen für Systeme und Kommunikationsprotokolle, Nutzungs- und Administrationsrichtlinien

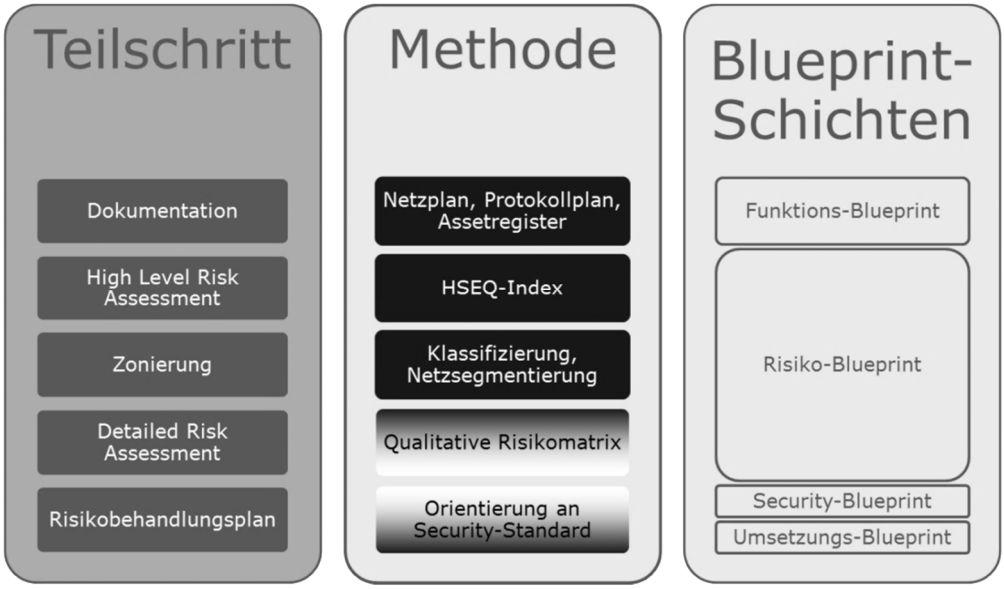


**Abb. 5:** Übersetzung der Ergebnisse der Norm ins Leitsystem mittels vierschichtiger Blueprints

Die Blueprint-Schichten – insbesondere mit ihrer letzten Schicht, den Umsetzungs-Blueprints – verdeutlichen, wie die konsequente und strukturierte Ausführung und Dokumentation der Prozesse des Managementsystems letztendlich den Anwender befähigt, sich die eingangs formulierte Frage selbst zu beantworten: „Und was heißt das jetzt für mein Leitsystem? Sagt mir doch einfach, welche Firewall ich kaufen soll."

# 6 Safety-Risikoanalyse: Keine Parallelstrukturen!

Wenn Safety-Systeme (Safety Instrumented Systems, SIS) vorhanden sind, ist zumindest eine Art der Risikoanalyse auch dem „System-Team" in der Regel hinlänglich bekannt: Die Safety-Risikoanalyse. Der Wunsch, keine Parallelstrukturen aufbauen zu wollen, liegt nahe: Die Frage nach der pragmatischen Vereinbarkeit der Safety-Risikoanalyse, etwa nach IEC 61508 [IEC10b] oder IEC 61511 [IEC16], mit der Security-Risikoanalyse nach IEC 62443 [IEC18b], wird laut. Eine Security-Risikoanalyse hat eine grundlegend andere Zielsetzung als eine Safety-Risikoanalyse: Safety will ein Safety-System konzeptionieren, das die Umgebung vor der An-

lage schützt. Security hingegen will Anforderungen definieren, um das Safety-System vor seiner Umgebung schützen. Folglich finden beide Risikoanalysen zu unterschiedlichen Entwicklungszeitpunkten statt, brauchen unterschiedliche Eingangsgrößen sowie unterschiedliche Einschätzungsmethoden, und haben unterschiedliche Ergebnisse, die sich durchaus auch widersprechen können. Böswillige Angriffe sind statistisch viel schwieriger fassbar als die gefährlichen Vorfälle, die im Rahmen der Safety-Risikoanalyse betrachtet werden. Die IEC 61508 bzw. IEC 61511 macht es sich an dieser Stelle einfach: Böswillige Gefährdungen (Security Threat Events) sollen mit berücksichtigt werden – dazu ziehe man die IEC 62443 zu Rate. Ein Blick in die IEC 62443 offenbart: Die Norm deckt auch die Security für SIS ab – dazu wird jedoch auf die IEC 61508 verwiesen. Das Ergebnis ist ein klassisches Henne-Ei-Problem: Was muss zuerst da sein: die Safety-Henne oder das Security-Ei? Der Technical Report IEC TR 63069 [IEC17], der sich noch im Entwurfsstadium befindet, stellt eine Methode dar, dieses Henne-Ei-Problem aufzulösen. Die grundlegende Idee besteht in der Definition eines Security-Environments – das Security-Ei, das als gegeben angenommen wird. Das hat zwei Konsequenzen: Zum einen kann die Safety-Risikoanalyse unverändert durchgeführt werden. Zum anderen wird bei der Durchführung der Security-for-Safety-Risikoanalyse zusätzliches Safety-Know-How gebraucht (siehe Abbildung 6).

