atp magazin

SONDERDRUCK
*Transforming Automation*
**Ausgabe 3/2024**

**Peer-Review:** 06.11.2023

# ISO 27000 oder IEC 62443?

## Wie man beide Normreihen sinnvoll für die OT-Security kombiniert

Karl-Heinz Niemann, Hochschule Hannover; Pierre Kobes, Dr. Kobes Consulting

*Betreiber von Produktionsanlagen stehen oft vor der Frage, welche Norm für die Absicherung der Anlage gegen Cyberangriffe heranzuziehen ist. Aus dem IT-Bereich ist die Normreihe ISO 27000 bekannt. Im Produktionsbereich wird häufig die Normreihe IEC 62443 herangezogen. Dieser Beitrag gibt einen Überblick über beide Normreihen und schlägt einen Ansatz zur gemeinsamen Nutzung beider Standards vor.*

***#IEC 62442 #ISO 27001 #OT Security #Industrial Security***

ISO 27000 or IEC 62443?

How to combine both series of standards meaningful for OT security

*Operators of production plants are often faced with the question of which standard should be used to protect the plant against cyber-attacks. The ISO 27000 series of standards is known from the IT sector. In the production sector, the IEC 62443 series of standards is often used. This article provides an overview of both series of standards and proposes an approach for the joint use of both standards.*

***#IEC 62443 #ISO 27001 #OT security #industrial security***

## 1. Einführung

Planer und Betreiber von Produktionsanlagen stehen vor der Frage, welche Normen für ihre IT-Sicherheitskonzepte heranzuziehen sind. Da die Verantwortlichkeit in Bezug auf die IT-Sicherheit für die Operational Technology (OT Security) oft in anderen Händen liegt, als die für Information Technology (IT Security), gibt es häufig die Fragestellung, welche Normen zu Grunde zu legen sind.

Personen aus dem IT-Umfeld referenzieren in der Regel auf die Normreihe ISO 27000, während Personen aus dem OT-Umfeld eher die Normreihe IEC 62443 favorisieren. Dieser Beitrag beschreibt die Grundlagen und Ausrichtung der beiden Normreihen und gibt Anregungen, wie im OT-Kontext eine kombinierte Nutzung aussehen kann.

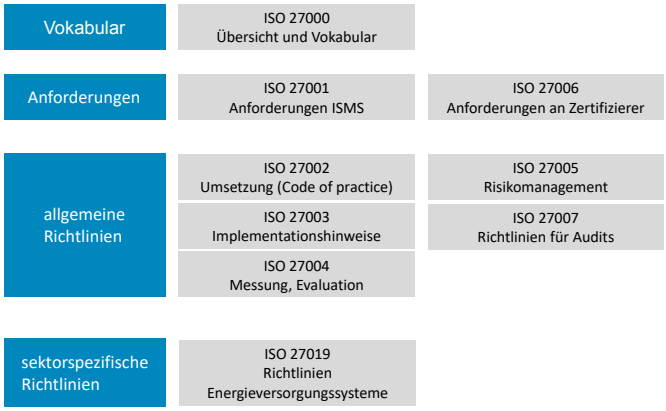


**Abbildung 1:** Übersicht über die wesentlichen Teile der Normreihe ISO 27000 (in Anlehnung an [3]).

## 2. IT-Sicherheitsnormen im Überblick

Dieser Abschnitt gibt zunächst einen Überblick über die IT-Sicherheitsnormen, die im Produktionsbereich anzuwenden sind. Dies sind im Wesentlichen die Normreihen ISO 27000 und IEC 62443. Die beiden folgenden Unterkapitel stellen die Normreihen vor. Soweit verfügbar, werden im Literaturverzeichnis jeweils die deutschen Fassungen der Normen referenziert.

### 2.1 Die Normreihe ISO 27000

Die Normreihe ISO 27000 definiert das Thema Informationssicherheitsmanagementsysteme (im Weiteren ISMS genannt). Eine Einführung und Übersicht über die einzelnen Teilnormen einschließlich einer kurzen Beschreibung finden sich in [1] oder online unter [2]. Abbildung 1 zeigt eine Übersicht über die wesentlichen Teile der Normreihe.

Die **ISO 27000** [1] erläutert zunächst die verwendeten Fachbegriffe und gibt danach einen Überblick über die Normreihe. Im Fokus steht der Aufbau eines Informationssicherheitsmanagementsystems (ISMS). Dieses ist gemäß [1] wie folgt definiert:



Dieses Dokument ist lizenziert unter der Lizenz Creative Commons Namensnennung 4.0 (CC BY 4.0):
https://creativecommons.org/licenses/by/4.0/

*„Ein Informationssicherheitsmanagementsystem (ISMS) umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die alle von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen."*

Die Norm fokussiert auf die Informationssicherheit, um Vertraulichkeit, Verfügbarkeit und Integrität von Information sicherzustellen. Dabei wird ein prozessorientierter Ansatz verfolgt, um die erforderlichen Prozesse im Unternehmen zu identifizieren und zu lenken. Die Normreihe verfolgt einen risikobasierten Ansatz, in dem Informationssicherheitsrisiken beschrieben, bewertet und behandelt werden. Die Aufrechterhaltung und Verbesserung des ISMS wird in einem kontinuierlichen Verbesserungsprozess überwacht, gesteuert und fortlaufend verbessert.
Die **ISO 27001** [4] definiert Anforderungen an ISMS. Es legt die Anforderungen an die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Aufrechterhaltung und Verbesserung von formalisierten (ISMS) im Zusammenhang mit den übergreifenden Unternehmensrisiken einer Organisation fest. Zu den Inhalten gehören u. a.:

