STORMSHIELD

Optimieren Sie den Schutz Ihres Betriebssystems

Alles Wissenswerte über die Norm IEC 62443

Inhalt

Zusammenfassung

Die Architektur von industriellen Automatisierungs- und Steuerungssystemen (Industrial Automation and Control Systems, IACS) wird immer komplexer. Zudem ist sie weitgehend mit externen Systemen vernetzt, was die Gefahr der Ausnutzung von Schwachstellen erhöht. Deshalb hat sich die Welt der Operational Technology (oder OT) zu einem bevorzugten Ziel für Cyberkriminelle entwickelt.

Die Folgen eines Cyberangriffs auf IACS können verheerend sein: Sie reichen von Produktionsschäden über Wirtschafts- und Finanzverluste bis hin zu Umweltschäden oder sogar dem Verlust von Menschenleben.

Aus diesen Gründen ist es wichtig, einen strikten und zuverlässigen Plan für das Risikomanagement zu erstellen, um operative und Industriesysteme erfolgreich zu schützen. Vor diesem Hintergrund **stellt die Norm IEC 62443 einen umfassenden Rahmen für das Risikomanagement auf, das mit der Einführung der industriellen Cybersicherheit in solche Systeme verbunden ist.**

Dieser Ansatz beinhaltet *de facto* eine umfassende Identifizierung der Assets sowie eine detaillierte Analyse der verschiedenen Bedrohungen und Schwachstellen, die IACS möglicherweise aufweisen. Dieser Standard leitet Industrieunternehmen bei der Umsetzung von Sicherheitsmaßnahmen in einer Weise an, die mit jedem industriellen und operativen System kompatibel ist.

Dieses Whitepaper erläutert die Norm IEC 62443 und **die erforderlichen Schritte, um eine Cyber-Governance einzuführen, die mit den betrieblichen Anforderungen im Einklang steht**. Es zeigt insbesondere die Bedeutung der IEC-62443-Zertifizierung im Hinblick auf die Auswahl der zur Einhaltung der Vorschriften eingesetzten Lösungen auf. Diese Zertifizierung garantiert in bestimmten Fällen, dass Sie den jeweiligen Lösungen vertrauen und die Infrastruktur von industriellen Automatisierungs- und Steuerungssystemen absichern können.

Zusammengefasst bietet dieses Whitepaper einen detaillierten Einblick in die Norm IEC 62443, damit Unternehmen die Herausforderungen besser verstehen und sie in einem definierten operativen Rahmen, d. h. bei der Umsetzung einer globalen Sicherheitspolitik, die sensible Assets in verschiedenen industriellen Automatisierungssystemen schützt, anwenden können.

Darüber hinaus gibt dieses Dokument Denkanstöße, wie sich diese Norm nach dem aktuellen Stand der Technik in Bezug auf industrielle Cybersicherheit integrieren lässt.

ÜBER dieses E-Book

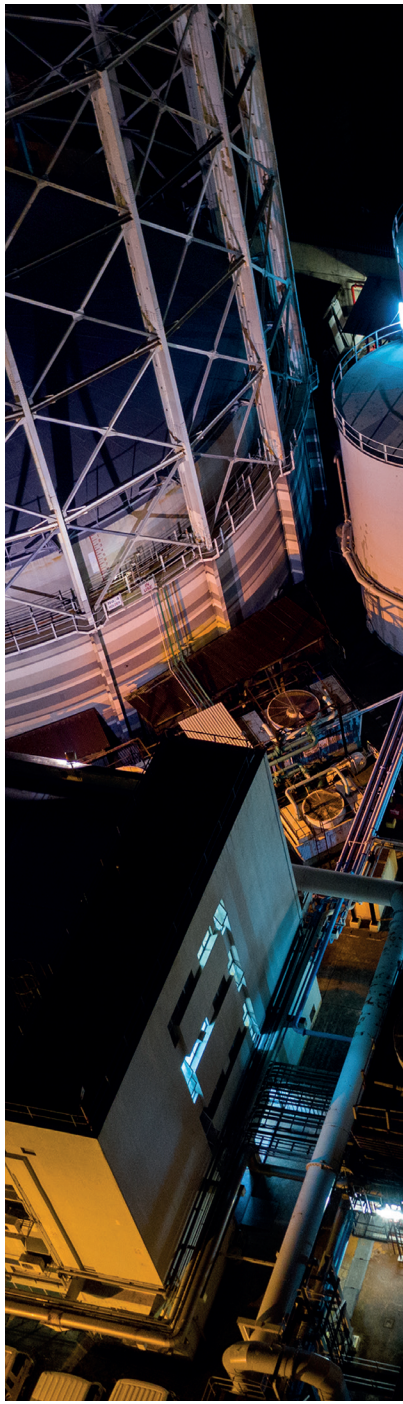
Dieses Whitepaper richtet sich an Betriebsleiter, Wartungsleiter, Fach- und Betriebsleiter, die für kritische Infrastrukturen zuständig sind, sowie an Verantwortliche für die Sicherheit von Informationssystemen.

26,8 %

der Computer innerhalb eines industriellen Kontrollsystems (ICS) waren bereits Cyber-Angriffsversuchen ausgesetzt.[1]

70 %

der Industrieunternehmen wurden im Jahr 2023 Opfer eines Cyberangriffs.[2]



1 : https://rendre-notre-monde-plus-sur.goron.fr/pourquoi-le-secteur-industriel-est-il-devenu-une-cible-privilegiee-des-cyberattaques/

2 : https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/pres-de-70-des-organisations-industrielles-ont-ete-victimes-dune-cyberattaque-en-2023/

70 %

potenzieller Anstieg von Cyberangriffen auf die Produktionsinfrastruktur gemäß mehreren Experten.[1]

3,8 Mio. €

durchschnittliche Kosten einer Computerpanne für ein Industrieunternehmen.[2]

1 : https://www.linkedin.com/pulse/cybers%C3%A9curit%C3%A9-industrielle-les-attaques-en-hausse-holiseum-qcsme/

2 : https://www.imsnetworks.com/ressources-et-actual/cout-cyberattaques-industrie/

Die vor vielen Jahren eingeläutete Ära der „Industrie der Zukunft“ hat das Umfeld für industrielle Automatisierungs- und Steuerungssysteme komplexer gemacht. Die Verknüpfung zwischen dem Industrienetzwerk und der traditionellen IT-Infrastruktur für die Verwaltung oder die Anbindung an externe Partner vergrößert die Angriffsfläche und erhöht damit auch die potenziell ausnutzbaren Sicherheitslücken.

Cyberbedrohungen und Herausforderungen für Industrieunternehmen

Die steigende Zahl von Angriffen auf Industriesysteme verdeutlicht, wie diese Schwachstellen ausgenutzt werden. So waren im Jahr 2023 fast 70 Prozent der Industrieunternehmen Opfer eines Cyberangriffs.[1] Im gleichen Jahr beliefen sich die Kosten für Datenlecks in allen Industriesystemen im Gesundheitswesen, in der Energiebranche sowie in der Pharma- und Fertigungsindustrie auf insgesamt über 25 Millionen[2] US-Dollar.

Die mit diesen Cyberangriffen verbundenen Risiken gehen weit über finanzielle Aspekte hinaus. Tatsächlich **kann die Interaktion zwischen Prozessen und der Hardware industrieller Automatisierungs- und Kontrollsysteme zu Industrieunfällen führen,** bei denen z. B. der Verlust von Menschenleben oder Umweltschäden weitaus schwerwiegendere Folgen darstellen.

Datenlecks

25

Mio. Dollar

Weltweite Kosten im Jahr 2023

1 : https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/pres-de-70-des-organisations-industrielles-ont-ete-victimes-dune-cyberattaque-en-2023/

2 : https://www.ibm.com/resources/downloads/cost-data-breach-report

Einführung eines Risiko-managements-systems

Die Ausführung eines Risikomanagementplans basiert auf einer Bedrohungs- und Risikobewertung, die darauf abzielt, Gegenmaßnahmen einzuleiten, um vorhandene Schwachstellen zu beheben und so die Cybersicherheit des gesamten Industriesystems zu erhöhen. Dieser Plan muss Teil eines umfassenden Governance-Ansatzes sein, um eine regelmäßige Überwachung der eingeführten Maßnahmen und neuer, zukünftiger Risiken zu gewährleisten.

Das in der Norm IEC 62443 beschriebene Prinzip beruht auf der **Identifizierung und Inventarisierung von Assets**, die als Daten im Zusammenhang mit geistigem Eigentum, Menschen, Servern oder auch Komponenten oder Prozessen des Industriesystems vorliegen können. Im Rahmen des Risikobewertungsprozesses wird die Wahrscheinlichkeit ermittelt, mit der eine Cyberbedrohung eine bestimmte Schwachstelle ausnutzt und Folgen für die identifizierten Assets verursacht.