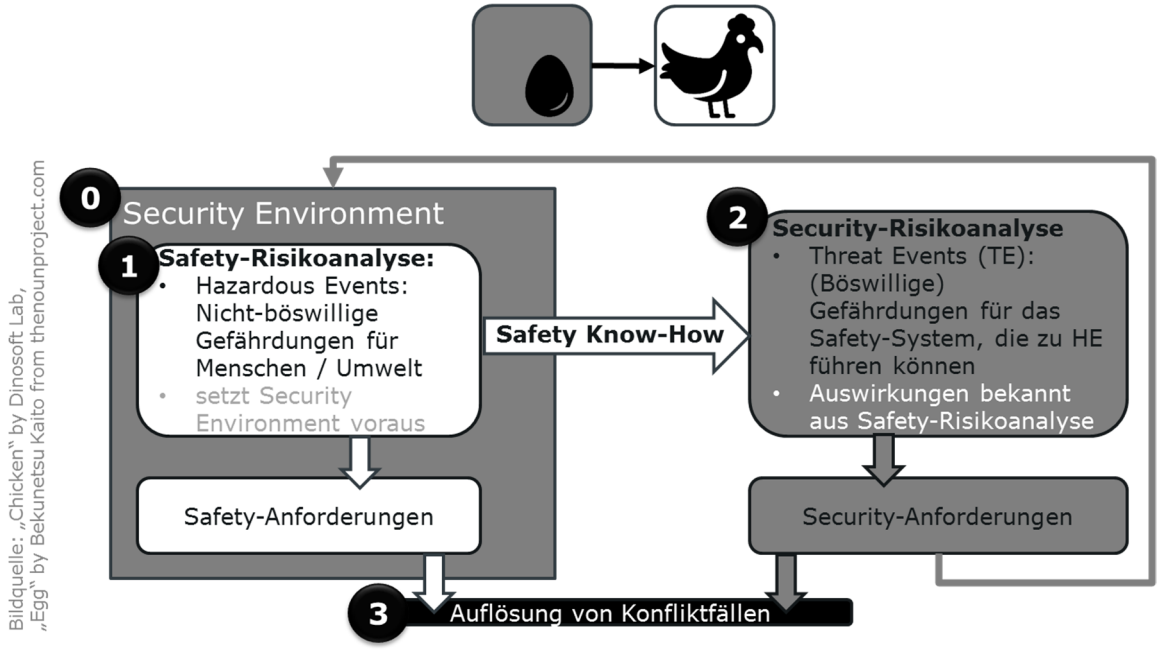


**Abb. 6:** Einbettung der Security-Risikoanalyse in den Gesamtprozess (IEC TR 63069 [IEC17])

Weil das Ergebnis der Safety-Risikoanalyse das SIS selbst ist, das die Security-Risikoanalyse wiederum schützen möchte, muss die Safety-Risikoanalyse zwingend vor der Security-Risikoanalyse stattfinden. Gleichzeitig bedeutet dies aber, dass sich das Wissen aus der Safety-Risikoanalyse für die Security-Risikoanalyse nutzen lässt, um Synergieeffekte zu erzielen. Mit der Methodik der Blueprint-Schichten gesprochen, ist der Funktions-Blueprint mitsamt Schutzzielen eines Safety-Systems durch die Beschreibung der Safety Integrity Functions (SIF) schon sehr genau beschrieben, und für den Risiko-Blueprint sind immerhin die Auswirkungen eines Ausfalls einer SIF und die gefährlichen Vorfälle, die zu diesem Ausfall führen, bereits bekannt. Ergänzt werden müssen Angriffsvektoren auf das SIS für den Risiko-Blueprint sowie die Security- und Umsetzungs-Blueprints. Hinzu kommt bei Safety-Systemen eine Besonderheit:

Es kann zu Konfliktfällen zwischen Safety- und Security-Anforderungen kommen, die vor der Finalisierung des Umsetzungs-Blueprints aufgelöst werden müssen.

