IEC 62443-4-2-konforme Konfiguration der FL MGUARD-Produktfamilie

Anwenderhandbuch

Anwenderhandbuch

IEC 62443-4-2-konforme Konfiguration der FL MGUARD-Produktfamilie

UM DE MGUARD 62443-4-2, Revision 04 2025-01-22

Dieses Handbuch ist gültig für:

Beachten Sie die ebenfalls zugehörigen Handbücher zu den aufgeführten Artikeln (Dokumente: 110191_de_xx, 110192_de_xx, 110193_de_xx). Die Handbücher und weitere Anwenderdokumentation finden Sie unter phoenixcontact.com. Geben Sie dazu im Suchfeld eine der hier aufgeführten Artikelnummern an.

Bezeichnung	Artikel-Nr.
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 2102	1357828
FL MGUARD 2105	1357850
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

109049_de_04

Inhaltsverzeichnis

1 Einführung

Um der Norm IEC 62443 zu entsprechen, müssen mehrere Anforderungen auf verschiedenen Ebenen erfüllt werden. Eine Ebene bezieht sich auf die Geräte, die in einer IEC 62443-Umgebung verwendet werden sollen.

Dieses Dokument beschreibt, wie mGuard Geräte, auf denen mindestens die Firmware mGuard 10.5 läuft, konfiguriert werden müssen, sowie organisatorische Maßnahmen, um die Anforderungen der Norm IEC 62443-4-2 zu erfüllen.

Die mGuard 10-Firmware wurde unter Verwendung des IEC 62443-4-1 zertifizierten "PxCCS Development Prozess" der PHOENIX CONTACT Cyber Security GmbH entwickelt.

1.1 Wofür steht die Norm IEC 62443-4-2?

Die Norm IEC 62443-4-2 definiert Sicherheitsanforderungen für Komponenten, die in industriellen Automatisierungs- und Steuerungssystemen (IACS) eingesetzt werden.

Diese Anforderungen werden **Komponentenanforderungen (Component Requirements [CR])** genannt und sind eng verwandt mit den **Systemanforderungen (System Requirements [SR])**, die in IEC 62443-3-3 definiert sind. Sowohl CR als auch SR sind technische Anforderungen, die von der übergeordneten Definition der in IEC 62443-1-1 definierten sieben **Basisanforderungen (Foundational Requirements [FR])** abgeleitet wurden.

Basisanforderungen (FR):

1. Identifizierung und Authentifizierung (Identification and Authentication Control [IAC]),
2. Nutzungskontrolle (Use Control [UC]),
3. Systemintegrität (System Integrity [SI]),
4. Datenvertraulichkeit (Data Confidentiality [DC])
5. Eingeschränkter Datenfluss (Restricted Data Flow [RDF]),
6. Rechtzeitige Reaktion auf Ereignisse (Timely Response to Events [TRE]) und
7. Ressourcenverfügbarkeit (Resource Availability [RA])

Den Basisanforderungen werden in der Norm IEC 62443-4-2 einzelne Komponentenanforderungen (CR) zugewiesen. Die Erfüllung der Komponentenanforderungen (CR) und gegebenenfalls der zugehörigen Erweiterungen (Requirement Enhancements [RE]) führt zur Einstufung in einen von vier Security-Leveln (SL).

Der Erfüllungsgrad der Komponentenanforderungen (CR) drückt somit die Fähigkeit einer Komponente aus, in einem IACS mit einem bestimmten Security Level (SL) verwendet zu werden.

Hierbei ist es wichtig zu beachten, dass Komponenten eines Automatisierungssystems auch kombiniert werden können, sodass das Gesamtsystem die gewünschten Systemanforderungen (SR) erfüllt, um ein bestimmtes Security-Level nach IEC 62443-3-3 zu erreichen. Es ist somit nicht notwendig, dass jede einzelne Komponente für jeden CR den angestrebten Security-Level (SL) erreicht.

1.2 Was ist ein Security-Level?

Security-Level (SL) spiegeln die erforderlichen Gegenmaßnahmen zur Verhinderung bestimmter Sicherheitsrisiken wieder. Es werden vier Security-Level SL 1 bis SL 4 definiert, die durch individuelle Sicherheitsmaßnahmen erfüllt werden können. Diese Maßnahmen sind in den Kapiteln Sicherheitskontext / Sicherheitskonzept und mGuard-Geräte konfigurieren beschrieben.

Die zugehörigen vier SL sind in der Norm IEC 62443-4-2 wie folgt definiert:

- SL 1: Verhindern der nicht autorisierten Offenlegung von Informationen durch Abhören oder zufälliges Aufdecken.
- SL 2: Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit einfachen Mitteln bei geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation suchende Einheit.
- SL 3: Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und moderatem Aufwand, IACS-spezifischen Fertigkeiten und mittlerer Motivation suchende Einheit.
- SL 4: Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifischen Fertigkeiten und hoher Motivation suchende Einheit.

1.3 Wer ist die Zielgruppe der IEC 62443-4-2?

In erster Linie Betreiber, Systemintegratoren und Hersteller, die in der Automatisierungstechnik tätig sind.
Systemintegratoren können leicht feststellen, mit welchen Komponenten sich bestimmte Security-Level erreichen lassen. Hersteller erhalten Unterstützung bei der Entscheidung, welche einzelnen Komponenten wie in einem Automatisierungssystem kombiniert werden können, um ein bestimmtes Security-Level für das Gesamtsystem zu erreichen.