- Kontext der Organisation
- Führung und Verpflichtung des Managements
- Sicherheitspolitik des Unternehmens
- Rollen, Verantwortlichkeiten und Befugnisse der Organisation
- Maßnahmen zum Umgang mit Risiken und Chancen
- Unterstützung, Kommunikation, Dokumentation
- Betrieb
- Bewertung der Leistung
- Verbesserungsprozess

Neben den Anforderungen an ein ISMS, beinhaltet die ISO 27001 einen Anhang, der tabellarisch Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken auflistet.
Die Norm ISO 27001 wurde im Jahr 2022 überarbeitet. In diesem Beitrag wird der Entwurf der deutschen Übersetzung [4] zitiert. Die wesentlichen Änderungen der aktualisierten Fassung bestehen in der Anpassung auf eine neue harmonisierte Struktur der Norm und Anpassungen am Informationssicherheitsmanagementsystem (ISMS), wie z. B. die verbindliche Benennung von Verantwortlichkeiten. Im Anhang wurden Anpassungen an den Stand der Technik vorgenommen. Dies betrifft z. B. Cloud-Dienste, die Sammlung und Analyse von Bedrohungsinformationen, die physische Sicherheitsüberwachung, sicheres Coding, Konfigurationsmanagement und vieles mehr. Weitere Informationen zur ISO 27001 und zu den Veränderungen durch die aktualisierte Ausgabe 2022 finden sich in [5].

Die **ISO 27002** [6] ist eine Anleitung für die Umsetzung von Informationssicherheitsmaßnahmen zur Erfüllung der im Anhang der ISO 27001 gelisteten Anforderungen. Insbesondere Abschnitt 5 bis Abschnitt 8 geben spezifische Ratschläge und Anleitung für bewährte Praktiken zur Erfüllung der Anforderungen aus der ISO 27001. Hierzu gehören beispielsweise:

- Vergabe von Zugangsrechten, Benutzerverwaltung, Zugangsverwaltung, Verwaltung von Kennwörtern.
- Datenträgerentsorgung
- Zugang zu Netzwerken und Netzwerkdiensten
- Schlüsselverwaltung
- Physischer Sicherheitsperimeter
- Sichern von Räumen und Einrichtungen
- Betriebsabläufe und Verantwortlichkeiten
- Schutz vor Schadsoftware
- Datensicherung
- Netzwerksicherheitsmanagement, Trennung von Netzwerken
- Lieferantenbeziehungen
- u.v.m.

Die obige Liste gibt keinen vollständigen Auszug aus der Norm, sondern soll lediglich als exemplarische Aufzählung dienen. Auch diese Norm wurde im Jahr 2022 aktualisiert. Die Zitation [6] bezieht sich auf den Entwurf der deutschen Fassung.
Im Kontext der Automatisierungstechnik ist weiterhin die sektorspezifische Richtlinie ISO 27019 [7] von Interesse. Diese bietet einen Leitfaden, der auf der ISO 27002 [6] basiert und auf Prozessleitsysteme angewandt wird, die von der Energieversorgungsbranche zur Steuerung und Überwachung der Produktion oder Erzeugung, Übertragung, Speicherung und Verteilung von elektrischer Energie, Gas, Öl und Wärme sowie zur Steuerung der zugehörigen unterstützenden Prozesse verwendet werden. Eine weiterführende Beschreibung der weiteren Normteile findet sich in [8] und unter [2].

**2.2 Die Normreihe IEC 62443**

Basierend auf den Modellen und Anforderungen der Normreihe ISO 27000 werden in der Normreihe IEC 62443 die speziellen Anforderungen der IT-Sicherheit im Produktionsbereich berücksichtigt. Abbildung 2 zeigt die Struktur der Normreihe. Die grau hinterlegten Teile sind noch nicht erschienen und werden daher in diesem Beitrag nicht näher beschrieben. Weiterhin ist eine Erweiterung um eine Reihe 6 geplant, auf die hier aber nicht näher eingegangen wird.

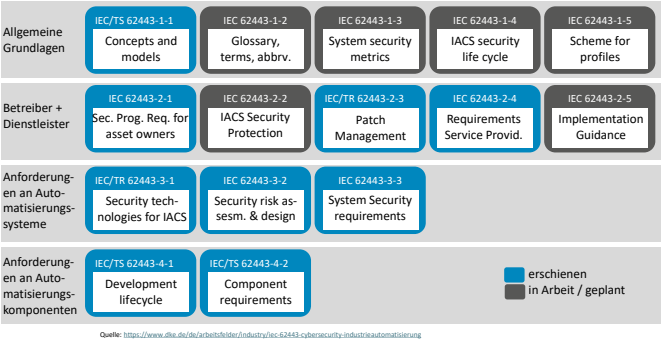


**Abbildung 2:** Struktur der Normreihe IEC 62443 [9].

Der Abschnitt **„Allgemeine Grundlagen“** der IEC 62443-1-1 [10] definiert die Terminologie, Konzepte und Modelle für die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS). Diese Definitionen bilden die Grundlage für die übrigen Normen der Reihe IEC 62443.
Im Teil für die **„Betreiber und Dienstleister“** definiert die IEC 62443-2-1 [11] die Anforderungen an das Security Programm des Betreibers, z. B.:

- Risiko-Management
- Netzwerksegmentierung
- Schutz der Daten und der Komponenten
- Pläne zur Business Continuity
- Zugangs- und Zugriffskontrolle
- Datensicherung
- usw.