Schließlich setzt die Organisation ausgehend von diesem Anfangsrisiko betriebliche, technische und administrative Maßnahmen ein, um die ermittelten Risiken zu verringern oder zu vermeiden (und etwaige Restrisiken zu akzeptieren). An dieser Stelle ist es wichtig zu beachten, dass die eingesetzten Mittel den Risiken angemessen sein müssen. **Das Ziel ist nicht, alle Risiken zu vermeiden, sondern vielmehr ein Maß an Restrisiken zu erreichen, das für das Unternehmen im Hinblick auf die eingesetzten Mittel und Herausforderungen akzeptabel ist**.

Die Norm IEC 62443 stützt sich auf die Einführung einer unternehmensweiten Sicherheitspolitik, die darauf abzielt, die sensiblen Assets eines industriellen Automatisierungs- und Kontrollsystems zu schützen. Dieser Ansatz vereinfacht die Betrachtung des gesamten Industriesystems, einschließlich der Anbindungen an externe Systeme, wie z. B. ein Office Support System.

Verbesserter Schutz des Betriebssystems

Die Umsetzung der auf der Bedrohungs- und Risikobewertung basierenden Sicherheitspolitik besteht darin, organisatorische und technische Cybermaßnahmen einzusetzen. Die in der Norm aufgelisteten technischen Sicherheitsmaßnahmen reichen jedoch nicht aus, auch wenn sie vollständig auf industrielle Automatisierungs- und Kontrollsysteme abzielen.

Eine technische Sicherheitsmaßnahme wird nämlich in Abhängigkeit vom Risiko und den betrieblichen Einschränkungen betrachtet: Diese Einschränkungen sind besonders wichtig, wenn die Governance von dem Team getragen wird, das für die Sicherheit des IT-Systems des Unternehmens zuständig ist. IT- und Fertigungs- bzw. Produktionsteams müssen zusammenarbeiten und ihre Kenntnisse sowie ihre Fähigkeiten vereinen, um die zu implementierenden Sicherheitsmaßnahmen festzulegen.

Letztlich **sollen die Einführung von Sicherheitsmaßnahmen sowie deren regelmäßige Überwachung und Optimierung im Einklang mit den Anforderungen an industrielle Automatisierungs- und Steuerungssysteme den Schutz des Betriebssystems verbessern.**

Governance

IT- und Fertigungs- oder Produktion-steams müssen zusammen-arbeiten.

AUFBAU DER NORM

ALLGEMEIN	**IEC-62443-1-1** Terminologie, Konzept und Modelle	**IEC-62443-1-2** Glossar der wichtigsten Begriffe und Abkürzungen	**IEC-62443-1-3** Maßnahmen für die Konformität des Sicherheitssystems	**IEC-62443-1-4** Lebenszyklus und Anwendungsfälle von IACS-Sicherheit
RICHTLINEN & PROZESSE	**IEC-62443-2-1** Anforderungen an ein IACS-Sicherheitsmanagementsystem	**IEC-62443-2-2** Leitfaden zur Implementierung eines IACS-Sicherheitsmanagementsystems	**IEC-62443-2-3** Patch-Management in einer IACS-Umgebung	**IEC-62443-2-4** Installations- und Wartungsanforderungen für Anbieter von IACS-
SYSTEME	**IEC-62443-3-1** IACS-Sicherheitstechnologien	**IEC-62443-3-2** Sicherheitsniveaus für Zonen und Kanäle	**IEC-62443-3-3** Anforderungen an das Sicherheitssystem und das Sicherheitsniveau	
VON KOMPONENTEN	**IEC-62443-4-1** Anforderungen an die Produktentwicklung	**IEC-62443-4-2** Technische Sicherheitsanforderungen an IACS-Komponenten		

IEC-62443-1-x führt die wichtigsten Konzepte der Norm IEC 62443 ein. Dieser Abschnitt befasst sich insbesondere mit den Prinzipien rund um Governance und Risikomanagement.

IEC-62443-2-x beschreibt die Elemente, die für das Cybersicherheits-management in industriellen Automatisierungs- und Kontrollsystemen erforderlich sind. Hierzu zählen insbesondere Anleitungen, wie diese Elemente entwickelt werden können.

IEC-62443-3-x stellt die grundlegenden Konzepte für das Verständnis des Cyberrisikomanagements in industriellen Automatisierungs- und Kontrollsystemen dar.

IEC-62443-4-x erläutert bewährte Verfahren für die Produktentwicklung bezüglich industriellen Automatisierungs- und Steuerungssystemen, insbesondere den Lebenszyklus der Produktentwicklung und die zu implementierenden Sicherheitsfunktionen.

IEC 62443 ISO 27001

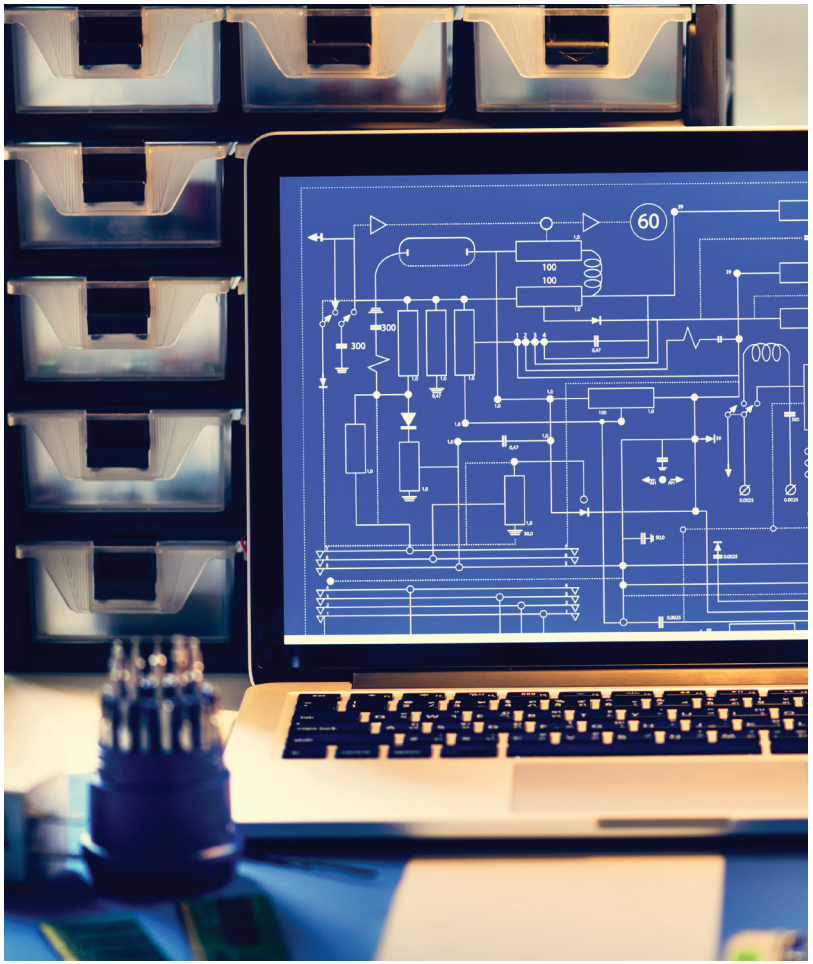
Auch wenn beide Standards das gleiche Ziel verfolgen, nämlich den Schutz eines Informationssystems, unterscheiden sie sich in den zu ergreifenden Maßnahmen sowie im Einsatzzweck des zu schützenden Systems und den Elementen, die zertifiziert werden können.

Um industrielle Automatisierungs- und Kontrollsysteme abzusichern, **definiert die Norm IEC 62443 die Politik, die Verfahren und die Mittel, die implementiert werden müssen**. Die Norm empfiehlt zwar, das Informationssystem als Ganzes in einem Sicherheitsprogramm zu berücksichtigen, sie zielt jedoch hauptsächlich auf operative Systeme ab. Im Übrigen fördert sie ihre Verbreitung, indem sie die Zertifizierung von Produkten, Systemen, Entwicklungsprozessen oder des Unternehmens anbietet.

Die Norm ISO27001 beschreibt ein Managementsystem und ermöglicht eine umfassendere Zertifizierung, indem sie die Verfahren präzisiert, die zur Festlegung und langfristigen Überwachung der Sicherheitspolitik des betrieblichen Informationssystems eingesetzt werden müssen.

Zusammenfassung

Die beiden Normen ergänzen sich gegenseitig – die bewährten Verfahren für ein Informationssicherheits-management-system gemäß ISO 27001 können auf die Maßnahmen und Verfahren angewendet werden, die im Rahmen der Einhaltung der Norm IEC 62443 eingesetzt werden.