# 7 Ausblick

Auch wenn die Umsetzung der IEC 62443 aufgrund ihres Umfangs und ihrer ständigen Weiterentwicklung zunächst wie ein enormer Zusatzaufwand wirkt: Letztendlich hilft sie, die Komplexität des Themas OT-Security beherrschbar zu machen. Voraussetzung für die schmale Gratwanderung zwischen sinnvoller Komplexitätsreduktion und unzulässiger Vereinfachung ist dabei, bei der Implementierung jedes Teilschritts sowohl die Ziele der Norm als auch den Alltag ihrer Anwender im Blick zu haben. Die konsequente Modellierung der IEC 62443 in Blueprint-Schichten von den funktionalen Anforderungen bis zur Umsetzung hilft, nicht bei papiernen Maßnahmen stehen zu bleiben, sondern eine technisch wirksame Umsetzung zu erreichen. Dieser Fokus kann sogar den alten Grundsatz herausfordern, nach dem ein Plus an Security immer ein Minus an Praktikabilität bedeutet: Die konsequente Ausrichtung auf bessere Transparenz, Strukturierung und Standardisierung kann Leit- und Automatisierungssysteme nicht nur sicherer machen – sondern auch robuster und besser wart- und bedienbar. Das nachhaltige Etablieren eines Managementsystems in Verbindung mit der eingeübten Modellierung in Blueprint-Schichten wappnet Betreiber von Leit- und Automatisierungssystemen zudem für die Zukunft. Für die Planung elementarer Veränderungen im Rahmen der „Industrie 4.0“, helfen diese Werkzeuge bei der Komplexitätsreduktion und Konkretisierung: So können sinnvolle Anwendungsfälle und Funktionen ausgewählt, ihre Risiken analysiert, angemessene Security-Maßnahmen identifiziert sowie deren konkrete Umsetzung geplant werden.

## Literatur

[BSI17] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium. Bundesanzeiger Verlag (2018).

[Demi94] W. Deming: The New Economics for Industry, Government, Education. MIT Press (1994).

[IEC10a] International Society of Automation (ISA) / International Electrotechnical Commission (IEC): ISA/IEC 62443-2-1:2010. Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program (2010).

[IEC10b] International Electrotechnical Commission (IEC): IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems (2010).

[IEC13] International Society of Automation (ISA) / International Electrotechnical Commission (IEC): ISA/IEC 62443-3-3:2013. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels (2013).

[IEC16] International Electrotechnical Commission (IEC): IEC 61511:2016. Functional safety – Safety instrumented systems for the process industry sector (2016).

[IEC17] International Electrotechnical Commission (IEC): IEC TR 63069:2017 (CD). Framework for functional safety and security (2017).

[IEC18a] International Society of Automation (ISA) / International Electrotechnical Commission (IEC): ISA/IEC 62443-2-1:2018 (CD). Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners (2018).

[IEC18b] International Society of Automation (ISA) / International Electrotechnical Commission (IEC): ISA/IEC 62443-3-2:2018 (CDV). Security for industrial automation and control systems - Part 3-2: Security risk assessment and system design (2018).

[IEC18c] International Society of Automation (ISA) / International Electrotechnical Commission (IEC): ISA/IEC 62443-2-2:2018 (CD): Security for industrial automation and control systems – Part 2-2: IACS protection levels (2018).

[ISO15] International Organization for Standardization (ISO): ISO 9001:2015. Quality management systems – Requirements (2015).

[ISO17] International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC): ISO/IEC 27001:2017. Information technology – Security techniques - Information security management systems – Requirements (2017).

[Kerst13] H. Kersten: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz – Der Weg zur Zertifizierung. Springer Vieweg (2013).

[KnLa15] E. Knapp, J. Langill: Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier Inc. (2015).

[Kobe17] P. Kobes: Guideline Industrial Security - IEC 62443 is easy. VDE Verlag GmbH (2017).

[NAMU17] NAMUR - Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V.: NA 163:2017 – IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen (2017).

[NIST13] National Institute of Standards and Technology (NIST): Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations (2013).

[NIST18] National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1 (2018).