Das Aktualisieren der Software von Automatisierungssystemen, das Patchen, ist von besonderer Bedeutung, weil es bei unsachgemäßem Vorgehen zu Betriebsstörungen kommen kann. Daher widmet die Normreihe dem Patch-Management einen eigenen Teil. Es handelt sich hierbei um die IEC TR 62443-2-3 [12].
Der Teil IEC 62443-2-4 [13] befasst sich mit dem Einsatz von Dienstleistern für Inbetriebnahme und Service aus Sicht der IT-Sicherheit. In der Einleitung der Norm steht: „Sie legt Anforderungen zu IT-Sicherheitsleitlinien, Vorgehensweisen und Praktiken fest, die auf die Lieferanten von industriellen Automatisierungssystemen während des Lebensweges ihrer Produkte anwendbar sind sowie auf Instandhaltungsdienstleister. Im Besonderen sind Integratoren angesprochen, die technische Lösungen zu einem Gesamtsystem zusammenführen.“
Der Abschnitt **„Anforderungen an Automatisierungssysteme“** ist für Planer von Automatisierungssystemen (Systemintegratoren) relevant. Die Norm IEC 62443-3-1 [14] beschreibt zunächst die zu Grunde liegenden Technologien wie z. B. Authentifizierung, Verschlüsselung, Filterung und Logging. Der Teil IEC 62443-3-2 [15] beschreibt den Ablauf der Sicherheitsanalyse und darauf aufbauend die Strukturierung einer Anlage in Zonen (abgeschottete Bereiche) und Conduits (gesicherte Verbindungen zwischen den Bereichen). Damit soll eine automatisierungstechnische Anlage in Teilbereiche unterteilt werden, die wiederum gegeneinander abgeschottet sind. Der Teil IEC 62443-3-3 [16] beschreibt konkrete Anforderungen an Automatisierungssysteme in Form von grundlegenden Anforderungen (Foundational Requirements).
Im Abschnitt **„Anforderungen an Automatisierungskomponenten“** werden Anforderungen an Hersteller definiert. Der Teil IEC 62443-4-1 [17] definiert die Anforderungen an den sicheren Produktentwicklungslebenszyklus, der bei der Entwicklung von Komponenten für die Automatisierungstechnik durch die Hersteller zu implementieren ist.
Der Teil IEC 62443-4-2 [18] beschreibt die technischen Anforderungen für die Komponenten von Automatisierungssystemen, Applikationen und Funktionen. Die Struktur der Anforderungen folgt der IEC 62443-3-3 [16], jedoch werden hier die Anforderungen beschrieben, welche die Komponenten erfüllen müssen.
Eine ergänzende Beschreibung der weiteren Normteile findet sich in [8].

## 3. Unterschiede und Gemeinsamkeiten zwischen den zwei Normreihen

Die ISO 27000 und IEC 62443 sind zwei Normreihen, die sich auf IT-Sicherheit zum einen und OT-Sicherheit zum anderen spezialisieren, um unterschiedliche Ziele zu erreichen. Beide Normreihen sind mit der Informationssicherheit verbunden, aber sie sind auf unterschiedliche Bereiche anwendbar. Während das Ziel der Reihe ISO 27000 darin besteht, Daten und Informationen zu schützen, zielt die Reihe IEC 62443 auf den Schutz von Automatisierungslösungen zum Steuern und Überwachen von physikalischen Prozessen. Die ISO 27000-Reihe (insbesondere die ISO 27001 [4] und ISO 27002 [6]) ist für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) vorgesehen, der Fokus der IEC 62443 ist die Implementierung von sicheren Industrieautomatisierungs- und -steuerungssystemen (IACS) vorgesehen.
Bei der Reihe ISO 27000 liegt die Priorität auf die Vertraulichkeit und Integrität von Daten, bei der Reihe IEC 62443 steht die Verfügbarkeit der Automatisierungslösung im Vordergrund, um die Kontinuität des operativen Betriebs sicherzustellen. Die Normreihe IEC 62443 richtet sich an alle beteiligten Partner, die für den Schutz von industriellen Anlagen ihren Beitrag liefern müssen: Betreiber, Systemintegratoren, Wartungsdienstleister und Produkthersteller. Die Anforderungen der IEC 62443 sind speziell auf den OT-Bereich zugeschnitten
Insgesamt ist es wichtig, dass Unternehmen beide Normreihen berücksichtigen, um eine umfassende IT- und OT-Sicherheitsstrategie zu entwickeln. Eine Kombination beider Normreihen kann dazu beitragen, dass Organisationen eine konsistente Herangehensweise an die IT-Sicherheit beibehalten, während sie unterschiedliche Ansätze für IT und OT anwenden.