IEC 62443

Defense in Depth (DiD)

Es ist in der Regel nicht möglich, die Sicherheitsziele durch den Einsatz einer einzigen Gegenmaßnahme oder Technik zu erreichen. Der Ansatz **von Defense in Depth (DiD) besteht darin, mehrere Schutzmittel oder Gegenmaßnahmen als Kaskade einzusetzen**. Das folgende Beispiel zeigt verschiedene Mittel, die auf mehreren Ebenen eingesetzt werden, von der Unternehmensführung über die Datensicherheit bis hin zur Peripherie oder auch der Hardware des Industriesystems.

ICS-spezifische Richtlinien, Standards, Verfahren, Bewusstsein	• PSS • Standards • Verfahren	• Schulungen • PCA (Plan für Geschäftskontinuität) • PRA (Plan zur Wiederaufnahme des Betriebs)
Physische Sicherheit	• Überwachung • Zugriffskontrolle	
Sicherheitsperimeter	• Firewalls • DMZ • VPN • IDS/IPS	
Netzwerksicherheit	• Zonen und Kanäle • Netzwerksegmentierung • Interne DMZ	• Firewalls vor Ort
Hardwaresicherheit	• Patchmanagement • Härtung für Workstations • Anschlusskontrolle	• Zugriffskontrolle • Kontinuierliches Monitoring • Audit
Anwendungssicherheit	• Zugriffskontrolle • Authentifizierung • Passwortverwaltung	• Updatemanagement
Datensicherheit	• Sichere Kommunikation (Verschlüsselung) • Authentifizierung • Endgeräteschutz	

Sicherheits-zonen

In großen oder komplexen Infrastrukturen weisen nicht unbedingt alle Komponenten das gleiche Sicherheitsniveau auf. Stattdessen sollten Zonen eingeteilt werden, in denen Geräte mit dem gleichen Sicherheitsniveau zusammengefasst werden.

Eine Sicherheitszone ist folglich eine logische Gruppierung von Assets mit den gleichen Sicherheitsanforderungen. Zonen können hierarchisch gegliedert werden, um Zonen innerhalb von Zonen – oder Unterzonen – einzurichten und einen mehrstufigen Schutz zu gewährleisten. Dieses Konzept ist übrigens eine der Säulen der Defense in Depth (DiD).

Eine Sicherheitszone hat eine Grenze, die die Festlegung der Kommunikation und des Zugangs erfordert, die erforderlich sind, damit sich Informationen und Personen innerhalb von und zwischen Sicherheitszonen bewegen können.

Die Festlegung einer Sicherheitszone **basiert auf der Bewertung der Sicherheitsanforderungen. Dazu wird bestimmt, ob ein bestimmter Asset innerhalb oder außerhalb der Zone berücksichtigt werden muss**. Diese Unterscheidung stützt sich auf die Art des Zugangs zum Asset, der entweder physisch oder über einen Kommunikationsweg erfolgen kann.

Sicherheitszonen

2 Definitions-möglichkeiten

1 Physisch

für Assets, die sich am gleichen Ort befinden.

2 Logisch oder virtuell

für Assets, welche die gleiche Funktion oder andere Eigenschaften aufweisen.

Kanäle (Conduits)

Mithilfe des Konzepts der „Conduits“ (Kanäle) können die Sicherheitsanforderungen für den Zugriff auf Assets mittels Kommunikation abgedeckt werden. Sie steuern die Verbindungen von Assets innerhalb einer Zone oder zwischen verschiedenen Zonen. Tatsächlich handelt es sich um eine **spezielle Art von Sicherheitszone, die als Kommunikationskanal bezeichnet wird**. Sie fasst die Kommunikation zusammen, die wiederum aus Informationsflüssen besteht.

Die Kanäle können daher physisch sein, wie ein Netzwerkkabel, oder logisch, wenn verschiedene Informationsflüsse das gleiche Sicherheitsniveau aufweisen.

Bei der Definition von Sicherheitsanforderungen zu berücksichtigende Fälle

Der Kanal überschreitet nicht die Grenzen der Zone: Der Kanal ist in der Regel durch die Kommunikationsprozesse innerhalb der Zone genehmigt.

Ein vertrauenswürdiger Kanal überschreitet die Grenzen der Zone: Der Kanal muss einen sicheren End-to-End-Prozess verwenden.

Sicherheits-niveaus

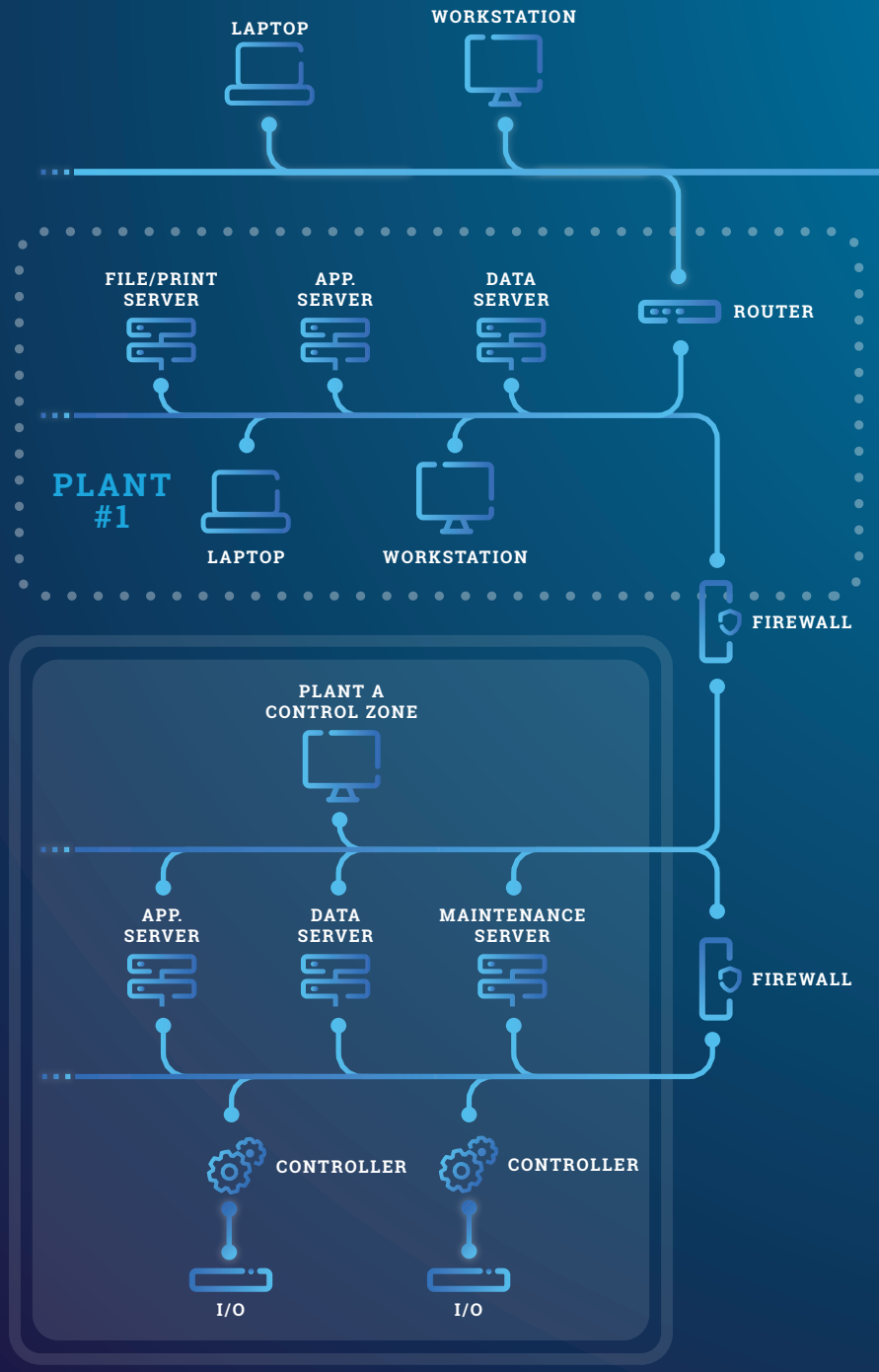
Die Einführung eines Risikomanagements stützt sich auf einen Prozess zur Bewertung der Bedrohungen für die Assets, die je nach dem erwarteten Sicherheitsniveau verschiedenen Zonen zugewiesen werden. Um den Einsatz von Gegenmaßnahmen oder auch von technischen und organisatorischen Mitteln zu erleichtern, schlagen die Sicherheitsziele der Norm IEC 62443 **verschiedene Sicherheitsniveaus vor, die einen qualitativen Ansatz ermöglichen,** um die erwartete Sicherheit pro Zone zu gewährleisten.

