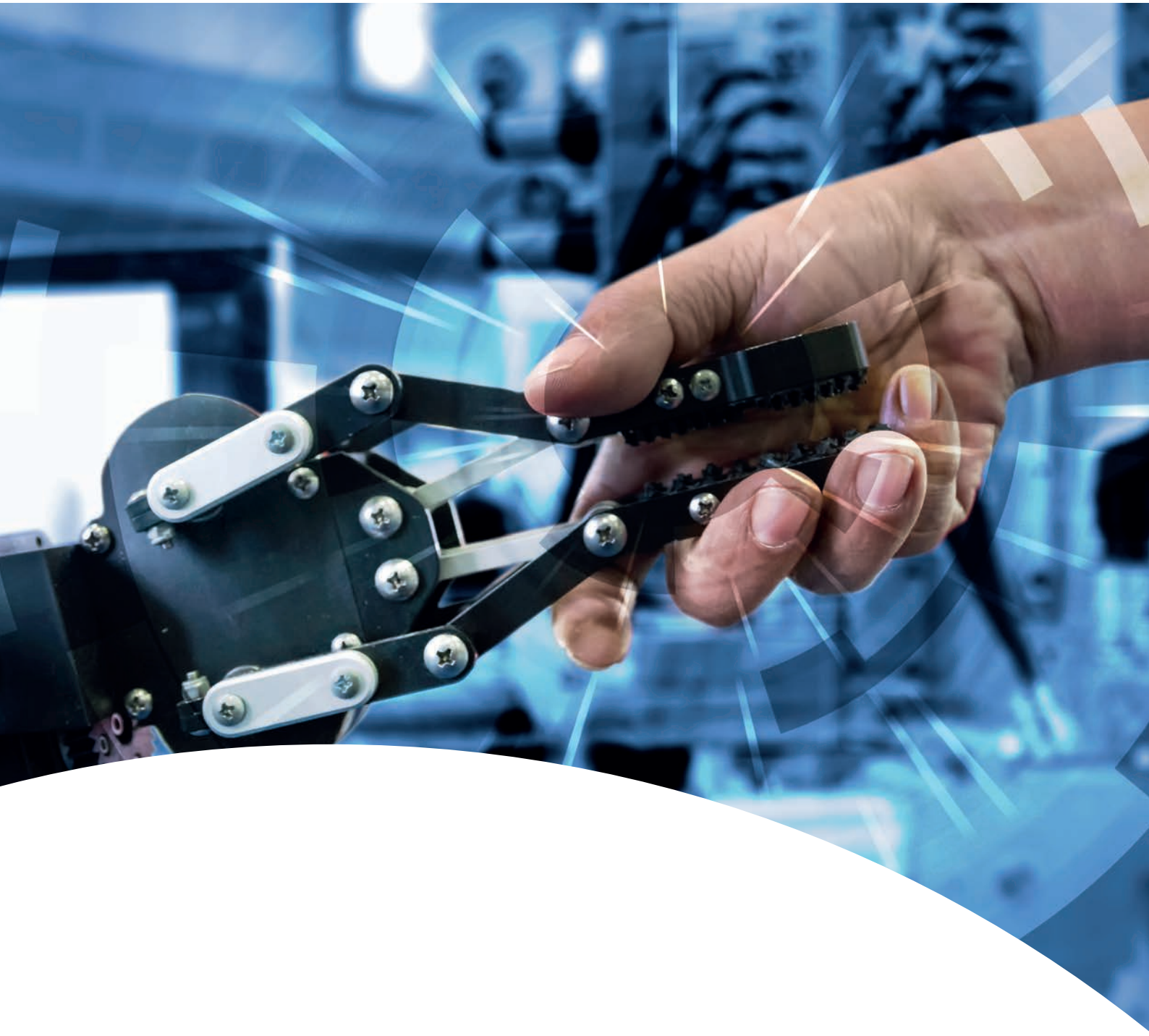
IEC 62443 richtig angewendet

# Industrial Security komplett durchdacht



TÜV®

TÜV NORD Zertifizierung

TÜV NORD GROUP

# Zukunftssicherung für Industrieunternehmen

Vernetzung im Bereich der Sensorik und Aktorik ist in der Industrie seit Jahren unverzichtbar. Für diese Anwendungen haben sich verschiedene Standards parallel entwickelt, die in unterschiedlichen Sektoren vielfältig eingesetzt werden. Industriesysteme waren bisher allerdings Inseln und von den Office-Netzwerken getrennt. Dies hat sich den letzten Jahren komplett geändert: Industrielle Netzwerke wurden geöffnet und mit anderen IT-Komponenten verbunden. Es liegt im Trend, Cloud-Infrastrukturen anzubinden, um mit ihrer Hilfe neue Geschäftsmodelle zu erschließen. Sehr verbreitet sind heute Digitale Zwillinge von Industrieanlagen – die Simulation der Anlage in der Cloud, wodurch sich wieder ganz neue Anwendungen und Potenziale ergeben. Diese Tendenzen bei Vernetzung und neuen Geschäftsmodellen sind häufig Teil der Digitalisierungsstrategien von Unternehmen oder ganzen Sektoren. Ihre Chancen führen aber auch zu neuen Risiken.