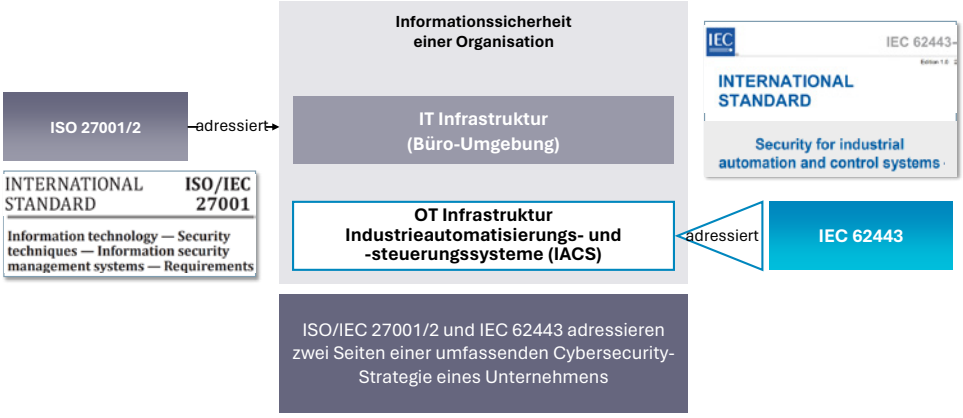


**Abbildung 3:** ISO 27001/ ISO 27002 und IEC 62443 sind zwei Bestandteile einer umfassenden Cybersecurity-Strategie.

## 4. Kombinierter Einsatz beider Normreihen für den Schutz von industriellen Anlagen

Die Normreihen ISO 27000 und IEC 62443 sind zwei komplementäre Teile eines umfassenden Ansatzes für die Security im OT-Bereich. Die Standards ISO 27001 und ISO 27002 haben sich seit vielen Jahren für die Informationssicherheit in der Office-Umgebung vieler Organisationen etabliert. Die OT-Infrastruktur von industriellen Anlagen ist in der Regel in der IT-Infrastruktur der Organisation eingebunden. Die Normreihe IEC 62443 befasst sich mit dem Schutz von industriellen Automatisierungslösungen und berücksichtigt die spezifischen Belange von OT-Umgebungen. Jedoch sind viele Verfahren und Anforderungen der IT unverändert auch im OT-Bereich anzuwenden. Die Prozesse und das Management der Security im OT-Bereich sollten daher Bestandteil eines einheitlichen Ansatzes sein und auf bestehende Informationssicherheit auf Basis der Normreihe ISO 27000 aufbauen.

### 4.1 Das ISMS als übergreifende Komponente

Die Normreihe ISO 27000 hat den Anspruch, für verschiedene Organisationen anwendbar zu sein, die ganz unterschiedlich in Struktur, Größe oder Zweck sein können. Das Fundament der Informationssicherheit ist die Verwaltung der Security entsprechend einem Informationssicherheitsmanagementsystem (ISMS). In der ISO 27001 [19] sind die Anforderungen an Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS in den Abschnitten 4 bis 10 enthalten. Die Norm schreibt vor, dass alle Anforderungen erfüllt sein müssen, wenn eine Organisation die Konformität mit der ISO 27001 für sich beansprucht. Dies gilt auch für die Organisation der Security des Betreibers eines industriellen Produktionsbereichs.

Die Eigenschaften und Ziele eines ISMS wie zum Beispiel Verantwortlichkeiten und Befugnisse vom obersten Management zuweisen, verbindliche Ziele durch das Topmanagement vorgeben oder Planung und Durchführung von Maßnahmen zum Umgang mit Risiken und Chancen sind auch für den Produktionsbereich eines Unternehmens relevant. Für die Verwaltung der Security im OT-Bereich gilt es, die ISMS-Anforderung der ISO 27001 für die OT-Umgebung anzupassen.

### 4.2 Die zwei Normreihen als Basis für den Schutz von industriellen Anlagen

Zusätzlich zu den Anforderungen für ein ISMS beinhalten die ISO 27001 und ISO 27002 Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Diese decken alle Security-Belange eines ganzheitlichen Ansatzes zur Risikominderung ab und sind als Vorschlag zu verstehen. Die Anforderungen für den betrachteten Anwendungsbereich sollen entsprechend ihrer Relevanz ausgewählt werden. Die ISO 27002 sieht vor, dass je nach Anwendungsbereich zusätzliche Anforderungen hinzugefügt werden können. Es bietet sich an, die zusätzlichen Anforderungen für den OT-Bereich aus der IEC 62443 zu nehmen.

Die Normreihe IEC 62443 adressiert OT-spezifische Belange für die Security im OT-Bereich. Für den Schutz von industriellen Anlagen müssen Anforderungen an Verfügbarkeit und Integrität erfüllt sein, um die Aufrechterhaltung des operativen Betriebs und den Schutz von Menschen, und Umwelt sicherzustellen. Der Verlust des operativen Betriebs kann z. B. eine Explosion, ein Stromausfall oder die fehlerhafte Dosierung einer lebensrettenden Medizin zur Folge haben. Viele Anlagen beinhalten gezielte Sicherheitssysteme zum Schutz von Menschen und Umwelt. Die Security-Anforderungen der Reihe IEC 62443 wurden mit dem Ziel definiert, einen sicheren operativen Betrieb sicherzustellen.

Die geschilderte Diskussion zeigt auf, wie die Normreihe IEC 62443 die Normreihe ISO 27000 mit Besonderheiten der OT-Umgebung erweitert. Die IEC 62443 deckt jedoch nicht alle Bestandteile ab, die für den Schutz von industriellen Anlagen erforderlich sind. Insbesondere sind keine Anforderungen an ein ISMS enthalten. Die Norm nimmt an, dass diese von einer anderen Norm, z. B. der ISO 27001, definiert werden. Deshalb macht es Sinn, beide Standards für den Schutz von industriellen Anlagen zu kombinieren (s. Abbildung 4). Der betrachtete Anwendungsbereich ist der industrielle Produktionsbereich. Deshalb sollte die IEC 62443-2-1 [11], die das Security-Programm des Betreibers betrifft, in Verbindung mit der Normreihe ISO 27000 gebracht werden. Die weiteren Dokumente der IEC 62443-Serie adressieren die Beiträge von Systemintegratoren, Wartungsdienstleistern und Produktherstellern für den Schutz von industriellen Anlagen des Betreibers ab. Die Anforderungen in diesen