Die Sicherheitsniveaus werden anhand von Kriterien festgelegt, die für jede Art von Bedrohung spezifisch sind, wie z. B. die Fähigkeiten, Mittel oder Ressourcen, die für die Durchführung eines Angriffs erforderlich sind. Die folgende Tabelle beschreibt die vier erwarteten Sicherheitsniveaus entsprechend der möglicherweise auftretenden Bedrohungen.

Sicherheitsniveau	Ziele	Kompetenzen	Motivationen	Mittel	Ressourcen
1	Gelegentliche oder zufällige Verstöße	Keine Kompetenzen in Bezug auf Angriffe	Fehler	Unbeabsichtigte Handlungen	Auf eine Person beschränkt
2	Cyberkriminalität, Hacker	Allgemein	Gering	Einfach	Gering (Einzelperson)
3	Terroristischer Hacktivist	Spezifisch für industrielle Kontrollsysteme	Moderat	Ausgereift (Angriff)	Moderat (Hacker-Gruppe)
4	Nation/Staat	Spezifisch für industrielle Kontrollsysteme	Erhöht	Ausgereift (Kampagne)	Umfangreich (multidisziplinäres Team)

BEISPIEL FÜR DIE SEGMENTIERUNG NACH ZONEN UND KANÄLEN

Die nebenstehende Abbildung zeigt eine Organisation, die aus drei Werken und einem separaten Hauptsitz besteht. Alle drei Werke sind mit dem Unternehmensnetzwerk verbunden, um die Kommunikation mit dem Hauptsitz und den anderen Werken zu ermöglichen.

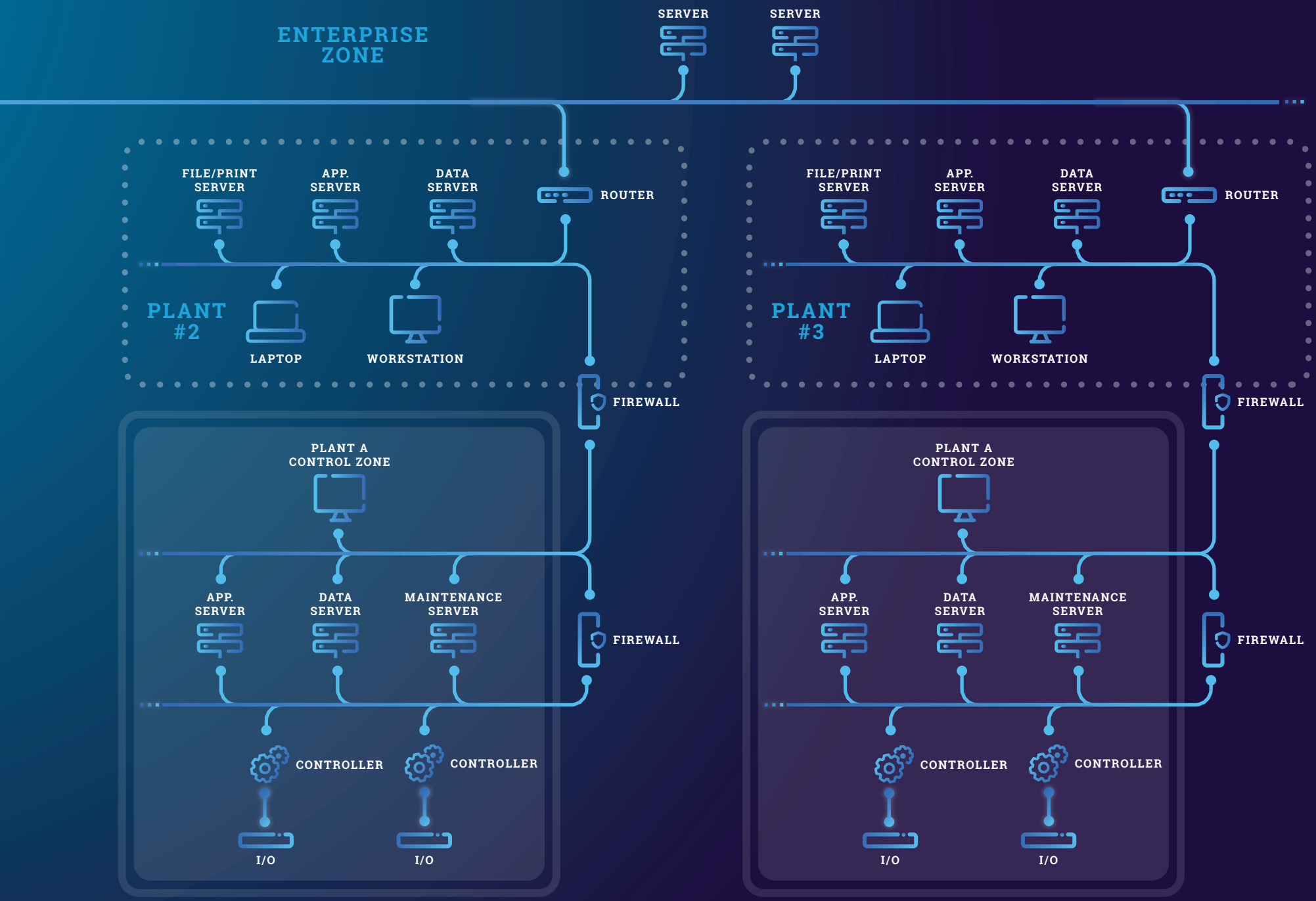


In der Zeichnung sind vier mögliche Kanäle definiert (es wären weitere vorhanden, diese werden aber zur Vereinfachung ausgeblendet).

Oben in der Abbildung ist der Unternehmenskanal dargestellt. Er verbindet mehrere Werke an verschiedenen Orten mit dem Datenzentrum des Unternehmens. Wenn das Wide Area Network (WAN) mithilfe von Miet- oder Privatkommunikation aufgebaut wird, kann dieser Kanal als vertrauenswürdig betrachtet werden.

Wenn er sowohl öffentliche als auch private Netzwerke nutzt, kann er als unzuverlässig eingestuft werden. Der Kanal umfasst alle Kommunikationsgeräte und Firewalls, die die Verbindungen im Werk bilden.

Instanzen der zweiten Klasse von Kanälen werden in jedem Werk angezeigt. Hier hat jedes Werk einen eigenen vertrauenswürdigen Kanal für die Steuerungskommunikation.


ENTERPRISE ZONE
SERVER
SERVER
FILE/PRINT SERVER
APP. SERVER
DATA SERVER
ROUTER
PLANT #2
LAPTOP
WORKSTATION
FIREWALL
PLANT A CONTROL ZONE
APP. SERVER
DATA SERVER
MAINTENANCE SERVER
FIREWALL
CONTROLLER
CONTROLLER
I/O
I/O
FILE/PRINT SERVER
APP. SERVER
DATA SERVER
ROUTER
PLANT #3
LAPTOP
WORKSTATION
FIREWALL
PLANT A CONTROL ZONE
APP. SERVER
DATA SERVER
MAINTENANCE SERVER
FIREWALL
CONTROLLER
CONTROLLER
I/O
I/O

7 Grundanforderungen

Die verschiedenen Sicherheitsmaßnahmen, die im Rahmen des von der Norm IEC 62443 vorgeschlagenen Risikomanagements umgesetzt werden müssen, sind in Familien gegliedert.

FR1

Identifizierungs- und Authentifizierungskontrolle

Identifizierung und Authentifizierung aller Benutzer (Personen, Softwareprozesse und Geräte), bevor diese Zugriff auf das System erhalten.

FR2

Nutzungskontrolle

Durchsetzung der Privilegien, die einem authentifizierten Benutzer (Personen, Softwareprozesse oder Geräte) zugewiesen wurden.

FR3

Systemintegrität

Sicherstellung der Integrität von Daten, Software und Hardware.

FR4

Datenschutz

Gewährleistung der Vertraulichkeit von Informationen in den Kommunikationsflüssen sowie in den Datenspeichern.

FR5

Einschränkung des Datenflusses

Segmentierung des Kontrollsystems durch Zonen und Kanäle, um unnötigen Datenfluss zu begrenzen.

FR6

Rechtzeitige Reaktion auf Ereignisse

Reaktion auf Angriffe, indem die zuständige Behörde benachrichtigt, die erforderlichen Beweise für den Verstoß gemeldet und bei Entdeckung von Vorfällen rechtzeitig Abhilfemaßnahmen ergriffen werden.

FR7

Ressourcenverfügbarkeit

Sicherstellen, dass das System gegen verschiedene Arten von DoS-Ereignissen resistent ist. Dazu zählt auch die teilweise oder vollständige Nichtverfügbarkeit von Systemfunktionen auf verschiedenen Ebenen.