Jegliche Vernetzung und damit verbundene Öffnung bringt die Gefahr von Missbrauch durch unberechtigte Personen mit sich. Jedes Industrieunternehmen braucht daher neben einer Digitalisierungsstrategie auch eine Strategie zur Sicherung der eigenen Werte – des Produktionsprozesses, des eigenen Know-hows und der Elemente, auf denen das eigene Geschäftsmodell basiert. Eine solche Cybersicherheitsstrategie sollte auf fundierten Konzepten und Methoden basieren. Für Industrielle Sicherheit wurde die Norm IEC 62443 definiert. Sie enthält ein etabliertes Vorgehensmodell für eine industrielle Cybersicherheitsstrategie und ist damit unkoordinierten Einzelaktivitäten klar überlegen.

### Cybersicherheits-Zertifizierungen am Horizont

Der europäische Gesetzgeber hat zudem mit dem Cyber Security Act (CSA) eine Initiative gestartet, um in Zukunft europaweite Cybersicherheits-Zertifizierungen für Industriesegmente einfordern zu können. Inwieweit dies freiwillig oder verpflichtend erfolgt, wird sich erst in der Ausgestaltung zeigen. Es ist nach aktuellen Diskussionen damit zu rechnen, dass mindestens Zulieferer im Bereich der Kritischen Infrastrukturen (KRITIS) zukünftig unter die Zertifizierungspflicht fallen. Aktuell geht es also darum, sich auf die neuen Anforderungen vorzubereiten, um später aus einer starken Position agieren zu können, sobald gesetzliche Verpflichtungen wirksam werden.

Zudem sollte Sicherheit über einen ganzheitlichen Ansatz verfolgt werden. Zu betrachten sind sowohl die eingesetzte Technik als auch die genutzten Prozesse. Falls einer dieser Aspekte nicht berücksichtigt wird, kann kein effektives Sicherheitskonzept umgesetzt werden.

Die Norm IEC 62443 berücksichtigt genau dies und adressiert die drei typischen Rollen in der Industrie: Betreiber, Integratoren und Hersteller von Komponenten.



# Auf einmal steht die komplette Produktion still

**Betreiber von Industrieanlagen müssen den Schutz vor digitalen Bedrohungen sicherstellen. Eindeutig definierte Vorgehensmodelle, wie sie in der Norm IEC 62443 beschrieben sind, helfen dabei.**

Mitte 2017, nach den aufsehenerregenden Ausbrüchen des Erpressungstrojaners WannaCry, rollte eine zweite Ransomware-Welle um den Globus. Dabei handelte es sich um eine neue Variante des Trojaners Petya. Doch wie Sicherheitsforscher im weiteren Verlauf feststellten, war das Ziel dieses Angriffs gar nicht die Erpressung von Lösegeld. Eine Reihe von Indizien deutete vielmehr auf eine politisch motivierte Cyberattacke hin.

Denn das Angriffsziel war vor allem die Ukraine. Die neue Petya-Version verbreitete sich zuerst über ein Update der in der Ukraine programmierten Steuersoftware MeDoc. Was den Angriff weit über die Grenzen des osteuropäischen Staates hinaus wirken ließ: Praktisch alle Unternehmen, die in der Ukraine Steuern zahlen müssen, nutzen diese Software. Betroffen waren mehrere internationale Großkonzerne, unter anderem der dänische Logistikriese Maersk. Über ein gefälschtes Microsoft-Zertifikat, das von der MeDoc-Software anscheinend nicht gründlich genug geprüft wurde, verschaffte sich der Trojaner Zugang zu den befallenen Systemen.

### Die Gegenmaßnahmen sind wohlbekannt

Wieder einmal betonten Sicherheitsforscher, welche Maßnahmen zur Verteidigung unverzichtbar seien: Alle aktuellen Sicherheits-Updates in Windows einspielen, die Signaturdateien des verwendeten Virenscanners aktuell halten – und regelmäßige Backups des Systems und aller von ihm verwalteten Daten auf abgesicherten, physisch vom Netzwerk getrennten Sicherungssystemen erstellen. Bei der Frage, wie solche Vorfälle zukünftig verhindert werden und was wirksame Strategien gegen Angriffe sein können, die zum Stillstand von Industrieanlagen und damit zu Produktionsausfällen führen können, war die Antwort also klar: Im Fall von Petya wie auch von WannaCry war die Lösung ein kontinuierliches Patchen des Betriebssystems.