2 Sicherheitskontext / Sicherheitskonzept

2.1 Sicherheitskonzept

Um zuverlässige Sicherheit zu erreichen, ist das Defense-in-Depth-Design von Automatisierungssystemen eine wichtige Maßnahme bei der Gestaltung und Umsetzung eines auf der Normenreihe IEC 62443 basierenden Prozesses.

Die Umsetzung von Defense-in-Depth-Maßnahmen führt zu einer Sicherheitsarchitektur, in der Sicherheit in mehreren Schichten aufgebaut wird.

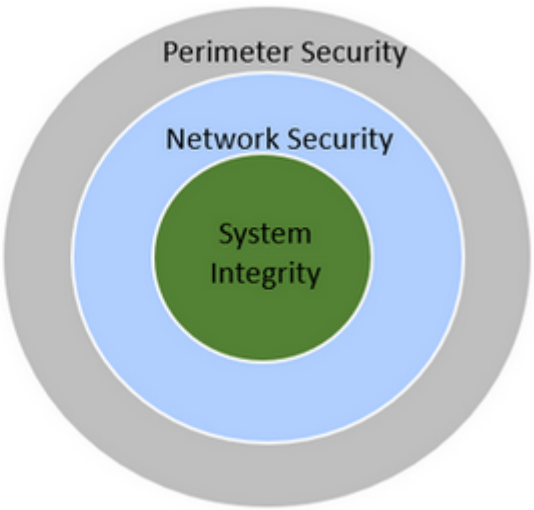
Das Ergebnis ist eine generische Schichtenarchitektur, die zu einer vollständig segmentierten Struktur der Vermittlungsschicht führt. Die Sicherheitsarchitektur von mGuard-Geräten und Anwendungsfälle sind im Sicherheitskontext (mGuard) beschrieben.

Der mGuard-Sicherheitskontext ergibt sich aus der Kombination von technologischen und organisatorischen Maßnahmen, die zusammengenommen die Anforderungen aus der Norm IEC 62443-4-2 und die Philosophie eines ganzheitlichen Sicherheitsansatzes umsetzen.

2.1.1 Das Defense-in-Depth-Konzept

Ein allgemeines Defense-in-Depth-Konzept besteht aus drei Schichten:

Bild 2-1 Defense-in-Depth-Konzept



2.1.1.1 Perimetersicherheit (Perimeter Security)

Perimeter sind die äußeren Grenzen des Netzwerkes, die durch physische Maßnahmen wie Zäune, Türen, physische Zutrittskontrolle usw. geschützt werden.

2.1.1.2 Netzwerksicherheit (Network Security)

Diese Schicht enthält die Unternehmens- oder Bürozone (Office Zone) und eine Service-Management-Zone, die durch bekannte IT-Sicherheitskonzepte geschützt sind.

2.1.1.3 Systemintegrität (System Integrity)

Diese Schicht enthält OT-Geräte und -Anwendungen, die durch IEC 62443-Konzepte zu schützen sind.

2.1.1.4 Phoenix Contact Industrial Security-Leitfaden

Die zunehmende Vernetzung von Systemen, Komponenten und Geräten sowie die wachsende Menge der zu übertragenden und zu speichernden Daten führen zu einem erhöhten Risiko von Cyber-Angriffen.

Die logische Konsequenz daraus muss eine hohe Priorisierung des bestmöglichen Schutzes vor Cyber-Angriffen, Bedrohungen und missbräuchlicher oder fehlerhafter Datenverwendung und -manipulation sein.

Weitere allgemeine Informationen zur Cyber-Sicherheit finden Sie im Phoenix Contact Industrial Security-Leitfaden unter:

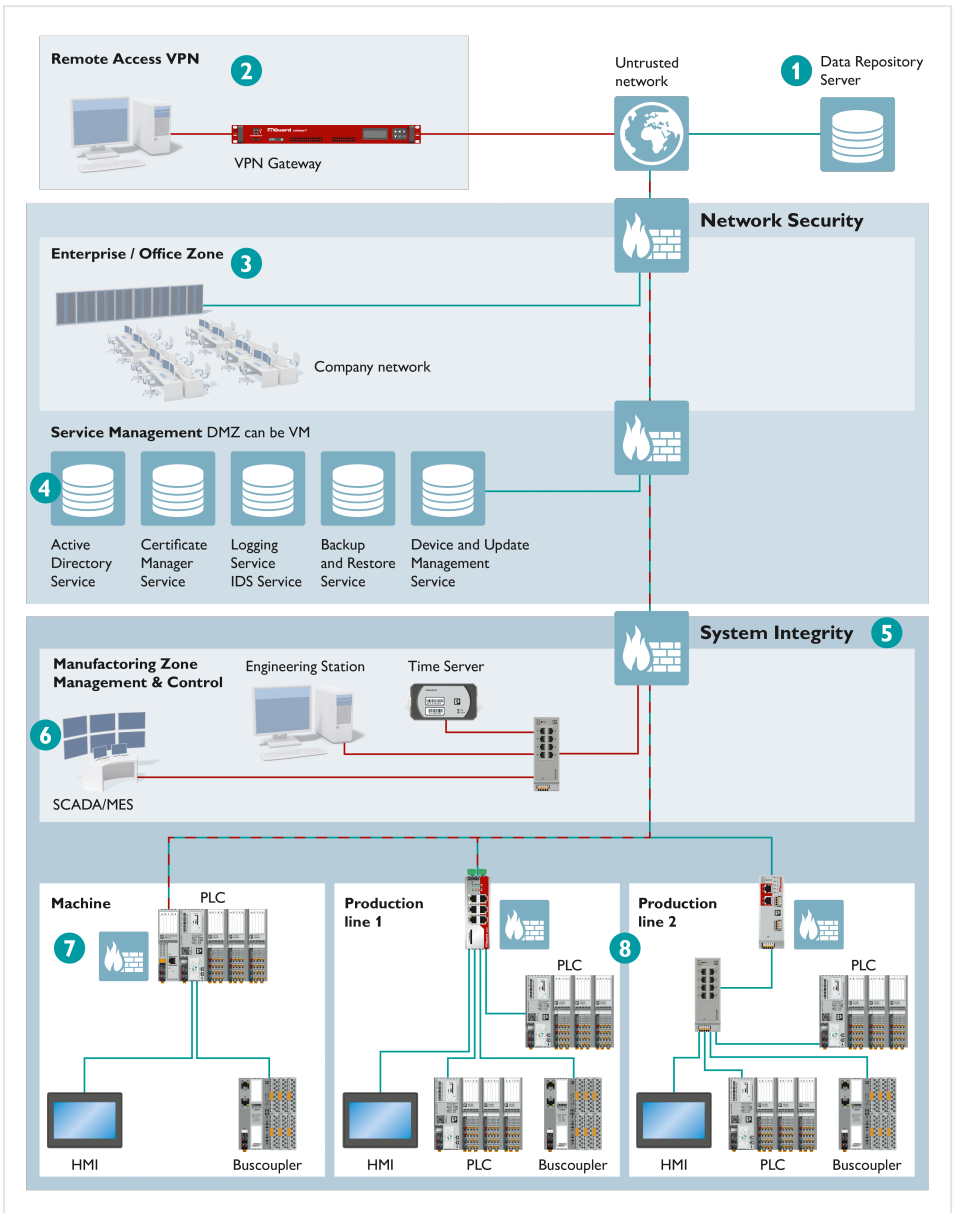
security.plcnext.help/se/Industrielle_Sicherheit_Leitfaden/Sicherheit_Intro.htm