Zertifizierungszweig gemäß IEC 62443-4

Der Zertifizierungszweig gemäß IEC 62443-4 bescheinigt, dass ein Produkt (Hardware, Komponente oder System) den Anforderungen entspricht, die in Teil 62443-4 der Norm aufgeführt sind. Dieser Teil der Norm betrifft folglich Produkte, die in industriellen Automatisierungs- und Steuerungssystemen eingesetzt und verwendet werden.

Man unterscheidet zwei Arten von Zertifizierungen:

IEC 62443-4-1 zielt auf den Entwicklungsprozess von Sicherheitsprodukten ab.

IEC 62443-4-2 bezieht sich auf die Erfüllung der 7 Grundanforderungen, die in Teil IEC 62443-1-1 der Norm beschrieben sind.

Besonderheiten der Norm IEC 62443-4-1

Dieser Teil der Norm legt die Anforderungen für die Gewährleistung eines sicheren Entwicklungslebenszyklus fest. Das Hauptziel dieser Anforderungen besteht darin, **einen Rahmen für einen tiefgreifenden Sicherheits- und Verteidigungsansatz** bei der Planung, dem Aufbau, der Wartung und der Außerbetriebnahme von Produkten zu schaffen, die in industriellen Automatisierungs- und Steuerungssystemen eingesetzt werden.

Die Zertifizierung gemäß IEC 62443-4-1 deckt die folgenden Hauptaspekte ab:

Sicherer Entwicklungs-prozess
zur Einrichtung und Pflege des Programms für die sichere Entwicklung während des gesamten Lebenszyklus der Produktentwicklung.

Risikomanagement
zur Bereitstellung von Richtlinien für die Identifizierung und Bewertung sowie das Management von Sicherheitsrisiken, die mit Produkten und Systemen verbunden sind.

Einhaltung von bewährten Verfahren
zur Förderung der Einführung bewährter Verfahren für das Sicherheitsmanagement von Software und Hardware, die in industriellen Systemen eingesetzt werden.

Konzeptionelle Sicherheit
zur Hervorhebung der Integration der Sicherheit während aller Phasen der Produktrealisierung, von der Entwurfsphase bis hin zu den Test- und Wartungsphasen.

Dokumentation und Rückver-folgbarkeit
zur Festlegung des Anforderungsniveaus für eine angemessene Dokumentation und Nachvollziehbarkeit der Entwicklungsprozesse sowie der ergriffenen Sicherheitsmaßnahmen.

ERWARTETER NUTZEN

Benutzer von zertifizierten Produkten können darauf vertrauen, dass sie ein Produkt erhalten, das mit einem optimalen Sicherheitsniveau entwickelt, hergestellt und gewartet wird. Diese Zertifizierung deckt alle Prozesse der Softwareentwicklung in acht großen Themenbereichen ab:

1

das Sicherheitsmanagement, das unter anderem den Entwicklungsprozess, die Zuständigkeiten oder die Verwaltung privater Schlüssel umfasst

2

die Definition des Sicherheitsbedarfs, mit einem Bedrohungsmodell und einer Risikoanalyse

3

Security By Design, das die Prinzipien der sicheren Architektur und des sicheren Designs bedeutet

4

die Sicherheit der Implementierung mittels guter Programmierpraktiken

5

die Tests und Verifizierung, die sicherstellen soll, dass die Implementierung ordnungsgemäß erfolgt, indem Penetrationstests sowie Tests auf Schwachstellen durchgeführt werden

6

die Verwaltung von Sicherheitsvorfällen und erkannten Schwachstellen

7

die Verwaltung von Updates, die Veröffentlichung von Patches, die Dokumentation und die Informationsprozesse

8

die Dokumentation der Sicherheitsregeln, um einen effektiven Einsatz der Lösung in der Zielumgebung zu gewährleisten, mit Härtungsanleitungen, Benutzerdokumentationen und sogar sicheren Löschverfahren

Eine Zertifizierung gemäß IEC 62443-4-1 ermöglicht es somit, den Produktentwicklungsprozess an die hohen Sicherheitsbedürfnisse der Benutzer von Produkten für die industrielle Automatisierung und Steuerungssysteme anzupassen. Diese Benutzer profitieren somit von gut dokumentierten Sicherheitskonfigurationen und Patch-Management-Verfahren mit einer klaren und prägnanten Kommunikation über die im Produkt erkannten Sicherheitslücken.

Stormshield steht Ihnen zur Seite

Stormshield unterstützt industrielle Automatisierungs- und Kontrollsysteme bei der Einhaltung der IEC 62443 durch drei Produktlinien, die Peripherieschutz, Desktopschutz sowie End-to-End-Datenschutz bieten.

Mit der gemäß IEC 62443-4-1 zertifizierten Produktreihe Stormshield Network Security können Sie darauf vertrauen, dass Sie ein Produkt erhalten, das mit einem optimalen Sicherheitsniveau entwickelt, produziert und gepflegt wird. Darüber hinaus sind die Funktionen der verschiedenen Stormshield-Lösungen sehr nützlich bei der Erfüllung der 7 Grundanforderungen der Norm:

FR1: Identifizierung, Authentifizierungskontrolle (IAC)

Die Lösung Stormshield Network Security ermöglicht es, sowohl Netzwerke (einschließlich WLAN) als auch Maschinen und Benutzer zu identifizieren und gleichzeitig die damit verbundenen Zugriffskontrollen in die Sicherheitsrichtlinien zu integrieren.

Die Funktionen zur Benutzerverwaltung und -authentifizierung sind sehr flexibel und ermöglichen entweder die Übernahme von Daten aus der Unternehmensdatenbank oder die Einrichtung einer eigenständigen und vollständigen Infrastruktur, die auch die Verwaltung externer Benutzer ermöglicht.

FR2: Nutzungskontrolle (UC)

Die Nutzungskontrolle beruht in erster Linie auf den Sicherheitsrichtlinien, die innerhalb des Peripherieschutzes festgelegt werden. Die Lösung Stormshield Network Security geht über Netzwerksegregation oder -segmentierung, Zugriffsbeschränkungen (WLAN oder mobile Geräte) oder Sitzungskontrollen hinaus: Die Lösung ermöglicht es auch, die Dauer von Sitzungen zu begrenzen, Remote-Verbindungen zu trennen oder bösartigen mobilen Code abzufangen und zu blockieren.

Zusätzlich garantiert die System Event Management-Lösung von Stormshield sichere Audit-Prozesse für Aktionen, die in industriellen Automatisierungs- und Kontrollsystemen durchgeführt werden.

FR3: Systemintegrität (SI)

Die Lösungen für Netzwerk- und Desktop-Sicherheit kontrollieren die Systemintegrität und schützen beispielsweise vor bösartigem Code. Beide Lösungen sind außerdem in der Lage, über ihre Sicherheitsrichtlinien vordefinierte Abhilfemaßnahmen zu implementieren.

Darüber hinaus gewährleistet die detaillierte Paketanalyse von Stormshield Network Security die Integrität der Kommunikation und der Sitzungen sowie die Verifizierung der an die Steuerungen gesendeten Befehlscodes.

Die Lösung Stormshield Endpoint Security bietet Schutz vor Modifizierungen auf der Ebene der Systemanwendungen, während die Lösung Stormshield Data Security die Informationsintegrität abdeckt.

Schließlich kann der Schutz von Audit-Informationen durch das gleichzeitige Senden der Protokolle an mehrere Server erreicht werden.

FR4: Datenschutz (DC)

Der Zugriff auf Informationen wird sowohl für Daten in Transit über die sichere Kommunikation von Stormshield Network Security als auch für gespeicherte Daten über die Datenschutzlösung Stormshield Data Security gewährleistet.

Die von diesen Lösungen verwendeten Verschlüsselungsmechanismen sind auf höchstem europäischen Niveau qualifiziert und garantieren die Verwaltung von Ressourcen, die nach ihrer Außerbetriebnahme nicht länger auf Informationen zugreifen dürfen.

FR5: Einschränkung des Datenflusses (RDF)

Das Datenflussmanagement gewährleistet, dass industrielle Automatisierungs- und Steuerungssysteme den Anforderungen rund um Sicherheitszonen und Kanäle entsprechen. Allein die Routing-Funktionen in Stormshield Network Security sowie die Kontrolle des Netzwerkflusses bis hin zur Anwendungsebene bieten eine optimale Antwort auf alle Sicherheitsanforderungen.

So ermöglicht die Lösung die Segmentierung des Netzwerks, den Schutz der Grenzen von Sicherheitszonen und die Kontrolle ausgehender Nachrichten über einen Mechanismus, der die Datenströme standardmäßig blockiert und nur autorisierte Kommunikation zulässt.

FR6: Rechtzeitige Reaktion auf Ereignisse (TRE)

Jedes Stormshield-Produkt stellt Ereignisprotokolle bereit, mit denen sich die Aktionen in industriellen Automatisierungs- und Kontrollsystemen, die durchlaufenden Netzwerkdaten sowie die generierten Sicherheitswarnungen nachverfolgen lassen.