### Nur aktuelle Betriebssysteme bieten Sicherheit

Inbesondere industrielle Steuerungen basieren jedoch häufig auf dem eigentlich veralteten Windows XP. Hier ist eine Umsetzung der genannten Schutzmaßnahmen gar nicht ohne Weiteres möglich, da dieses Betriebssystem bereits regulär keine Updates mehr erhält. In diesem Fall ist deshalb ein Update des gesamten Betriebssystems die einzig richtige Lösung. Aktuell gehaltene Windows-10-Systeme waren von vielen Schadsoftware-Attacken wie WannaCry nicht betroffen und auch gegen andere Angriffsvarianten deutlich besser geschützt.

*Im industriellen Umfeld gibt es gute Gründe, warum Rechner nicht immer mit den jeweils neuesten Betriebssystem-Versionen ausgerüstet werden. Doch die Bedrohung durch Schadsoftware erfordert bei vernetzten Systemen eine regelmäßige Aktualisierung – zumindest durch Einspielen relevanter Patches.*

# Szenario 1: Betreiber von Industrieanlagen

Auch hier bewährt sich das in der Norm IEC 62443 beschriebene vollständige Vorgehensmodell. Setzt ein Unternehmen die von der Norm vorgesehenen Maßnahmen konsequent um, führen die darin definierten Anweisungen dazu, dass erforderliche Patches ins System eingespielt werden.

Zudem besitzt die Norm eine umfangreiche Best-Practice-Handlungsempfehlung, um das komplizierte Problem des Patch-Managements von Industriekomponenten zu lösen. Die konkrete Anforderung lautet „COMP 3.2: Security patch testing and installation“ (siehe auch Infokasten unten auf dieser Seite). Sie besagt, dass nach einem Kompatibilitätstest verfügbarer Patches diese in einer akzeptablen Zeit installiert werden müssen. Relevant ist hier vor allem, dass Maßnahmen, die an sich bekannt sind, aber aus unterschiedlichen Erwägungen in der Praxis dann doch nicht umgesetzt werden, von der Norm eindeutig eingefordert werden. Neben dieser enthält IEC 62443 noch eine umfangreiche Serie an weiteren Anforderungen, um typischen Gefährdungen von Industriellen Anlagen wirksam zu begegnen.

### Bedrohungen werden zunehmen

Die Umsetzung der Norm IEC 62443 stellt ein Vorgehensmodell dar, um Sicherheit nicht nur punktuell, sondern ganzheitlich anzugehen. Solche Vorgehensmodelle werden mittlerweile immer wichtiger, da im Industrieumfeld die Frage nach Cybersecurity steigende Priorität hat und die Bedrohungslage zudem steigt. Die erwähnten Trojaner Petya und WannaCry sind Beispiele für eher breit gestreute Angriffe, die mehr oder weniger jeden Windows-basierten Rechner ins Visier nahmen. Mittlerweile sind aber auch schon Fälle bekannt, in denen Industriekomponenten oder Sicherheitssysteme gezielt attackiert wurden.

Der öffentlich bekannt gewordene Vorfall TRITON ereignete sich im Dezember 2017 und richtete sich gegen eine konkret installierte industrielle Sicherheitssteuerung im Mittleren Osten. Bei diesem Vorfall wurde der sichere Zustand ausgelöst – es wird allerdings vermutet, dass die Angreifer eigentlich versuchten, die Sicherheitssteuerung wirkungslos werden zu lassen. Wir müssen uns also darauf einstellen, dass zukünftig weitaus mehr und aggressivere Angriffe gegen Industrieanlagen stattfinden werden. Belastbare Vorgehensweisen wie die der Norm IEC 62443 einzuführen wird daher immer wichtiger.

## IEC 62443-2-1, COMP 3.2

Der Normteil IEC 62443-2-1 (Entwurfsfassung) definiert in der Anforderung COMP 3.2: Security patch testing and installation Folgendes: „Security patches applicable to device software shall be tested for compatibility with the IACS, approved for installation and installed within a time period after their release that meets acceptable risk targets.“

PCs in Industrieanlagen erfüllen hochspezialisierte Aufgaben. Daher gibt es die Tendenz, das System möglichst nicht zu verändern. Doch auf das Einspielen von Updates und Patches zu verzichten, birgt bei den oft vitalen Systemen hohe Sicherheitsrisiken.

# Sicherheit muss integraler Bestandteil sein

**Integratoren sind heute nicht nur durch die Bereitstellung von Vernetzung oder gar die Anbindung von Anlagen an Cloud-Dienste gefordert. Sie müssen auch die Sicherheit des Systems von Anfang an in ihren Konzepten mit berücksichtigen.**

Heute ist eine Vernetzung von Komponenten industrieller Anlagen untereinander oder mit der Außenwelt weit verbreitet. Ein Beispiel ist etwa die direkte Anbindung der Fabrikräume an ein IT-Rechenzentrum. Solche Verbindungen sind die Voraussetzung für eine effiziente Steuerung von Produktionsanlagen oder einen belastbaren Überblick über aktuelle Kennwerte in MIS- oder ERP-Systemen (Management Information Systems, Enterprise Resource Planning). Die Vorteile solcher Lösungen sind so ausgeprägt, dass die Motivation für eine Vernetzung stark ansteigt – auch in Segmenten oder Unternehmen, wo dies bisher nicht der Fall war.