2.2 Sicherheitskontext (mGuard)

Um die in der Normenreihe IEC 62443 definierten Anforderungen zu erfüllen, muss das Gerät (mGuard) in den vorgesehenen Anwendungsfällen eingesetzt werden, die sich aus dem definierten Sicherheitskontext (Anwendungsfälle) ergeben. Die folgende Abbildung zeigt den allgemeinen Sicherheitskontext:

- Blau-grüne Verbindungen repräsentieren Sicherheitsmechanismen (z. B. HTTPS).
- Rote Verbindungen stellen virtuelle private Netzwerke (VPNs) dar.

Bild 2-2 Das mGuard-Sicherheitskonzept



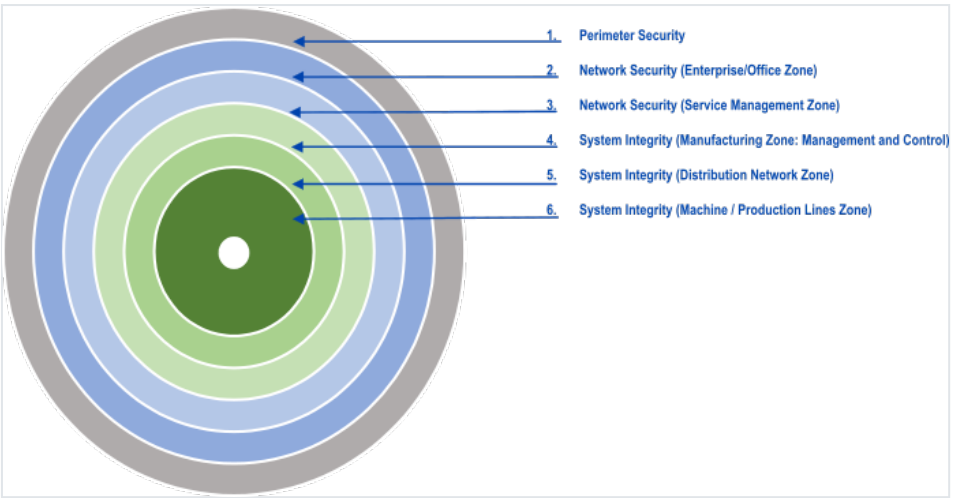
Die verschiedenen Ebenen (Zonen und Leitungen) sind durch Nummern gekennzeichnet:

Nummer	Beschreibung	Details
1	**Data Repository Server**	Stellt Daten für das Patch-Management/ Asset-Management bereit.
2	**VPN-Server**	Fernwartungszugriff über VPN
3	**Unternehmens-/ Bürozone (Office Zone)**	Fabrik-IT; ERP-Systeme (Enterprise Resource Planning); Produktionssteuerungssysteme. Geschützt durch Firewall
4	**Service-Management-Zone**	Diese Zone kann als entmilitarisierte Zone (DMZ) betrachtet werden, da sie die ICS-Netze (Zonen 5 bis 7) durch eine strenge Kontrolle des Informationsflusses vom externen Netz entkoppelt. Jegliche Kommunikation zwischen dem externen und dem ICS-Netz muss diese Zone passieren. Implementiert eine zentrale Benutzerverwaltung, Patch-/ Aktualisierungsverwaltung und Protokollierung. Sie enthält die folgende Infrastruktur: • Active Directory/RADIUS-Server oder LDAP-Server für Authentifizierungszwecke • Firewall- oder VPN-Komponente (z. B. als "jump host" implementiert), die die Kommunikation mit den anderen Zonen (Conduits) übernimmt
5	**Systemintegrität**	Fabrik OT, bestehend aus den Zonen 6 bis 8
6	**Fertigungszone**	Verwaltung, Überwachung und Steuerung des Hauptprozesses und der Unterprozesse. Implementiert SCADA, Zeitsynchronisation und Engineering. Diese Zone setzt sich wie folgt zusammen: • Kontrollzentrum (SCADA = Supervisory Control and Data Acquisition) • NTP-Server, der eine GPS-basierte Zeitbasis für die anderen beteiligten Geräte bereitstellt • Ethernet-Switch • Engineering-System (z. B. PLCnext Engineer) • Firewall, die die Kommunikation mit den anderen Zonen übernimmt (Conduits)