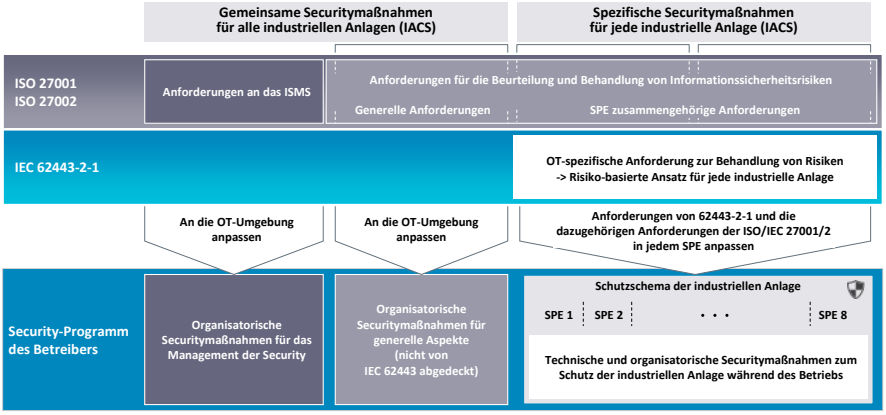


**Abbildung 4:** Kombination der Anforderungen der ISO 27001/ISO 27002 und der IEC 62443-2-1 für Security-Programme des Betreibers.

Dokumenten haben ihren Ursprung in den Security-Anforderungen der IEC 62443-2-1 [11].

**Erweiterung und Anpassung des ISMS für den industriellen Produktionsbereich**

Obwohl die Normreihe IEC 62443 keine Anforderung an ein ISMS stellt, fordert die erste Anforderung der IEC 62443-2-1 [11], dass das Security-Programm des Betreibers mit einem etablierten ISMS koordiniert werden muss. Es wird empfohlen, dass Organisationen die Security im IT-Bereich auf Basis eines ISMS nach ISO 27001 [4] etablieren. Das Security-Management im Produktionsbereich sollte auf dem bestehenden ISMS basieren und für die OT-Umgebung angepasst werden. Dies erfordert z. B., dass zwischen IT und Produktion klare Verantwortlichkeiten für die Verwaltung der Schnittstellen definiert werden, die Einzigartigkeit der fachlichen Kompetenzen in IT bzw. OT in der Ressourcenplanung berücksichtigt wird und die Konzepte und Begriffe beider Standards effektiv benutzt werden.

**Berücksichtigung der Anforderungen der ISO 27001/ISO 27002 für die Gestaltung der Security-Maßnahmen nach IEC 62443-2-1**

Ein pragmatischer Ansatz, die Anforderungssätze der ISO 27001/ISO 27002 und die der IEC 62443-2-1 in Zusammenhang zu bringen, ist es die bestehende Struktur der IEC 62443-2-1 in sogenannten Security-Programm-Elementen (SPE) zu verwenden. Die SPE bilden Anforderungsgruppen, die jeweils ein Teil der Security-Belange eines ganzheitlichen Schutzschemas von industriellen Anlagen bilden. Beispiele dafür sind *Security der Netzwerke und Kommunikation, Konfigurationsmanagement, Security der Komponenten, Zugriffskontrolle der Anwender oder Schutz der Daten*. Einige Elemente sind in Untergruppen aufgeteilt, um spezifische Belange abzudecken. So wurde z. B. für *Fernzugriff* oder *kabellose Kommunikation* eine eigene Untergruppe im SPE 3 - *Security der Netzwerke* und Kommunikation gebildet.

Es macht Sinn, zu jedem Element und ggf. Untergruppe der IEC 62443-2-1 die dazugehörigen Anforderungen der ISO 27001/ISO 27002 hinzuzufügen. Bei der Auslegung der Security-Maßnahmen zum Schutz der industriellen Anlagen sollten die Gesamtheit der Anforderungen berücksichtigt werden. Zu bemerken ist, dass dies nicht bedeutet, dass alle Anforderungen erfüllt werden müssen. Die relevanten Anforderungen sollten in einem Risiko-basierten Ansatz entsprechend der Bedarfsanalyse für die jeweilige industrielle Anlage bewertet werden.

Obwohl die meisten Anforderungen der ISO 27001/ISO 27002 einem oder mehreren SPE zuzuordnen sind, sind einige von genereller Art, wie z. B. *Kontakt mit Behörden*, *Beschäftigungs- und Vertragsbedingungen* oder *Geistige Eigentumsrechte*. Die Normreihe IEC 62443 deckt diese Aspekte nicht ab. Die Relevanz und Anwendung dieser generellen Anforderungen müssen von dem Betreiber einer industriellen Produktionsanlage einzeln bewertet werden.

Das Hinzufügen der dazugehörigen Anforderungen der ISO 27001/ISO 27002 zu jedem SPE bzw. Untergruppe bringt Vorteile mit sich. Dies soll anhand von SPE 3 – *Security der Netzwerke und Kommunikation* / Untergruppe NET 3 – *Fernzugriff* dargestellt werden.

Anlagenteile werden oft aus Arbeitsplätzen außerhalb des Produktionsbereichs durch externe Dienstleister gewartet. Das Erlauben eines Fernzugriffs für einen externen Dienstleister muss genau geregelt werden, um die dadurch entstandene Angriffsfläche möglichst gering zu halten. Demzufolge sind in der Untergruppe NET 3 – *Fernzugriff* die Anforderungen der IEC 62443-2-1 stringent gestaltet:

» **NET 3.1:** Nur autorisierte Applikationen im Rahmen eines Fernzugriffs erlauben.