### Klares Bild vom anfallenden Planungs- und Betriebsaufwand

Daraus resultieren für Unternehmen wichtige Zukunftschancen. Allerdings setzt Vernetzung eine umfassende Strategie voraus. Unternehmen, die Schritte dieser Art umsetzen wollen, müssen sich über den damit einhergehenden Planungs- und Betriebsaufwand im Klaren sein. Insbesondere ist die Vernetzung industrieller Anlagen nicht ohne Investitionen in angemessene Sicherheitsmaßnahmen möglich.

### Sicherheit von Anfang an mit konzipieren

Denn Netzwerke sind nicht nur die Grundlage für integrierte Systeme, sondern leider auch ein Einfall- und Verbreitungsweg für allgegenwärtige Schadsoftware. Besonders problematisch ist es, wenn bereits in Test- und Entwicklungsphasen eine Vernetzung ohne Schutzmaßnahmen stattfindet.

Damit sind solche Systeme vom Tag 1 an gefährdet und bieten Schadsoftware möglicherweise Gelegenheit, sich von Anfang an im System einzunisten und dort für längere Zeit in einen Schlafzustand zu fallen, um erst wesentlich später (auch nach der Implementation entsprechender Schutzmaßnahmen) aktiv zu werden.

Besonders hohe Risiken bergen vernetzte Industrieanlagen mit Übergängen ins Internet. Prinzipiell müssen Integratoren vernetzter Industrieanlagen die von ihnen realisierten Systeme sowohl gegen gezielte Angriffe absichern, die sich gegen ihre konkrete Infrastruktur richten, als auch gegen zufällige beziehungsweise breit angreifende Schadsoftware, die auf allgemeine Schwachstellen in der Sicherheitsarchitektur zielt. Eine typische Bedrohung sind dabei nicht zuletzt sogenannte Man-in-the-middle-Attacken – ein Angreifer schleust sich selbst in die Kommunikationskette ein, indem er sich den jeweiligen Gegenstellen als ihren rechtmäßigen Kommunikationspartner ausgibt. Auf diese Weise lassen sich nicht nur vertrauliche Daten ausspionieren, sondern auch Kommunikationsinhalte verändern. Die problematischen Auswirkungen kann man sich leicht ausmalen.

*Vernetzung oder gar die Integration von Cloud-Lösungen vergrößert die Anforderungen an Schutz- und Sicherheitskonzepte von Industrieanlagen. Diese Anforderungen bereits bei der Konzeption von Architekturen und Kommunikationsketten mit zu berücksichtigen, wird zu einer zentralen Aufgabe für Integratoren.*

# Szenario 2: Integratoren von Industrieanlagen

**Schutzkonzept ist eine wichtige Teilaufgabe für Integratoren**
Einen Lösungsansatz bietet die Norm IEC 62443 mit dem Konzept einer kontrollierten Vernetzung und der Bildung von Zonen zur Separierung und Abtrennung von Kommunikationspartnern. Zu diesem Zweck können Firewalls oder auch sogenannte Datendioden eingesetzt werden – Letztere übertragen Daten nur in einer Richtung. Die Konzeption des Netzwerks und seiner Sicherheitsmechanismen liegt im Aufgabenbereich des Integrators. Sein Know-how wird zum entscheidenden Faktor für die Absicherung der Anlage. Neben der reinen Vernetzung findet heute mit der Nutzung von Cloud-Diensten sogar eine Speicherung empfindlicher Daten außerhalb des eigenen Netzwerks statt.

Mit der integrierten Nutzung von Cloud-Diensten steigt die Notwendigkeit der Verfügbarkeit solcher Dienste zunehmend an. Bei allen Vorteilen von Cloud-basierten Lösungen geht damit jedoch auch ein Verlust der eigenen Datenhoheit einher. Mit dieser Herausforderung umzugehen, wird in solchen Fällen ebenfalls zur Aufgabe des Integrators.

Zum Kontext von „Industrie 4.0“ zählt in einem weiteren Evolutionsschritt die Vision, auch Sensoren und Aktoren direkt mit der Cloud kommunizieren zu lassen. Auf dieser Basis werden ganz neue Anwendungen möglich – zum Beispiel der Digitale Zwilling einer Industrieanlage, der ihren gesamten Prozessablauf für Analysen und Optimierungen in einer Cloud simuliert.

Die damit einhergehende Steigerung der Komplexität in der Kommunikation zwischen physischer Anlage und Cloud potenziert jedoch auch die Herausforderung, diese Architektur abzusichern. Auch dafür bietet die Norm IEC 62443 klar definierte Vorgehensweisen.

## IEC 62443-2-1, SP 03.02

The service provider shall have the capability to ensure that the physical network segmentation architecture used in the Automation Solution, including its use of network security devices or equivalent mechanisms, is implemented according to the Automation Solution design approved by the asset owner.