7	**Maschinenebene**	Hauptprozess Sammelt und verarbeitet die Daten des Prozesses und der Unterprozesse. Diese Zone ist wie folgt aufgebaut: • PLCnext Control mit I/O-Geräten • In der Steuerung sind Firewall und VPN-Server integriert, die die Kommunikation mit den anderen Zonen (Conduits) übernehmen • HMI für Steuerungs- und Visualisierungszwecke • Buskoppler
8	**Ebene der Produktionslinie Sub-Prozess**	Führt eine spezifische Automatisierungsfunktion in einer peripheren Einheit (Remote-Station) aus. Diese Zone setzt sich wie folgt zusammen: • PLCnext Control, jeweils mit dezentralen I/O-Geräten, die an den Feldbus angeschlossen sind • HMI zur Steuerung und Visualisierung • Ethernet-Switch • VPN integrierte Firewall und/oder VPN-Server (**mGuard Security Appliance**), der die Kommunikation mit den anderen Zonen (Conduits) übernimmt • Buskoppler

Der mGuard-Sicherheitskontext basiert auf dem Defense-in-Depth-Konzept und bietet sechs Sicherheitsebenen (Zonen/Conduits):

Bild 2-3 Defense-in-Depth-Konzept (Sicherheitsebenen)



Perimeter Security - die äußere Schicht

Zugriffsschutz für das Unternehmensnetz durch folgende Maßnahmen:

- Physische Isolierung
- Digitale Isolierung durch Netzwerksegmentierung
- Logische Zugangskontrollen
- Einsatz von speziell konfigurierten Firewalls. Die angegebene Firewall muss den ermittelten Bedrohungen und Schwachstellen entsprechen.
- VPN oder andere Sicherheitsmaßnahmen für den Fernzugriff
- Dokumentation aller Fernzugriffspunkte

Netzwerksicherheitsschichten

Schutz des Werksnetzes, bestehend aus der Unternehmensnetzzone und der Service-Management-Zone, die als demilitarisierte Zone (DMZ) betrachtet wird. Mögliche Maßnahmen sind:

- Identifizierung aller Netzwerkgeräte und Hosts
- Analyse von Protokollen/Verkehr
- Überprüfung von drahtloser Kommunikation/Verkehr
- Analyse von Switch-/Router-Konfigurationen

Maßnahmen in der DMZ:

- OS-Check auf Schwachstellen
- OS-Patch-Verwaltung
- Verhinderung der Nutzung von USB- oder Wechselmedien im Kontrollraum
- Beschränkung der Verbindung mit externen Computern

Systemintegrität - die inneren Schichten

Maßnahmen für SCADA-Anwendungen:

- Überwachung des Netzwerks auf Klartextübertragung und Verwendung von Verschlüsselung
- Sicherstellung der Verwendung von individuellen Benutzerkonten
- Eingeschränkter Zugang zum Desktop

Maßnahmen für Steuerungs-Teilnetze auf der Ebene der Maschinen/Produktionslinien (Hauptprozess und Teilprozesse):

- Verkabelte vs. drahtlose Kommunikation
- Ethernet vs. serielle Kommunikation
- Aufzeichnung des Datenverkehrs auf Ethernet-Verbindungen

Maßnahmen für Feldsteuerungen:

- Ethernet vs. seriell angeschlossene Geräte
- Ethernet-Geräte im Labor auf Schwachstellen getestet
- Standardpasswörter des Herstellers entfernt

2.2.1 Sicherheitskontext (Anwendungsfälle)

Die mGuard-Security-Router sind für den Zonenschutz in Produktionsstätten vorgesehen. Sie können verwendet werden, um Produktionszellen oder Automatisierungszellen vom Produktionsnetz in der Systemintegritätsschicht zu trennen. Siehe rote Umrandung auf dem vorherigen Bild.

Um die Anforderungen zu erfüllen, sind organisatorische Maßnahmen und lokale/ interne Einstellungen am mGuard-Gerät sowie Einstellungen an externen unterstützenden Systemen erforderlich.

Die folgenden Maßnahmen sind zwingend erforderlich, um die in der Norm IEC 62443-4-2 festgelegten Anforderungen zu erfüllen.

2.2.1.1 Organisatorische Maßnahmen

1. Das mGuard-Gerät muss von Personal konfiguriert werden, das bzgl. Sicherheit und den Anforderungen der Norm IEC 62443-4-2 geschult ist.
2. Geschützt durch den Perimeter muss das mGuard-Gerät in einem zugangsbeschränkten Schaltschrank in der Produktionsanlage installiert werden, zu dem nur qualifiziertes Personal Zugang hat.
3. Die Nutzung und Konfiguration des mGuard-Geräts richtet sich ausschließlich an Anwender, die mit den relevanten Sicherheitskonzepten der Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften, insbesondere der Normenreihe IEC 62443, vertraut sind.
4. Die übergeordneten Netzwerke müssen nach dem Defense-in-Depth-Prinzip und den Anforderungen der Normenreihe IEC 62443 abgesichert werden.
5. Das mGuard-Gerät darf nicht zur Prozesssteuerung verwendet werden.