Der schreibgeschützte Zugriff auf diese Protokolle gewährleistet eine kontinuierliche Überwachung der Ereignisse durch ausschließlich autorisierte Personen. Darüber lassen sich Sicherheitsvorfälle mit der Lösung Stormshield Log Supervisor effektiv verwalten.

FR7: Ressourcenverfügbarkeit (RA)

Die Verfügbarkeit von Ressourcen bezieht sich auf die Anforderungen an die Handhabung von Denial-of-Service-Angriffe oder Serviceverschlechterungen. Diese Anforderungen werden sowohl von Stormshield Network Security als auch von Stormshield Endpoint Security im Hinblick auf die Verwaltung von Backups und Wiederherstellungen, die Konfiguration von Sicherheitsfunktionen und die Verwaltung von Beschränkungen der Ressourcennutzung erfüllt.

Die Lösung Stormshield Network Security schützt auch Netzwerke vor Denial-of-Service-Angriffen und bietet Netzteilredundanz, um bei Bedarf auf ein sekundäres Energienetzwerk umzuschalten.

Die wichtigsten Vorteile der Zusammenarbeit mit Stormshield

Stormshield ist seit zehn Jahren ein wichtiger Akteur im Bereich der industriellen Cybersicherheit auf europäischer Ebene und bietet umfassende und maßgeschneiderte Lösungen für industrielle Automatisierungs- und Steuerungssysteme. Unsere Teams aus Experten für industrielle Cybersicherheit stehen Ihnen zur Seite und begleiten Sie in allen Phasen Ihres Industrieprojekts. Mit unseren detaillierten Schulungen können Ihre operativen Teams in Bezug auf die besten Praktiken im Bereich der Cybersicherheit ihre Kompetenz ausbauen.

Die drei Produktreihen von Stormshield erfüllen alle Sicherheitsregeln der 7 Grundanforderungen der Norm. Die Lösungen unterstützen industrielle Automatisierungs- und Steuerungssysteme bei der Einhaltung der Norm IEC 62443, indem sie Peripherieschutz, Desktopschutz und End-to-End-Datenschutz bieten.

3 Haupt-punkte

Mit der Produktreihe Stormshield Network Security, die als einzige reine Cyber-Lösung gemäß IEC 62443-4-1 zertifiziert ist, können Sie darauf vertrauen, dass Sie Produkte erhalten, die mit einem optimalen Sicherheitsniveau entwickelt, produziert und gepflegt werden.

Neben einem Entwicklungsprozess, der die Anforderungen der Norm erfüllt, unterscheiden sich die Produkte von Stormshield Network Security in drei wichtigen Punkten von den Produkten unserer Hauptkonkurrenten.

Nahtlose Integration in bestehende Infrastrukturen

Die Segmentierung in Subnetzwerke in Kombination mit dem Hybridmodus (Routing + transparenter Modus) sorgt für eine sichere Verbindung zwischen Geräten, indem besonders kritische Assets isoliert werden, um den Datenfluss innerhalb industrieller Automatisierungs- und Steuersysteme besser kontrollieren zu können.

Der Hybridmodus ermöglicht die Implementierung von Netzwerkrouting- und Segmentierungsfunktionen bei minimalen Änderungen an der bestehenden operativen Infrastruktur.

Die Vielzahl der möglichen Konfigurationen gewährleistet die Kompatibilität mit einer sehr großen Bandbreite an Architekturen und garantiert so eine nahtlose Integration der Firewalls in bestehende Infrastrukturen.

Detaillierte Inspektion des Befehlsflusses

Die Intrusion Prevention Engine bietet eine Tiefenanalyse (DPI – Deep Packet Inspection) der Kommunikation innerhalb von industriellen Systemen. Diese Analyse schützt vor bösartigem Code und ermöglicht eine Kontrolle der Protokollkonformität sowie eine genaue Analyse der Nachrichten, die zwischen den Steuerungen und den höheren Verwaltungsebenen (Überwachung/SCADA) ausgetauscht werden.
Der innovative Ansatz dieser Analyse gewährleistet eine präzise Kontrolle der Nachrichten, die an die Steuerungen gesendet werden und unterstützt eine granulare Verwaltung der zulässigen Aktionen.
Sie können das Schutzniveau auch erhöhen, indem Sie die übertragenen Befehle und Werte (Geschwindigkeit, Druck, Menge…) einschränken, um anormales Verhalten oder das Abdriften des industriellen Prozesses zu begrenzen.

Auf höchstem europäischen Niveau zertifiziert

Die Zertifizierung gemäß IEC 62443-4-1 beweist Stormshields Engagement, vertrauenswürdige Produkte für industrielle Systeme anzubieten. Dieses Vertrauen zeigt sich auch in der Common-Criteria-Zertifizierung der Stormshield-Produkte, die von verschiedenen europäischen Instanzen anerkannt wird. Diese Anerkennung als qualifiziertes Produkt (NATO oder EU Restreint) bestätigt, dass Stormshield-Produkte auf höchstem europäischen Niveau zertifiziert sind.
Auf der Grundlage zertifizierter Produkte gewährleistet dieser Ansatz gegenseitiges Vertrauen in die Daten, die zwischen den verschiedenen Systemkomponenten ausgetauscht werden. Die zu 100 % europäischen Lösungen von Stormshield tragen zur Sicherheit und Souveränität Ihrer sensiblen Assets bei, damit Sie jederzeit die Kontrolle behalten.

Antwort von Stormshield auf die Norm IEC62443

Um den Einsatz von Gegenmaßnahmen oder auch von technischen und organisatorischen Mitteln zu erleichtern, schlagen die Sicherheitsziele der Norm IEC62443 **verschiedene Sicherheitsniveaus vor, die einen qualitativen Ansatz ermöglichen,** um die erwartete Sicherheit pro Zone zu gewährleisten.

Die Sicherheitsniveaus (Security Level – SL) werden anhand von Kriterien festgelegt, die für jede Art von Bedrohung spezifisch sind, wie z. B. die Fähigkeiten, Mittel oder Ressourcen, die für die Durchführung eines Angriffs erforderlich sind. Die folgende Tabelle beschreibt die vier erwarteten Sicherheitsniveaus entsprechend der möglicherweise auftretenden Bedrohungen.

Niveau de sécurité	Cible	Compétences	Motivations	Moyens	Ressources
1	Violations occasionnelles ou accidentelles	Pas de compétences en matière d'attaques	Erreur	Actes non intentionnel	Limitées à un individu
2	Cybercrime, pirate	Générique	Faible	Simple	Faible (individu isolé)
3	Hacktiviste, terroriste	Spécifiques aux systèmes de contrôle industriel	Modérée	Sophistiqués (attaque)	Modérées (groupe de pirates)
4	Nation/Etat	Spécifiques aux systèmes de contrôle industriel	Elevée	Sophistiqués (campagne)	Etendues (équipe multidisciplinaires)