Vernetzte Maschinen und Industrieanlagen ermöglichen heute zum Teil vollständig automatisierte Produktion. Doch Sicherheit darf bei ihrer Konzeption nicht vergessen werden.

Empfehlenswert ist es, Sicherheitskonzepte wie die Bildung von Zonen oder den Einsatz von Datendioden bereits bei der Planung der Architektur mit zu berücksichtigen.

# Mehr Schutz für Industriekomponenten

**Komponentenhersteller sehen sich mit zum Teil widersprüchlichen Anforderungen konfrontiert. Um etwa Echtzeitprotokolle ohne ausreichendes Sicherheitsniveau zu schützen, können Vorkehrungen bei der Architektur helfen.**

Vernetzte Automatisierungskomponenten bestehen häufig aus mehreren Teilen. Spezialisierte Sensoren können zwar unter Umständen während des Betriebs eigenständig arbeiten, oft benötigen sie aber auch zusätzliche Industrie-PCs zur Steuerung. Auch für ihre Parametrierung oder Konfiguration sind häufig spezielle Windows-Anwendungen notwendig, die über ein Netzwerk mit der Anlagenkomponente interagieren müssen. Für diese Kommunikation werden in der Regel Standardprotokolle eingesetzt, die oft keine ausreichenden Sicherheitseigenschaften aufweisen.

### Protokolle ohne Absicherung begünstigen Manipulationen

Diese in der industriellen Praxis häufig anzutreffende schwache Absicherung des Kommunikationskanals zwischen Steuerung und Komponenten begünstigt Angriffe – etwa den Diebstahl von Anmeldedaten. Gelingt das Aussponieren dieser Daten, ergibt sich daraus die Gefahr, dass sich ein Angreifer zum Beispiel an der Konfigurationsschnittstelle eines Sensors anmeldet und die Konfiguration manipuliert, wodurch dann andere Messwerte erzeugt werden. Je nach Relevanz der betroffenenen Komponente für die Automatisierung kann daraus schnell eine Gefährdung für die gesamte Anlage entstehen. Die Lösung für dieses Problem ist der Einsatz von Mechanismen zur Absicherung der Kommunikation, also der Einsatz von sicheren Kommunikationsprotokollen für die Vernetzung von Komponenten mit ihren Steuersystemen oder anderen Bestandteilen der Anlage.

Im Idealfall berücksichtigt bereits der Entwicklungsprozess die notwendigen Anforderungen an die Sicherheit. Um dieses Vorgehen umfassend zu unterstützen, beschreibt die Norm IEC 62443 einen sicheren Entwicklungsprozess. Die dafür relevanten Normteile enthalten die Anforderung, dass Entwickler sich Gedanken über Angreifermodelle und Bedrohungen machen müssen und dass das zu erreichende Sicherheitsniveau als Teil des Entwicklungsprozesses definiert werden muss. Da sicherheitstechnische Aspekte somit in der gesamten Entwicklung strukturell berücksichtigt werden, führt dies zu Produkten beziehungsweise Lösungen mit weniger Schwachstellen. Komponentenhersteller sollten sich und ihre Entwicklungsabteilungen deshalb mit den Vorschriften und Vorgehensmodellen unbedingt vertraut machen.


*Die zur Steuerung eingesetzten Echtzeitprotokolle beinhalten in der Regel keine ausreichenden Sicherheitseigenschaften. Diesem Schwachpunkt müssen konzeptionelle Maßnahmen wie Zonen und kontrollierte Informationsflüsse entgegenwirken.*

# Szenario 3: Komponentenhersteller

Durch eine Prüfstelle für IT-Sicherheit kann eine unabhängige und effektive Prüfung der Einhaltung von technischen Sicherheitsanforderungen sowie eine Schwachstellenprüfung erfolgen. Von der Entwicklung unabhängige Prüfungen führen zu einem hohen Sicherheitsniveau. Zudem erhöht dieses Vorgehen die Wahrscheinlichkeit, unbeabsichtigte Fehler tatsächlich zu entdecken.

**Echtzeitprotokolle durch Zonen und Conduits schützen**
Eine weitere Schwierigkeit im Bereich industrieller Kommunikation besteht darin, dass neben der Notwendigkeit zur Konfiguration von Komponenten häufig auch die eigentliche Prozesssteuerung über Kommunikationskanäle stattfindet – und dies in der Regel mit echtzeitfähigen Protokollen. Diese Protokolle wurden jedoch nie nach Cybersicherheitsaspekten entwickelt. Bei solchen Netzwerken ist es daher besonders wichtig, das zentrale Konzept der Zones and Conduits der IEC 62443 zu nutzen. Das bedeutet, dass verschiedene Kommunikationsbereiche (Zonen) definiert werden und nur kontrollierte Informationsflüsse (Conduits) zwischen diesen Zonen zugelassen werden. Diese wichtige Maßnahme ist ein gutes Mittel, um trotz der technischen Beschränkungen aktueller Anlagenarchitekturen eine wirksame Verbesserung des Sicherheitsniveaus zu erzielen.