2.2.1.2 Interne Maßnahmen, die nur auf dem Gerät konfiguriert werden

6. Die Zugriffsmöglichkeit auf das mGuard-Gerät über die Protokolle SSH und SNMP muss deaktiviert werden. Nur menschliche Anwender dürfen sich beim Web-based Management (WBM) des Gerätes anmelden.
7. Der „root“-Zugang zum Gerät darf nicht verwendet werden. Nur Anwender mit den Benutzerrollen "admin" und "audit" dürfen sich am Gerät anmelden.
8. Nur Konfigurationsprofile, die durch ein mGuard-Maschinenzertifikat kryptografisch signiert sind, dürfen vom und zum mGuard-Gerät herunter- oder hochgeladen werden.

2.2.1.3 Interne und externe Maßnahmen in Bezug auf externe Unterstützungssysteme

9. Es muss ein externer bzw. ein Remote-Authentifizierungsserver verwendet werden. Das mGuard-Gerät benutzt den externen Authentifizierungsserver als Client zur Authentifizierung. Es bleibt dem Kunden überlassen, welcher verfügbare und geeignete Authentifizierungsserver verwendet und betrieben wird.
   Der Authentifizierungsserver muss mindestens die folgenden Funktionen zur Verfügung stellen:

   – Erkennung von ungültigen Anmeldeversuchen
   – Vorübergehende Sperrung von Anwendern nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen

10. Es muss ein Remote-Protokollserver (Syslog-Server) verwendet werden. Die Remote-Log-Dateien müssen kontinuierlich ausgewertet werden.
11. Um das mGuard-Gerät mit den externen Authentifizierungs-, NTP- und Syslog-Servern zu verbinden, müssen zertifikatsbasierte IPsec-VPN-Verbindungen verwendet werden.
    1. Die Verwendung von Pre-Shared Keys (PSK) in diesen VPN-Verbindungen ist nicht zulässig.
    2. Die Verwendung von schwachen Verschlüsselungs- und Hash-Algorithmen in diesen VPN-Verbindungen ist nicht zulässig. Die folgenden Verschlüsselungs- und Hash-Algorithmen müssen mindestens verwendet werden: AES-256 / SHA-512 / Diffie-Hellman = 2048 Bits oder höher / PFS = 2048 Bits oder höher

3 mGuard-Geräte konfigurieren

Um die in der Norm IEC 62443-4-2 definierten Anforderungen zu erfüllen, muss das Gerät in den dafür vorgesehenen Anwendungsfällen, die sich aus dem definierten Sicherheitskontext ergeben, verwendet werden (siehe Sicherheitskontext). Mehrere Funktionen des Gerätes (mGuard) müssen dazu nach bestimmten Vorgaben eindeutig und verpflichtend konfiguriert werden.
Die folgenden Kapitel führen Sie durch die Anforderungen und beschreiben, welche Einstellungen auf dem mGuard-Gerät vorgenommen werden müssen, um die Anforderungen nach IEC 62443-4-2 zu erfüllen.

Im Dokument wird sowohl auf das Menü des Web-based Managements (WBM-Menü), in dem die Einstellungen vorgenommen werden, als auch auf die entsprechintegrienden Kapitel in der Anwenderdokumentation Bezug genommen. Verweise auf die entsprechenden Kapitel im mGuard-Anwenderhandbuch „Web-based Management“ (110191_en_xx) wurden hinzugefügt --> (UM: <Kapitel>).
Das Anwenderhandbuch (UM DE MGUARD10 / Dokument-ID: 110191_en_xx) und weitere Dokumente sind zum Download im Phoenix Contact Web Shop unter phoenixcontact.net/product/1357875 in der Rubrik "Download --> Handbuch" verfügbar.

3.1 FR 1 - Identifizierung und Authentifikation (IAC)

Alle Nutzer (menschliche Nutzer, Softwareprozesse und Geräte) identifizieren und authentifizieren, bevor
ihnen der Zugriff auf das System oder Betriebsmittel gewährt wird.

Security-Level	Erfüllung	Links
CR 1.1 Identifizierung und Authentifikation von menschlichen Nutzern		
SL 2	Um menschliche Benutzer bei der Anmeldung am Web-based Management (WBM) sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen.	
	Maßnahme 1 (Intern) Eine Anmeldung über SSH und SNMP ist nicht erlaubt und muss auf dem mGuard-Gerät unterbunden werden. Dazu müssen folgende Funktionen auf dem Gerät **deaktiviert** werden (**Kontrollkästchen abwählen**): – Aktiviere SSH-Fernzugang – Erlaube SSH-Zugang als Benutzer root	Verwaltung >> Systemeinstellungen >> Shell-Zugang (UM: 4.1.3)
CR 1.1 RE1 Eindeutige Identifizierung und Authentifikation		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. Der externe Authentifizierungsserver muss die eindeutige	

Security-Level	Erfüllung	Links
	Identifizierung und Authentifikation jedes Benutzers vornehmen und bereitstellen.	
	Maßnahme 2 (Intern/Extern) Integrieren Sie einen externen Authentifizierungsserver.	Authentifizierung >> RADIUS (UM: 6.3)
	Maßnahme 3 (Intern) RADIUS-Authentifizierung für den Zugriff über WBM aktivieren. Das mGuard-Gerät muss so konfiguriert sein, dass es die RADIUS-Authentifizierung „Als einzige Methode für die Passwortauthentifizierung” zulässt.	Verwaltung >> Web-Einstellungen >> Zugriff (UM: 4.2.2)
	Maßnahme 4 (Intern/Extern) Verwalten Sie Zertifikate für die sichere Kommunikation über IPsec VPN mit externen Servern.	Authentifizierung >> Zertifikate (UM: 6.4)