» **NET 3.2:** Sicherstellen, dass erlaubte Fernzugriffe dokumentiert sind, einschließlich der Beschreibung von Anlass, Umstand, verwendete Verschlüsselungs- und Authentisierungstechnologies, Zeitdauer, Ort und Identität des externen Arbeitsplatzes.

» **NET 3.3:** Sicherstellen, dass ruhende Verbindungen nach einer bestimmten Zeitdauer getrennt werden.

Diese OT-spezifischen Anforderungen sind eine zusätzliche Detaillierung der Anforderungen der ISO 27001/ISO 27002, die die Telearbeit ansprechen. Im Abbildung 5 sind beispielhaft einige Anforderungen der ISO 27001/ISO 27002 dargestellt, die zu diesem Thema gehören.

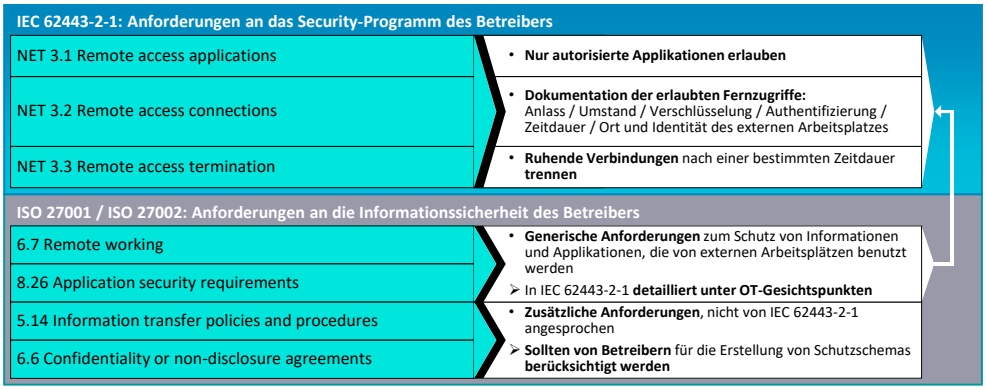


**Abbildung 5:** Hinzufügen von Anforderungen der ISO 27001 / ISO 27002 bei der Gestaltung von Anwendungsfällen mit Fernzugriff.

Die ISO/IEC 27001/ISO 27002 fordert den Schutz der Informationen, die in externen Arbeitsplätzen verarbeitet oder gespeichert werden, die Sicherung von Anwendungsdiensten in öffentlichen Netzwerken und den Schutz der Transaktionen bei Anwendungsdiensten. Die o. g. Anforderungen der IEC 62443-2-1 ergänzen hier die ISO 27001/ISO 27002 mit spezifischen Anforderungen für den OT-Bereich. Darüber hinaus deckt die ISO 27001/ISO 27002 Aspekte ab, die nicht von der IEC 62443 angesprochen werden, die aber durchaus für den Anwendungsfall eines Fernzugriffs durch einen externen Dienstleister wichtig sein können:

» Festlegung von Richtlinien und Verfahren zur Informationsübertragung

» Vereinbarungen zur Informationsübertragung

» Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Bei der Gestaltung von Anwendungsfällen, die einen Fernzugriff auf eine industrielle Anlage benötigen, sollten alle Aspekte berücksichtigt werden, die von beiden Standards gedeckt werden. Weitere Informationen zur Security von Fernzugriffen finden sich auch in [20].

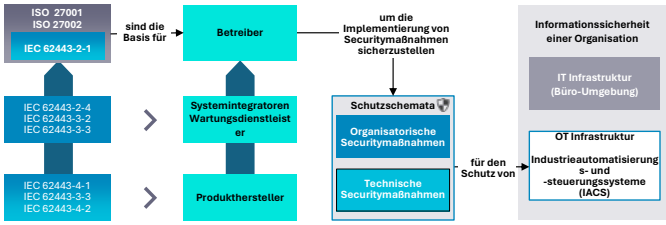


**Abbildung 6:** Die IEC 62443 adressiert alle für den Schutz von industriellen Anlagen beteiligten Partner.

### 4.3 Die IEC 62443 bringt einen Mehrwert in einem kombinierten Ansatz

Um ihre industriellen Anlagen zu schützen, sind Betreiber darauf angewiesen, dass technische Lösungen mit geeigneten Security-Maßnahmen entwickelt werden. Dafür müssen Produkte mit entsprechenden Security-Funktionen auf dem Markt verfügbar sein. Die Normreihe IEC 62443 bietet den Mehrwert, alle beteiligten Partner anzusprechen, welche diese unterstützen müssen. Abbildung 6 zeigt die Verbindung der

**Tabelle 1:** Beispiele von spezifischen OT-Herausforderungen.

| Anforderungen der ISO 27001 und ISO 27002 | Herausforderungen im OT-Bereich | Referenz in IEC 62443 |
|---|---|---|
| 7.7. Clear desk and clear screen | Das Sperren des Operator-Bildschirms kann einen unsicheren Zustand bewirken | *ISA/IEC 62443-2-1 USER 1.18* sieht vor, dass Operator-Bildschirme von automatischen Bildschirm-Sperren ausgeschlossen sein können |
| 8.7 Protection against malware | Antivirus-Produkte sind oft nicht kompatibel mit OT-Systemen | *ISA/IEC 62443-2-1 COMP 2.3* fordert einen Test der Kompatibilität der Antimalware-Software |
| 8.13 Information backup | Die Netzwerk-Belastung von automatischen Sicherungen kann Sicherheitsmeldungen blockieren | *ISA/IEC 62443-3-3 SR 5.1 RE(1)* fordert eine physikalische Segmentierung zwischen kritischen und nicht-kritischen Netzwerksegmenten |
| 8.8 Management of technical vulnerabilities | Das Patchen kann den operativen Betrieb unterbrechen | *ISA/IEC 62443-2-3 section 5 part f* Fordert das Testen und Planen der Patch-Aktivitäten, um die Kontinuität des operativen Betriebs sicherzustellen |