FR1: Identifizierung, Authentifizierungs- und Zugangskontrolle (Access Control, AC)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
1.1	**Identifizierung und Authentifizierung menschlicher Benutzer**	SL1 SL2 SL3 SL4	Stormshield bietet mehrere Methoden für die Benutzerauthentifizierung – sogar MFA für den Traffic, der die Firewall selbst adressiert, sowie für den Traffic, der die Firewall passiert. Wenn ein Gerät die Authentifizierung nicht unterstützt, ist es möglich, es direkt mit der Firewall zu verbinden und die Authentifizierungsfunktionen (Portal oder SSL-VPN) zu nutzen.
1.2	**Softwareprozess und Geräteidentifizierung/ -authentifizierung**	SL1 SL2 SL3 SL4	Stormshield bietet die Möglichkeit, Richtlinien auf der Basis von MAC-Adressen zu erstellen.
1.3	**Kontoverwaltung**	SL1 SL2 SL3 SL4	Stormshield stellt Einzel- oder Gruppenkonten auf der Grundlage von Internal LDAP, External LDAP, Multiple AD oder Radius bereit. Es ist möglich, verschiedenen Benutzern oder Benutzergruppen unterschiedliche Granularitäten zuzuweisen.
1.4	**ID-Management**	SL1 SL2 SL3 SL4	Stormshield kann jedem Benutzer eine andere Rolle zuweisen.
1.5	**Authentifizierungsmanagement**	SL1 SL2 SL3 SL4	Stormshield kann Benutzer dazu zwingen, sich über eine interne oder externe Datenbank zu authentifizieren. Es ist möglich, ein Ablaufdatum für Passwörter festzulegen und die Änderung des Passworts bei der Anmeldung zu erzwingen.
1.6	**Drahtloses Zugriffsmanagement**	SL1 SL2 SL3 SL4	Stormshield unterstützt WLAN-Verbindungen nicht, aber dank des Hybridmodus ist es möglich, ein WLAN-Netzwerk an einen dedizierten Port anzuschließen. Selbst wenn das WLAN-Netzwerk denselben Adressraum nutzt, kann beim Übergang vom WLAN-Netzwerk zum physischen Netzwerk eine Authentifizierung und IPS-Analyse erzwungen werden.
1.7	**Stärke der passwortbasierten Authentifizierung**	SL1 SL2 SL3 SL4	Es ist möglich, die Länge und Entropie sowie den Zeichentyp eines Passworts sowohl für den Firewall-Administrator als auch für Endbenutzerkonten zu erzwingen.
1.8	**PKI-Zertifikate (Public Key Infrastructure)**	SL1 SL2 SL3 SL4	Alle Stormshield-Firewalls umfassen eine PKI, sie können jedoch auch mit einer externen PKI kombiniert werden.
1.9	**Stärke der Public-Key-Authentifizierung**	SL1 SL2 SL3 SL4	Stormshield kann die Gültigkeit eines Zertifikats sowie die CRL prüfen. Diese Prüfung umfasst auch die Gültigkeit der Zertifizierungsstelle (CA), die das jeweilige Zertifikat herausgegeben hat.
1.10	**Authenticator-Feedback**	SL1 SL3 SL4	Passwörter werden während des Authentifizierungsprozesses verschleiert.
1.11	**Fehlgeschlagene Anmeldeversuche**	SL1 SL2 SL3 SL4	Fehlgeschlagene Anmeldeversuche werden in einem eigenen Protokoll mit dem Namen „l_auth“ gespeichert und in der GUI angezeigt. Außerdem erkennt die Angriffserkennung sie in SSH- und LDAP-Systemen.
1.12	**Benachrichtigung über die Systemnutzung**	SL1 SL2 SL3 SL4	Es ist möglich, beim Zugriff auf die Firewall einen benutzerdefinierten Hinweis anzuzeigen.
1.13	**Zugriff über nicht vertrauenswürdige Netzwerke**	SL1 SL2 SL3 SL4	Der Zugriff auf das Gerät oder das interne Netzwerk über nicht vertrauenswürdige Netzwerke kann auf der Grundlage verschiedener Methoden wie Benutzer, Netzwerke, Standort oder IP-Reputation gefiltert werden.

FR2: Nutzungskontrolle (Use Control, UC)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
2.1	**Erzwungene Autorisierung**	SL1 SL2 SL3 SL4	Stormshield ist in der Lage, verschiedenen Ports unterschiedliche Authentifizierungsregeln zuzuweisen, um je nach Herkunft der eingehenden Verbindung unterschiedliche Richtlinien festzulegen. Für den an die Firewall gerichteten Traffic kann je nach Rolle eine READ/WRITE-Berechtigung erstellt werden. Für den Traffic, der die Firewall passiert, kann eine Schablone mit autorisierten Befehlen für Industrieprotokolle erstellt und verschiedenen Benutzern zugewiesen werden.
2.2	**Drahtlose Nutzungssteuerung**	SL1 SL2 SL3 SL4	Stormshield-Firewalls tragen dazu bei, einen drahtlosen Zugangspunkt mit dem Gerät zu verbinden und die Authentifizierung zu erzwingen, um auf das andere Netzwerksegment zuzugreifen. Der Stormshield Endpoint Security Agent ist in der Lage, den Zugriff ausschließlich für festgelegte WLAN-Netzwerke zu akzeptieren.
2.3	**Nutzungssteuerung für tragbare und mobile Geräte**	SL1 SL2 SL3 SL4	Anhand von BYOD-Signaturen können bestimmte Geräte autorisiert oder geblockt werden. Außerdem können Mobilgeräte dazu gezwungen werden, einen sicheren Kanal zu öffnen, um auf das interne Netzwerk zuzugreifen. Auf diese Weise lassen sich benutzerdefinierte Richtlinien erstellen.
2.4	**Mobiler Code**	SL1 SL2 SL3 SL4	Stormshield kann die Nutzung des mobilen Codes abfangen und analysieren, um bösartige Aktivitäten zu verhindern.
2.5	**Sitzungssperre**	SL1 SL2 SL3 SL4	Authentifizierte Benutzer können zulässige Authentifizierungszeiträume festlegen.
2.6	**Schließen von Remote-Sitzungen**	SL1 SL2 SL3 SL4	Es ist möglich, Remote-Sitzungen, die für eine bestimmte Zeit inaktiv waren, manuell durch den Benutzer oder erzwungen durch einen Superuser zu schließen.
2.7	**Kontrolle gleichzeitiger Sitzungen**	SL1 SL2 SL3 SL4	Gleichzeitige Sitzungen können gesteuert werden, indem parallele Verbindungen von mehreren Hosts blockiert werden.
2.8	**Audit-fähige Ereignisse**	SL1 SL2	Alle System- und Benutzerzugriffsereignisse sind konfigurierbar. Zu jedem Ereignis können E-Mails versendet, Ereignisprotokolle erstellt und Warnmeldungen generiert werden.
2.9	**Audit-Speicherkapazität**	SL1 SL2 SL3 SL4	Wenn der Speicherplatz einen bestimmten Schwellenwert erreicht, wird der Administrator per SNMP, Mail oder Alert gewarnt. In jedem Fall rotieren die Protokolle. Die Festplattennutzung wird in jedem Fall über SNMP verwaltet.
2.10	**Reaktion auf Fehler bei der Audit-Verarbeitung**	SL1 SL3 SL4	Um Fehler bei der Audit-Verarbeitung zu vermeiden, ist Stormshield in der Lage, Protokolle lokal zu speichern und sie an vier verschiedene Syslog-Server gleichzeitig zu senden.
2.11	**Zeitstempel**	SL1 SL2 SL3 SL4	Alle Protokolle und Systemereignisse werden mit einem Zeitstempel versehen. Zeitstempel können mit einer internen Uhr oder einem externen NTP-Server synchronisiert werden.
2.12	**Nichtabstreitbarkeit (Non-Repudiation)**	SL1 SL2 SL3 SL4	In der Firewall selbst sind alle Protokolle personenbezogen und es lässt sich feststellen, ob und wann ein Benutzer eine Regel geändert hat.

FR3: Systemintegrität (System Integrity, SI)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
3.1	**Kommunikationsintegrität**	SL1 SL2 SL3 SL4	Stormshield bietet verschiedene Technologien, um die Kommunikationsintegrität zu gewährleisten. Bei bestimmten Industrieprotokollen, die die Firewall durchlaufen, speichert die IPS-Engine den Status der Kommunikation, um böswillige Versuche, Pakete im Rahmen eines MIDM-Angriffs einzuschleusen, zu erkennen. Bei Firewalls, die mehrere Ports im selben Netzwerk verwalten, kann das Gerät den Daten-Traffic mit einer „IP SPOOFING"-Warnung blockieren, wenn der Versuch, eine legitime IP zu ersetzen, festgestellt wird. Stormshield bietet auch die Möglichkeit, ein transparentes Layer2-IPSEC-VPN einzurichten. Auf diese Weise kann die Layer2-Kommunikation mit jedem Gerät verschlüsselt werden, das diese Funktion nicht von Haus aus unterstützt.
3.2	**Schutz vor Schadcode**	SL1 SL2 SL3 SL4	Stormshield bietet einen ganzen Satz von Signaturen, um Schadcodes abzufangen und zu blockieren.
3.3	**Verifizierung von Sicherheitsfunktionen**	SL1 SL2 SL3 SL4	Es ist möglich, ein Ereignis mit dem Befehl „SENDALARM" künstlich auszulösen. Es ist auch möglich, künstlich Protokolle in das System einzuschleusen, um die Verbindung zu externen SIEM- und Audit-Plattformen zu testen.
3.4	**Software- und Informationsintegrität**	SL1 SL2 SL3 SL4	Der gesamte Code, der auf der Firewall ausgeführt wird, ist signiert. Ein Versuch, ihn zu verändern, führt zu einem Fehler in der Bootphase.
3.5	**Input-Validierung**	SL1 SL2 SL3 SL4	Das Industrie-Plugin-System analysiert alle Industrie-Befehle, um ihre Übereinstimmung mit der RFC und den Benutzeranforderungen zu validieren. Ein nicht-validiertes Paket wird automatisch blockiert.
3.6	**Deterministischer Output**	SL1 SL2 SL3 SL4	Dieser Punkt bezieht sich in erster Linie auf die Entwicklungsmethodik, aber in Bezug auf den Betrieb der Firewall selbst können wir bestätigen: Es ist möglich, die Reaktion auf jede Art von Angriff zu konfigurieren: IPS: Angriffe erkennen und blockieren. IDS: Angriffe erkennen und protokollieren, aber nicht blockieren. FW: Angriffe ignorieren und mit dem normalen Betrieb fortfahren. Dieses Verhalten kann für jede Sicherheitsrichtlinie definiert werden.
3.7	**Fehlerbehandlung**	SL1 SL2 SL3 SL4	Dieser Punkt bezieht sich in erster Linie auf die Entwicklungsmethodik, aber in Bezug auf den Betrieb der Firewall selbst können wir bestätigen: Wenn ein Administrator eine Sicherheitsrichtlinie hinzufügt, wird die gesamte Richtlinienkette überprüft. Wird eine Anomalie festgestellt, wird sie an den Administrator weitergeleitet.
3.8	**Sitzungsintegrität**	SL1 SL2	Bezüglich des Zugriffs auf die Firewall selbst: Es ist stets nur ein Benutzer zur gleichen Zeit befugt, die Konfiguration zu ändern. Wenn ein anderer Benutzer versucht, eine Konfiguration zu ändern, die bereits von einem anderen Administrator bearbeitet wurde, muss der Benutzer Administratorrechte anfordern, um seine Änderung vorzunehmen.
3.9	**Schutz von Audit-Daten**	SL1 SL2 SL3 SL4	Protokolle werden durch die Unterstützung von bis zu vier externen Syslogs gesichert. Einige Modelle verfügen über redundante Datenträger.