	Maßnahme 5 (Intern/Extern)
	Konfigurieren Sie eine zertifikatsbasierte, sichere IPsec-VPN-Verbindung zum externen Server.
	Es dürfen nur sichere Verschlüsselungsmaßnahmen sowie sichere Verschlüsselungs- und Hash-Algorithmen verwendet werden. Diese werden im WBM gekennzeichnet und im Anwenderhandbuch beschrieben:
	
	IPsec VPN
	– ISAKMP SA (Schlüsselaustausch)
	  – Verschlüsselung: AES-256
	  – Hash/Prüfsumme: SHA-256, -384, -512
	  – Diffie-Hellman: 2048 Bit oder höher
	– IPsec-SA (Datenaustausch)
	  – Verschlüsselung: AES-256
	  – Hash/Prüfsumme: SHA-256, -384, -512
	– Perfect Forward Secrecy (PFS)
	  – 2048 Bit oder höher
		IPsec VPN >> Verbindungen (UM: 8.2, 8.2.2, 8.2.3)
		Sichere Verschlüsselung (UM: 3.1)

CR 1.1 RE2 Multifaktor-Authentifikation über alle Schnittstellen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 1.2 Identifizierung und Authentifikation von Softwareprozessen und Geräten		
SL 2	Das mGuard-Gerät ist in der Lage, sich selbst zu identifizieren und sich gegenüber jeder anderen Komponente (Software-Anwendung,	

Security-Level	Erfüllung	Links
	eingebettete Geräte, Host-Geräte und Netzwerkgeräte) zu authentifizieren.	
	Maßnahme 1 (Intern) Eine Verwendung der Protokolle SSH und SNMP ist nicht erlaubt und muss auf dem mGuard-Gerät unterbunden werden. Dazu müssen folgende Funktionen auf dem Gerät **deaktiviert** werden (**Kontrollkästchen abwählen**): – Aktiviere SSH-Fernzugang – Erlaube SSH-Zugang als Benutzer root	Verwaltung >> Systemeinstellungen >> Shell-Zugang (UM: 4.1.3)
CR 1.2 RE1 Eindeutige Identifizierung und Authentifikation		
SL 2	Die Kommunikation mit externen Komponenten, wie z. B. Remote-Authentifizierungs-, NTP- oder Syslog-Servern, muss über eine zertifikatsbasierte IPsec VPN-Verbindung erfolgen. Das mGuard-Gerät muss sich gegenüber dem externen Kommunikationspartner über X.509-Zertifikate identifizieren und authentifizieren	
	Maßnahme 2 (Intern/Extern) Verwalten Sie Zertifikate für die sichere Kommunikation über IPsec VPN mit externen Servern.	Authentifizierung >> Zertifikate (UM: 6.4)

	Maßnahme 3 (Intern/Extern)
	Konfigurieren Sie eine zertifikatsbasierte, sichere IPsec-VPN-Verbindung zum externen Server.
	Es dürfen nur sichere Verschlüsselungsmaßnahmen sowie sichere Verschlüsselungs- und Hash-Algorithmen verwendet werden. Diese werden im WBM gekennzeichnet und im Anwenderhandbuch beschrieben:
	
	IPsec VPN
	– ISAKMP SA (Schlüsselaustausch)
	  – Verschlüsselung: AES-256
	  – Hash/Prüfsumme: SHA-256, -384, -512
	  – Diffie-Hellman: 2048 Bit oder höher
	– IPsec-SA (Datenaustausch)
	  – Verschlüsselung: AES-256
	  – Hash/Prüfsumme: SHA-256, -384, -512
	– Perfect Forward Secrecy (PFS)
	  – 2048 Bit oder höher
		IPsec VPN >> Verbindungen (UM: 8.2, 8.2.2, 8.2.3)
		Sichere Verschlüsselung (UM: 3.1)

Security-Level	Erfüllung	Links
	Maßnahme 4 (Intern/Extern) Siehe CR 1.1	Siehe CR 1.1
	Maßnahme 5 (Intern/Extern) Integrieren Sie einen Remote-Syslog-Server über eine sichere IPsec-VPN-Verbindung.	Logging >> Einstellungen >> Einstellungen (UM: 11.1.1)
	Maßnahme 6 (Intern/Extern) Integrieren Sie einen Remote-NTP-Server über eine sichere IPsec-VPN-Verbindung.	Verwaltung >> Systemeinstellung >> Zeit und Datum (UM: 4.1.2)
CR 1.3 Nutzerkontenverwaltung		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. Der externe Authentifizierungsserver muss die eindeutige Identifizierung und Authentifikation jedes Benutzers vornehmen und bereitstellen. **Maßnahme 1 (Intern/Extern)** Siehe CR 1.1	Siehe CR 1.1
CR 1.4 Verwaltung der Kennungen		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. Der externe Authentifizierungsserver muss die eindeutige Identifizierung und Authentifikation jedes Benutzers vornehmen und bereitstellen. **Maßnahme 1 (Intern/Extern)** Siehe CR 1.1	Siehe CR 1.1
CR 1.5 Verwaltung der Authentifizierer		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. Der externe Authentifizierungsserver muss die eindeutige Identifizierung und Authentifikation jedes Benutzers vornehmen und bereitstellen. **Maßnahme 1 (Intern/Extern)** Siehe CR 1.1	Siehe CR 1.1