ISO 27001/ISO 27002 und der IEC 62443 sowie die Beitragskette der beteiligten Partner für die Erstellung von ganzheitlichen Schutzschemata zum Schutz von industriellen Anlagen.
Die ISO 27001 beinhaltet vier Anforderungen (5.19 bis 5.22) bezüglich Lieferanten und Lieferantenbeziehungen sowie viele Hinweise zu Lieferanten in den zusätzlichen Anleitungen von anderen Anforderungen. Die Normreihe IEC 62443 unterstützt die Implementierung solcher Anforderungen durch jeweilige Dokumente, die die Pflichten der Lieferanten in ihren unterschiedlichen Rollen festlegen. Das gibt den Betreibern die Basis, Security-Forderungen an Systemintegratoren, Wartungsdienstleister oder Produkthersteller zu stellen. Zum Beispiel fordert die IEC 62443-4-1 [17], dass Hersteller Gegenmaßnahmen für möglichen Bedrohungen in ihren Produkten einbauen, Security-Prinzipien beim Design vorgeben, schwachen Code durch Vorgabe von Programmierrichtlinien verhindern, Security-Schwachstellen mit Test-Techniken, wie Fuzz-Testing, Penetrationstest oder binäre Codeanalyse auffinden, Security-Richtlinien für die Benutzer des Produkts erstellen und einen Prozess zur Behandlung von entdeckten Schwachstellen während der Vermarktung etablieren.
Die IEC 62443-4-2 [18] stellt auch Anforderungen an die Security-Fähigkeiten von Produkten und Lösungen und differenziert die Stärke der Security-Maßnahmen in vier Security-Level entsprechend dem tolerablen Restrisiko des Betreibers.

## 5. Fazit und Ausblick

Die ISO 27001/ISO 27002 und die Normreihe IEC 62443 ergänzen sich gegenseitig für die Implementierung von ganzheitlichen, Risiko-basierten Schutzschemata für industrielle Anlagen:

- Die kombinierten Anforderungen der ISO 27001 [4]/ISO 27002 [6] und IEC 62443-2-1 [11] sind die Basis für Betreiber bei der Erstellung von Security-Programmen, die die Implementierung von technischen und organisatorischen Security-Maßnahmen sicherstellen.
- Die Anforderungen der IEC 62443-2-4 [13], IEC 62443-3-3 [16] und IEC 62443-3-2 [15] sind die Basis für Systemintegratoren und Wartungsdienstleistern für das Design und die Wartung von technischen Lösungen mit adäquaten Security-Fähigkeiten.
- Produkthersteller können Betreiber, Systemintegratoren und Wartungsdienstleistern auf Basis der Anforderungen der IEC 62443-4-1 [17] unterstützen mit der Bereitstellung von gut entwickelten Produkten mit adäquaten Security-Funktionen und durch Aufrechterhaltung des Security-Zustands der Produkte während der Kommerzialisierung.

Die Anforderungen der IEC 62443-3-3 [16] und IEC 62443-4-2 [18] sind die Basis für die Produkthersteller, nach Levels differenzierte Security-Fähigkeiten in Produkten und Lösungen zu entwickeln.
Künftig werden weitere Anforderungen in Bezug auf die OT-Security zu beachten sein, die sich aus der europäischen Regulierung ergeben. Allgemein wird künftig der Cyber Resilience Act für Geräte mit digitalen Elementen gelten. Ein erster Entwurf [21] liegt vor, befindet sich aber noch in der Abstimmung. Für Betreiber kritischer Infrastrukturen ist die NIS2-Richtline [22] von Interesse. Diese Richtlinie wurde auf EU-Ebene bereits verabschiedet und wird zurzeit in deutsches Recht umgesetzt [23, 24].

## Danksagung

Dieses Papier fasst die Vorarbeiten der Autoren Niemann [8] und Kobes [25] zusammen. Diese beiden Dokumente sind unabhängig voneinander entstanden. Prof. Niemann dankt dem ABB Center of Expertise PLC in Heidelberg für die Unterstützung bei der Erstellung des ursprünglichen Beitrags. Dr.Kobes dankt der ISA GCA für die Zusammenarbeit bei der Erstellung seines ursprünglichen Beitrags. Beide genannten Dokumente betrachten das hier beschriebene Thema mit höherem Detaillierungsgrad und sind zur weiteren Vertiefung empfohlen.

## Referenzen

[1] DIN EN ISO/IEC 27000. (2020). Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018). Deutsche Fassung EN ISO/IEC 27000:2020. Abgerufen von: https://www.iso27001security.com/html/27000.html.

[2] IsecT Ltd. (2020). Overwiew on ISO 27000 standard series. Abgerufen von: https://www.iso27001security.com/html/iso27000.html.

[3] Kroeselberg, D., Buchi, F., u. Meulenbroek, H. (2017). *Cyber Security Tutorial Energy Automation and IEC 62443*. Abgerufen von: https://www.pcic-library.com/sites/default/files/final/EUR17_63.pdf.