Die Steuerung von Aktoren und Sensoren ist oft zeitkritsch und setzt deshalb auf Echtzeitprotokolle ohne Sicherheitseigenschaften. Gerade hochspezialisierte Sensoren werden dabei häufig durch spezielle Industrie-PCs gesteuert, überwacht oder parametrisiert.

## IEC 62443-4-2, CR 4.1

**Normteil IEC 62443-4-2 CR 4.1 – Information confidentiality**
Provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 [11] SR 4.1.

## IEC 62443-3-2, ZCR 3.1

**Normteil IEC 62443-3-2 ZCR-3.1: Establish zones and conduits**
The organization shall establish zones and conduits by grouping IACS and related assets. Grouping shall be based upon the results of the high-level cybersecurity risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

# Die Norm IEC 62443

**Haftungsrisiken senken, Verbraucher und Arbeitnehmer schützen**
Eine Zertifizierung nach IEC 62443 analysiert und bewertet die Sicherheitskonzepte und -maßnahmen. Sie belegt, dass das zertifizierte Unternehmen nach „Stand der Technik“ arbeitet und seine gesetzlichen Sorgfaltspflichten erfüllt – wichtige Voraussetzungen, um Haftungsrisiken zu minimieren. Zusätzlich können so Komponenten gemäß Produktsicherheitsgesetz (ProdSichG) sicher in Verkehr gebracht werden. Und nicht zuletzt schützen Betriebe auf diese Weise ihre Arbeitnehmerinnen und Arbeitnehmer gemäß Betriebssicherheitsverordnung.

Die Norm IEC 62443 verfolgt einen ganzheitlichen Ansatz. Das bedeutet, dass Technik und Prozesse bei der Erstellung von Industrial-Security-Konzepten gleichermaßen betrachtet werden. Diese Konzepte behandelt die Norm in etwas mehr als zehn Teilen, welche inhaltlich ineinandergreifen. Die Normteile sind in vier thematisch sortierte Ebenen eingeteilt:

## General

Diese Ebene sammelt Normteile, welche die zentralen Konzepte erläutern und Begriffe definieren.

## Policies & Procedures

Diese Ebene enthält die Vorgehensweisen für Betreiber und Dienstleister (Integratoren).

**IEC 62443-2-1:** Dieser Teil beschreibt die Vorgehensweise für einen Betreiber und den Betrieb seines Sicherheitsmanagements.

**IEC 62443-2-4:** Dieser Teil definiert Anforderungen an Dienstleister, welche Industrial-Security-Kompetenz sie benötigen und wie diese erfasst werden kann.

## System

Diese Ebene enthält Vorgaben für Anlagen, insbesondere für deren Planungsphase.

**IEC 62443-3-2:** Dieser Teil beschreibt ein iteratives Vorgehen zur Durchführung einer Risikoanalyse im Rahmen einer Anlagenplanung oder Modernisierung.

**IEC 62443-3-3:** Dieser Teil enthält einen Katalog von sicherheitstechnischen Anforderungen an eine Anlage. Diese Maßnahmen dienen unter anderem dazu, den identifizierten Risiken aus einer vorangegangenen Risikoanalyse zu begegnen.

## Component

Diese Ebene enthält Anforderungen an die Hersteller von Industriekomponenten.

**IEC 62443-4-1:** Dieser Teil enthält Anforderungen an umzusetzende Prozeduren für die Entwicklungsprozesse von Herstellern.

**IEC 62443-4-2:** Dieser Teil enthält sicherheitstechnische Anforderungen an Komponenten und ist damit das Pendant zum Teil IEC 62443-3-3.

# Nutzung der Norm: top-down

Die Norm verfolgt den Ansatz, dass ein Betreiber (Asset Owner) ein für sich zu bestimmendes Sicherheitsniveau seiner Anlage (System) erreichen möchte **(IEC 62443-2-1)**. Sowohl für die Planung als auch für den laufenden Betrieb einer Anlage werden externe Dienstleister benötigt, die allerdings ebenfalls zur Sicherheit der Anlage beitragen müssen **(IEC 62443-2-4)**.

Im Rahmen einer Anlagenkonzeption oder Modernisierung kann über den Ansatz einer Risikoanalyse festgestellt werden, welche technischen Sicherheitsmaßnahmen in der Anlage benötigt werden **(IEC 62443-3-2)**. Diese werden als Anforderungen (System Requirements) definiert **(IEC 62443-3-3)**.

In einem weiteren Planungsschritt werden sie dann zu detaillierten Anforderungen an Komponenten (Component Requirements) heruntergebrochen, welche wiederum von Herstellern der Komponenten implementiert werden müssen **(IEC 62443-4-2)**. Um ein durchgängig und dauerhaft hohes Sicherheitsniveau bei den Komponenten zu erreichen, werden konkrete Anforderungen an ihren Entwicklungsprozess gestellt **(IEC 62443-4-1)**.

*IEC 62443-2-1*

## Betreiber

... möchte eine sichere Anlage nach **IEC 62443-2-1** betreiben und beauftragt den ...