Security-Level	Erfüllung	Links
	Maßnahme 2 (Intern/Extern) Die Standardkennwörter für die auf dem Gerät vorhandenen Benutzer "admin" und "root" müssen geändert werden. Der „root“-Zugang zum mGuard-Gerät darf nicht verwendet werden. Erstellen und verwenden Sie nur sichere und komplexe Passwörter, wie vom National Institute of Standards and Technology (NIST) beschrieben (pages.nist.gov/800-63-3/sp800-63b.html).	Authentifizierung >> Administrative Benutzer (UM: 6.1)
CR 1.5 RE1 Hardwaresicherheit für Authentifizierer		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 1.7 Stärke der Authentifikation durch Passwörter		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. **Maßnahme 1 (Intern/Extern)** Siehe CR 1.1 **Maßnahme 2 (Extern)** Der externe Authentifizierungsserver muss in der Lage sein, eine konfigurierbare Passwortstärke zu erzwingen. Erstellen und verwenden Sie nur sichere und komplexe Passwörter, wie vom National Institute of Standards and Technology (NIST) beschrieben (pages.nist.gov/800-63-3/sp800-63b.html).	Siehe CR 1.1 Authentifizierung >> Administrative Benutzer (UM: 6.1)
CR 1.7 RE1 Erzeugung und Lebensdauerbeschränkungen von Passwörtern für menschliche Nutzer		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	

Security-Level	Erfüllung	Links
CR 1.8 PKI-Zertifikate		
SL 2	mGuard-Geräte unterstützen X.509v3-Zertifikate mit Public-Key-Infrastruktur (PKI) mit Zertifizierungsstelle (Certification Authority [CA]), optionaler Zertifikatssperrliste (Certificate Revocation List [CRL]) und Filtermöglichkeit nach Subjects. Die unterstützten Mechanismen sind weltweit anerkannt und bewährt. Die PKI-Unterstützung gilt u. a. für die Konfiguration von zertifikatsbasierten IPsec-VPN-Verbindungen. **Maßnahme 1 (Extern)** Die Zertifikate müssen vom Kunden (Asset Owner) erstellt und verwaltet (z. B. mithilfe von Software-Tools von Drittanbietern wie XCA [hohnstaedt.de/xca]) und auf das mGuard-Gerät hochgeladen werden. **Maßnahme 2 (Intern/Extern)** Zur Authentifizierung von Gegenstellen über X.509-Zertifikate können die erforderlichen CA- oder Gegenstellen-Zertifikate verwendet werden: – CA-Zertifikate sind Zertifikate von Zertifizierungsstellen (CA). CA-Zertifikate dienen dazu, die von Gegenstellen vorgezeigten Zertifikate auf Echtheit zu überprüfen. – Ein Gegenstellen-Zertifikat ist die Kopie des Zertifikats, mit dem sich eine Gegenstelle beim mGuard-Gerät ausweist.	Authentifizierung >> Zertifikate (UM: 6.4) Authentifizierung >> Zertifikate >> CA-Zertifikate (UM: 6.4.3)y Authentifizierung >> Zertifikate >> Gegenstellen-Zertifikat (UM: 6.4.4) Siehe CR 1.1

Security-Level	Erfüllung	Links
CR 1.9 Stärke der Authentifikation durch öffentliche Schlüssel		
SL 2	mGuard-Geräte unterstützen X.509v3-Zertifikate mit Public-Key-Infrastruktur (PKI) mit Zertifizierungsstelle (Certification Authority [CA]), optionaler Zertifikatssperrliste (Certificate Revocation List [CRL]) und Filtermöglichkeit nach Subjects. Die unterstützten Mechanismen sind weltweit anerkannt und bewährt. **Maßnahme 1 (Extern)** Die Zertifikate müssen vom Kunden (Asset Owner) erstellt und verwaltet (z. B. mithilfe von Software-Tools von Drittanbietern wie XCA [hohnstaedt.de/xca]) und auf das mGuard-Gerät hochgeladen werden. **Maßnahme 2 (Intern/Extern)** Siehe CR 1.8	Authentifizierung >> Zertifikate (UM: 6.4) Siehe CR 1.8
CR 1.9 RE1 Hardwaresicherheit für eine Authentifikation durch öffentliche Schlüssel		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 1.10 Rückmeldung vom Authentifizierer		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät verdeckt die Rückmeldung von Authenticator-Informationen während des Authentifizierungsprozesses. Dazu gehören eingegebene Kennwörter, angezeigte Fehlermeldungen und Log-Dateien.	
CR 1.11 Erfolglose Anmeldeversuche		
SL 2	Um menschliche Benutzer sicher zu authentifizieren, muss das mGuard-Gerät über das RADIUS-Protokoll eine Verbindung zu einem externen Authentifizierungsserver aufbauen. **Maßnahme 1 (Intern/Extern)** Siehe CR 1.1 **Maßnahme 2 (Extern)** Die Erkennung von ungültigen Anmeldeversuchen und die vorübergehende Sperrung von Benutzern nach einer bestimmten Anzahl von ungültigen Anmeldeversuchen muss vom externen Authentifizierungsserver vorgenommen werden. Der externe Authentifizierungsserver muss entsprechend konfiguriert werden.	Siehe CR 1.1