[4] DIN EN ISO/IEC 27001:2023-Entwurf. (2023). Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022).Deutsche und Englische Fassung prEN ISO/IEC 27001:2023

[5] Brenner, M., Gentschen Felde, N., Hommel, W., Metzger, S., Reiser, H., & Schaaf, T. (2011). Praxisbuch ISO/IEC 27001. *Carl Hanser Verlag GmbH & Co. KG. 2022*

[6] DIN ISO/IEC 27002. (2022). Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022). Deutsche und Englische Fassung prEN ISO/IEC 27002:2022 – Entwurf.

[7] DIN EN ISO/IEC 27019. (2020). Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08). Deutsche Fassung EN ISO/IEC 27019:2020.

[8] Niemann, K. H. (2021). *Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443: eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie.* ABB Automation Products GmbH. https://doi.org/10.25968/opus-1973.

[9] IEC 62443. (2023). Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung, 2023. Abgerufen von: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung.

[10] IEC/TS 62443-1-1. (2009). Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. Abgerufen von: https://webstore.iec.ch/publication/7029.

[11] DIN EN IEC 62443-2-1:2020 - Entwurf VDE 0802-2-1:2020. (2020). IT-Sicherheit für industrielle Automatisierungssysteme – Teil 2-1: Anforderungen

an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC 65/756/CDV:2019). Deutsche und Englische Fassung prEN IEC 62443-2-1:2019.

[12] IEC TR 62443-2-3. (2015). Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment. Technical Report. Abgerufen von: https://www.vde-verlag.de/iec-normen/221941/iec-tr-62443-2-3-2015.html.

[13] DIN EN IEC 62443-2-4 (VDE 0802-2-4). (2023). IT-Sicherheit für industrielle Automatisierungssysteme. Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 65/936/CDV:2022).Deutsche und Englische Fassung prEN IEC 62443-2-4:2022.

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

[15] DIN EN IEC 62443-3-2:2021 (VDE 0802-3-2:2021). (2021). IT-Sicherheit für industrielle Automatisierungssysteme – Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 62443-3-2:2020). Deutsche Fassung EN IEC 62443-3-2:2020

[16] DIN EN IEC 62443-3-3:2020 (VDE 0802-3-3:2020-01). (2020). Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014).Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019

[17] DIN EN IEC 62443-4-1:2018 (VDE 0802-4-1). (2018). IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1 :2018). Deutsche Fassung EN lEC 62443-4-1 :2018

[18] DIN EN IEC 62443-4-2:2019 (VDE 0802-4-2:2019). (2019). IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019). Deutsche Fassung EN IEC 62443-4-2:2019

[19] DIN EN ISO/IEC 27001:2023:2023-04. (2023). Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022). Deutsche und Englische Fassung prEN ISO/IEC27001:2023 Entwurf.

[20] Langreder, P., Schmidt, F., Niemann, K. H. (2022). Fernwartung und OT-Security-Anforderungen und Implementierungsansätze. *atp magazin*, *64*(9), 64-73.

[21] European Commission. (2022). Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Cyber Resilience Act.

[22] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). (2022). NIS-Richtlinie. In: Amtsblatt der Europäischen Union.

[23] Bundesverband der Deutschen Industrie e.V. (2023). *Zweiter Leak NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. Kommentierung des Entwurfs vom 3. Juli 2023.* Abgerufen von: https://bdi.eu/publikation/news/zweiter-leak-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz

[24] Bundesministerium des Innern und für Heimat. (2023). *Diskussionspapier des Bundesministeriums des Innern und für Heimat Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland*. Abgerufen von: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.pdf?__blob=publicationFile&v=2

[25] Kobes, P. (2021). Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments. Abgerufen von: https://gca.isa.org/blog/white-paper-excerpt-applying-iso/iec-27001/2-and-the-isa/iec-62443-series-for-operational-technology-environments

## AUTOREN

Prof. Dr.-Ing. Karl-Heinz Niemann vertritt seit 2005 die Bereiche Prozessinformatik und Automatisierungstechnik an der Hochschule Hannover (HsH). Seit Anfang 2023 ist er Vorstand des Institutes für Sensorik und Automation der HsH. Zusätzlich ist er im Mittelstand Digitalzentrum Hannover und im Zukunftslabor Produktion des ZDIN tätig. Von 2002 bis 2005 war er an der Fachhochschule Nordostniedersachsen (heute Leuphana Universität) für den Bereich Prozessdatenverarbeitung zuständig. Zuvor war er in führenden Positionen in der Entwicklung von Prozessleitsystemen bei ABB, Elsag Bailey und Hartmann & Braun tätig.

**Prof. Dr.-Ing. Karl-Heinz Niemann**
Hochschule Hannover
Fakultät I - Elektro- und Informationstechnik
Postfach 92 02 61
30441 Hannover
✆ +49 511 92 96 12 64
@ karl-heinz.niemann@hs-hannover.de
www.orcid.org/0000-0001-8931-6789

Dr. Pierre Kobes blickt auf eine langjährige Erfahrung in der Automatisierungssparte von Siemens zurück. In den letzten zehn Jahren seiner Karriere war er verantwortlich für Standards, Regulierungen und Zertifizierungen. Er hat maßgeblich an der Entwicklung der Normenreihe IEC 62443 mitgewirkt und ist der Autor des Buchs „Guideline Industrial Security – IEC 62443 is easy!". Er ist seit 2020 als Berater tätig und treibt aktiv in Arbeitsgruppen der ISA99 und der DKE die Weiterentwicklung der Normenreihe IEC 62443 voran.

**Dr. Pierre Kobes**
Dr. Kobes Consulting
Kressenwiesenweg 26
69207 Sandhausen
@ kobes@kobesconsulting.de
www.kobesconsulting.de