*IEC 62443-2-1*

## Integrator

..., der mithilfe einer Risikoanalyse **(IEC 62443-3-2)** eine Anlage konzipiert und Anforderungen an diese ableitet **(IEC 62443-3-3)**. Die Umsetzung erfolgt durch ...

*IEC 62443-2-1*

## Hersteller

..., welche die Erfüllung der Anforderungen der Komponenten nachweisen **(IEC 62443-4-2)**. Die Entwicklung der Komponenten erfolgt nach einem Entwicklungsprozess unter Beachtung von Sicherheitsaspekten **(IEC 62443-4-1)**.

# Security4Safety als Business Assurance für Industrie 4.0

Der zuverlässige und dauerhaft sichere Betrieb von weltweit vernetzten Maschinen, Anlagen und Produkten ist eine elementare Herausforderung für eine erfolgreiche Umsetzung von Industrie 4.0. Doch wenn Maschinen, Komponenten unterschiedlichster Art oder Fahrzeuge automatisch Informationen austauschen, muss eine unbefugte Beeinflussung (Cyberattacken) von außen vermieden werden. Die zunehmende Automatisierung und Digitalisierung erzeugt neue Kundenanforderungen und Produktanforderungsprofile, welche die klassischen Geschäftsfelder derzeit revolutionieren. Hersteller sind daher gefordert, erweiterte Sicherheitsstandards, die den Aspekt der IT-Security betrachten, in den Entwicklungs- und Herstellungsprozess ihrer Produkte zu integrieren.

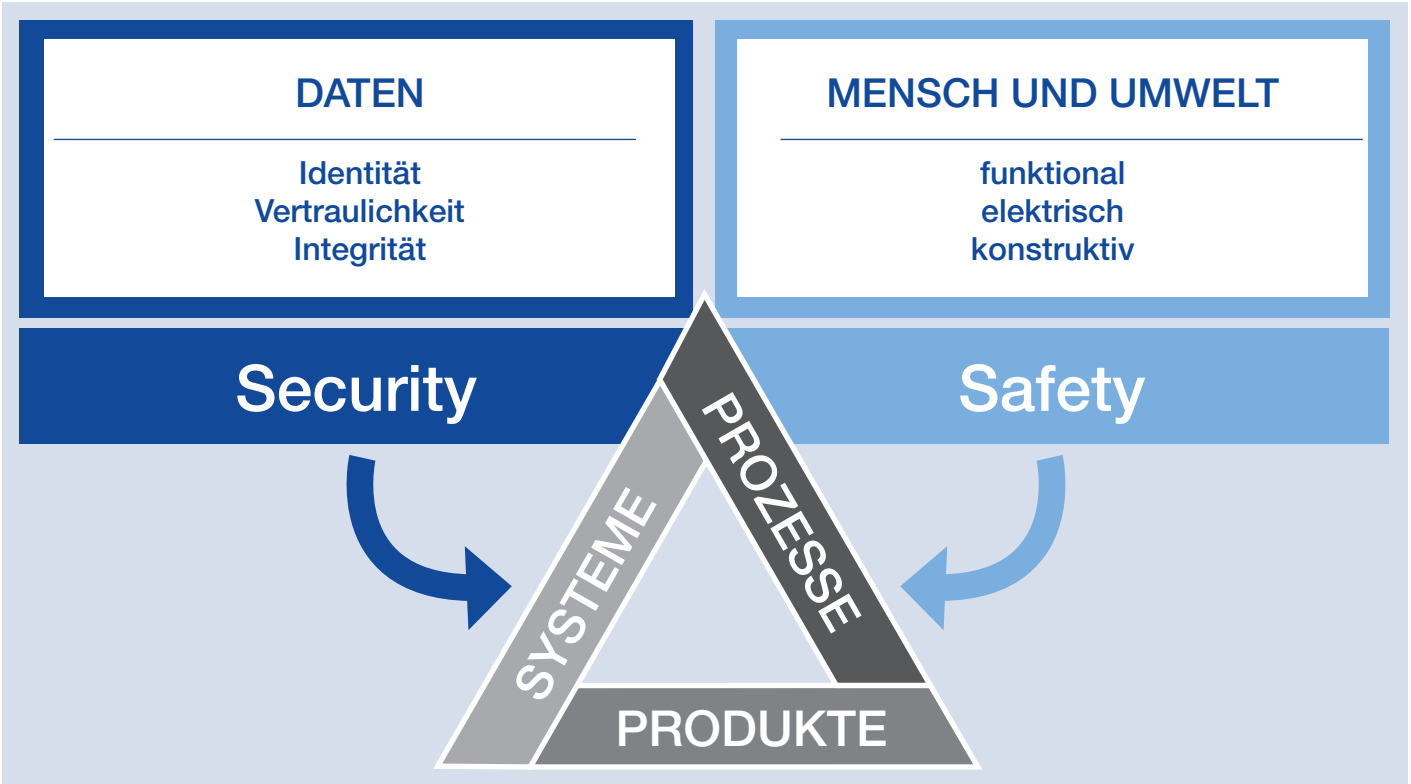
Industrie- und IT-Sicherheit sind in der heutigen Zeit untrennbar miteinander verwoben. Maschinen der industriellen Fertigung müssen nicht mehr nur für Mensch und Umwelt sicher sein, sondern auch vor Cyberangriffen und Manipulationen von außen geschützt werden.