FR4: Datenvertraulichkeit (Data Confidentiality, DC)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
4.1	**Informationsvertraulichkeit**	SL1 SL2 SL3 SL4	Stormshield kann dank VPN-Unterstützung (IPSEC oder SSL) die Vertraulichkeit der Informationen, die durch das Netzwerk fließen, gewährleisten. Wenn ein Benutzer auf das interne Netzwerk zugreifen muss, kann er über Stormshield einen sicheren Kanal öffnen, um alle ausgetauschten Informationen zu schützen. Die verwendeten Verschlüsselungsalgorithmen können je nach Benutzer und je nach gewünschtem Sicherheitsniveau variieren.
4.2	**Informationspersistenz**	SL1 SL2 SL3 SL4	Stormshield stellt SSH-Befehle bereit, um die Protokolle zu bereinigen, die Konfiguration zurückzusetzen und im Allgemeinen vertrauliche Informationen, die auf dem Gerät gespeichert sein könnten, zu löschen.
4.3	**Verwendung von Verschlüsselung**	SL1 SL2 SL3 SL4	Stormshield kann Verschlüsselung nutzen, um einen sicheren Kanal bereitzustellen. Die Verschlüsselung kann für jede Art von Kommunikation, die die Firewall durchläuft, definiert werden.

FR5: Eingeschränkter Datenfluss (Restricted Data Flow, RDF)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
5.1	**Netzwerksegmentierung**	SL1 SL2 SL3 SL4	Stormshield kann das Netzwerk in Segmente unterteilen und mehrere VLANs oder Netzwerkbereiche erstellen, die mit verschiedenen Ports verbunden sind. Selbst wenn das Netzwerk eine flache Architektur aufweist, ist es möglich, die Analyse der Daten, die von einem Port zum anderen fließen, zu erzwingen und so eine Art virtuelle Segmentierung zu schaffen, wenn zwei Geräte an verschiedene Ports der Firewall angeschlossen sind.
5.2	**Schutz für Zonengrenzen**	SL1 SL2 SL3 SL4	Die Objekte der Stormshield-Firewall (Netzwerk, Host, Bereiche) tragen dazu bei, die Assets der verschiedenen Sicherheitszonen zu verwalten. Wenn diese Objekte in Sicherheitsrichtlinien einbezogen werden, können die Kommunikationsregeln zwischen Sicherheitszonen festgelegt werden.
5.3	**Einschränkungen der allgemeinen Kommunikation zwischen Personen**	SL1 SL2 SL3 SL4	Stormshield ist in der Lage, soziale Medien, E-Mails und Kurznachrichten-Anwendungen auszufiltern.
5.4	**Anwendungspartitionierung**	SL1 SL2 SL3 SL4	Es ist möglich, eine Vorlage für zulässige Anwendungen zu erstellen und die Vorlage einer bestimmten SOURCE-Zone in Richtung einer bestimmten DESTINATION-Zone zuzuweisen.

FR6: Zeitnahe Reaktion auf Ereignisse (Timely Response to Events, TRE)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
6.1	**Zugänglichkeit von Audit-Protokollen**	SL1 SL2 SL3 SL4	Alle Firewalls verfügen über eine klare und intuitive Webschnittstelle, um auf die Protokolle zuzugreifen. Es ist möglich, eine Sicherheitsrichtlinie auszuwählen, um alle erstellten Protokolle anzuzeigen, oder von einer Sicherheitsrichtlinie aus zu einem Protokoll zu springen. Protokolle werden auch in einem grafischen Format angezeigt, um intuitiver zu sein.
6.2	**Kontinuierliche Überwachung**	SL1 SL2 SL3 SL4	Stormshield bietet eine Schnittstelle für die Echtzeit-Überwachung, die es ermöglicht, die Ressourcennutzung oder den Status von Verbindungen und authentifizierten Benutzern sowie den Status von verschlüsselten Kanälen zu kontrollieren.

DE7: Ressourcenverfügbarkeit (Resource Availability, RA)

Grundlegende Anforderungen		Erreichtes Sicherheitsniveau	Antwort von Stormshield
7.1	**DoS-Schutz**	SL1 SL2 SL3 SL4	Stormshield bietet einen dedizierten DOS-Erkennungs- und Schutzmechanismus, der vollständig konfigurierbar ist.
7.2	**Ressourcenverwaltung**	SL1 SL2 SL3 SL4	Stormshield-Firewalls verfügen über einen internen Watchdog und mehrere Kerne, um zu verhindern, dass eine intensive Nutzung einer Ressource die Gesamtleistung des Geräts beeinträchtigt.
7.3	**Sicherung des Kontrollsystems**	SL1 SL2 SL3 SL4	Stormshield bietet mehrere Backup-Funktionen. Von der aktiven zur Backup-Partition, um stets über ein voll funktionsfähiges Backup auf der Firewall zu verfügen (nützlich bei Updates). Cloud-Backup, um stets über eine Kopie des Backups bei Stormshield-Partnern zu verfügen. Benutzerdefiniertes Backup, um eine eigene Cloud-Sicherung zu erstellen. SMC: Es ist möglich, mehrere Firewalls über eine zentrale Konsole zu verwalten. In diesem Fall ist es möglich, die Backups im SMC Stormshield Management Center zusammenzuführen.
7.4	**Wiederherstellung und Wiederaufbau des Kontrollsystems**	SL1 SL2 SL3 SL4	Es ist möglich, ein Backup auch auf anderen Plattformen wiederherzustellen und wiederaufzubauen. Außerdem können Sicherungspartitionen auf demselben Gerät wiederhergestellt werden.
7.5	**Notfallstromversorgung**	SL1 SL2 SL3 SL4	Stormshield SNi20 und SNi40 können im Pass-on-Fail-Modus eingesetzt werden. Wenn die Geräte auf transparente Weise konfiguriert werden, kann das Verhalten einer Leitung im Falle eines Problems simuliert werden. Auf diese Weise bleibt der Zugriff auf das OT-Gerät stets gewährleistet. Stormshield unterstützt auch HA: Falls die Master-Firewall betroffen ist, kann ein Slave ihren Platz einnehmen und alle aktiven Sitzungen aufrechterhalten.
7.6	**Netzwerk- und Sicherheits-konfigurationseinstellungen**	SL1 SL2 SL3 SL4	Stormshield bietet die Möglichkeit, die Konfiguration im CSV-Format für eine detaillierte externe Analyse zu exportieren.
7.7	**Geringste Funktionalität**	SL1 SL2 SL3 SL4	Stormshield ermöglicht die Erstellung von Sicherheitsrichtlinien auf der Basis von Port, Protokoll, Anwendungsprotokollen, Webservice, Geostandort, IP-Reputation und Benutzern. Standardmäßig blockiert die herrschende Richtlinie den gesamten Traffic. Auf diese Weise ist es möglich, alles zu blockieren und nur den wichtigen Traffic zuzulassen.
7.8	**Komponenteninventar des Kontrollsystems**	SL1 SL2 SL3 SL4	Stormshield-Firewalls sind in der Lage, den Traffic zu analysieren und die an der Kommunikation beteiligten Komponenten sowie das verwendete Industrieprotokoll zu identifizieren. Es ist möglich, das Objekt im CSV-Format zu exportieren/importieren und Stormshield mit Sensoren wie Nozomi zu kombinieren.

DER **EUROPÄISCHE ANBIETER DER WAHL** FÜR **CYBERSICHERHEIT**

www.stormshield.com