Unter dem Schlagwort Security4Safety verbindet TÜV NORD klassisches Wissen im Bereich der Produkt-, Betriebs- und Anlagensicherheit mit den neuen, digitalen Anforderungen der IT-Sicherheit. Im Zuge dieser Verschmelzung treffen zwei unterschiedliche Sicherheitsbegriffe aufeinander, die es miteinander in Einklang zu bringen gilt: Security im Sinne einer Kriminalprävention und Safety im Sinne einer Unfallvermeidung. Diese rücken jeweils unterschiedliche Aspekte in den Fokus. Mit unseren kombinierten Security- und Safety-Dienstleistungen decken Unternehmen beide Sicherheitsbegriffe umfassend ab. Die Zertifizierung zur Normenreihe IEC 62443 ist eines der zentralen Angebote im Bereich Security4Safety, in dem TÜV NORD Leistungen bündelt, die klassische Produkt- und Betriebssicherheit (Safety) mit IT-Sicherheit (Security) verzahnen. Die Zertifizierung ergänzt Audits zur Informationssicherheit und zum Datenschutz in den entsprechenden Qualitätsmanagement-Systemen sowie Prüfungen der Funktionalen Sicherheit.

TÜV NORD profiliert sich seit vielen Jahren als international anerkannter und zuverlässiger Partner für Prüf- und Zertifizierungsdienstleistungen. Unser S4S-Projektteam ist aktiv im Gremium zur Normung der IEC 62443 vertreten und direkt in die Gestaltung der Norm eingebunden. Dieses wichtige und aktuelle Insiderwissen fließt somit in die positive Fortentwicklung Ihres Unternehmens ein. Unsere Auditoren und Experten unterstützen Sie in allen Phasen von der Entwicklung bis zur Vermarktung Ihrer Produkte und geben Ihnen parallel ein objektives Feedback. Für die Normenreihe IEC 62443 sind wir einer der ersten Anbieter im Markt, der eine DAkkS-akkreditierte Zertifizierung gemäß IEC 62443 anbietet.

Eine Prüfung verspricht sowohl für die Entwicklung und Produktion als auch für das Marketing entscheidende Wettbewerbsvorteile:

- erhöhter Schutz vor Haftungsrisiken
- konsistente Reduktion von Risiken
- Bewertung von Safety und Security gemäß dem aktuellen Stand der Technik
- dokumentierte Risikobeurteilung zum Nachweis der Sorgfaltspflicht
- Wettbewerbsvorteil durch anerkannten Sicherheitsnachweis
- effektive und lösungsorientierte Projektbegleitung
- Know-how rund um Prozesse und Methoden



## TÜV NORD CERT – auf unser Know-how ist Verlass

*„Auf der ganzen Welt steht der Name TÜV® für Sicherheit und Qualität – und das seit mehr als 150 Jahren.*

*Im deutschsprachigen Raum hat die Marke einen Bekanntheitsgrad von 99 Prozent und ist ein Synonym für Verlässlichkeit: Verbraucher vertrauen einem Unternehmen, einem Produkt oder einer Dienstleistung deutlich mehr, wenn ein TÜV®-Prüfzeichen vorliegt.“*

### Führende Kompetenz rund um Technologie

TÜV NORD CERT ist die Zertifizierungsgesellschaft der TÜV NORD GROUP und steht weltweit mit einem Team aus mehr als 1.300 erfahrenen Experten für höchste Kompetenz. Wir beschäftigen ausgewiesene Fachleute aus unterschiedlichsten Branchen; als attraktiver Arbeitgeber bieten wir unseren Mitarbeitern optimale Entwicklungsmöglichkeiten und sorgen dafür, dass unser Team jederzeit auf dem neuesten Stand ist. Unser Dienstleistungsportfolio erweitern wir ständig – beispielsweise durch Ausbau und Weiterentwicklung unserer Labore oder durch Kooperationen mit namhaften Forschungsinstituten. Know-how, Erfahrung und konsequente Serviceorientierung: Dies sind die Grundlagen für exzellente Dienstleistungen, von denen unsere Kunden in vielfacher Weise profitieren.

Weitere Informationen zu Security4Safety finden Sie unter:
**www.security4safety.de**

**TÜV NORD CERT GmbH**
Langemarckstraße 20
45141 Essen
Tel.: 0800 245-7457 (kostenlose Service-Hotline)
Fax: 0511 9986 69 1900
info.tncert@tuev-nord.de
**www.tuev-nord-cert.de**

TÜV NORD
Zertifizierung

24-0473-11/18