Security-Level	Erfüllung	Links
CR 1.12 Nutzungshinweis des Systems		
SL 2	Das mGuard-Gerät zeigt vor der Authentifizierung über WBM (HTTPS) eine konfigurierbare Systembenachrichtigung an. **Maßnahme 1 (Intern)** Die Systembenachrichtigung kann individuell angepasst werden.	Verwaltung >> Systemeinstellung >> Host (UM: 4.1.1)
CR 1.14 Stärke der Authentifikation durch symmetrische Schlüssel		
SL 2	Das mGuard-Gerät erlaubt die Verwendung von Pre-Shared Keys (PSK) zur symmetrischen Authentifizierung von VPN-Verbindungen. Darüber hinaus verwendet mGuard-Gerät keine auf symmetrischen Schlüsseln basierende Authentifizierung. **Maßnahme 1 (Intern/Extern)** Es muss gewährleistet sein, dass die „Authentizifierungsmethode“ PSK nicht für die Authentifizierung verwendet wird, insbesondere nicht bei IPsec-VPN-Verbindungen. Stattdessen müssen zur sicheren Authentifizierung X.509-Zertifikate verwendet werden. Siehe CR 1.1	Siehe CR 1.1 IPsec VPN >> Verbindungen (UM: 8.2, 8.2.2, 8.2.3)
CR 1.14 RE1 Hardwaresicherheit für eine Authentifikation durch symmetrische Schlüssel		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	

3.2 FR 2 - Nutzungskontrolle (UC)

Durchsetzung der zugewiesenen Berechtigungen, die es einem authentifizierten Nutzer (menschlicher
Nutzer, Softwareprozess oder Gerät) erlauben, die geforderten Aktionen in der Komponente durchzuführen
und die Verwendung dieser Berechtigungen zu überwachen.

Security-Level	Erfüllung	Links
CR 2.1 Durchsetzung der Autorisierung		
SL 2	Auf dem mGuard-Gerät sind die voreingestellten Rollen "admin", "root", "netadmin" und "audit" konfiguriert. Die Rollen "root" und "netadmin" dürfen nicht verwendet werden.	
CR 2.1 RE1 Durchsetzung der Autorisierung für alle Nutzer (menschliche Nutzer, Softwareprozesse und Geräte)		
SL 2	Die Durchsetzung der Autorisierung ist für alle Nutzer gegeben. Software-Prozesse verwenden die gleichen Benutzer, Authentifizierungs- und Autorisierungsmechanismen wie menschliche Benutzer.	
CR 2.1 RE2 Abbildung der Berechtigung auf Rollen		

Security-Level	Erfüllung	Links
SL 2	**Maßnahme 1 (Intern/Extern)** Die Rollen "root" und "netadmin" dürfen nicht verwendet werden. **Maßnahme 2 (Intern/Extern)** Das mGuard-Gerät muss das RADIUS-Protokoll verwenden, um sich mit einem externen Authentifizierungsserver zu verbinden. Siehe CR 1.1 **Maßnahme 3 (Intern/Extern)** Um den autorisierten Benutzern, die auf dem Authentifizierungsserver verwaltet und authentifiziert werden, Berechtigungen zuweisen zu können, muss für jede Rolle (admin und audit) mindestens ein RADIUS-Filter ("Gruppe / Filter-ID") konfiguriert werden. Auf dem Authentifizierungsserver müssen den autorisierten Benutzern die entsprechenden Gruppen-/Filter-IDs zugewiesen werden, damit sie die rollenspezifischen Berechtigungen erhalten. Folgende Berechtigungen werden realisiert: – Benutzer mit der Rolle "admin" haben auf dem Gerät Lese- und Schreibrechte. – Benutzer mit der Rolle "audit" haben auf dem Gerät nur Leserechte.	Siehe CR 1.1 Authentifizierung >> Administrative Benutzer >> RADIUS-Filter (UM: 6.1.2)
CR 2.1 RE3 Eingriff des Aufsichtspersonals		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 2.2 Nutzungskontrolle von Funkverbindungen		
SL 2	**Nicht zutreffend**. Das Gerät verwendet keine der in der Norm definierten Funk-Technologien.	

Security-Level	Erfüllung	Links
CR 2.3 Nutzungskontrolle von tragbaren und mobilen Geräten		
SL 2	**Nicht zutreffend**. Das Gerät verwendet keine der in der Norm definierten tragbaren/ mobilen Geräte.	
CR 2.5 Sitzungssperrung		
SL 2	**Wird vom Gerät automatisch erfüllt.** Im Falle eines Zugriffs über HTTPS (Web-based Management) kann die Sitzung über einen konfigurierten Timeout automatisch beendet werden (Logout nach Ablauf der Sitzung). **Maßnahme 1 (Intern)** Der Timeout für den automatische Ablauf der Sitzung ist auf einen Standardwert (30 Minuten) eingestellt und kann konfiguriert werden.	Verwaltung >> Web-Einstellungen >> Allgemein (UM: 4.2.1)
CR 2.6 Beendigung einer Fernzugriffssitzung		
SL 2	**Wird vom Gerät automatisch erfüllt.** Nach einer vordefinierten Zeit beendet das mGuard-Gerät aktive Sitzungen, die über HTTPS (Web-based Management) initiiert wurden, automatisch. **Maßnahme 1 (Intern)** Der Timeout für den automatische Ablauf der Sitzung ist auf einen Standardwert (30 Minuten) eingestellt und kann konfiguriert werden.	Verwaltung >> Web-Einstellungen >> Allgemein (UM: 4.2.1)
CR 2.7 Kontrolle gleichzeitiger Sitzungen		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die gleichzeitige Anmeldung beim Web-based Management (WBM) des Gerätes ist auf 10 Web-Sitzungen (HTTPS) begrenzt. Sobald 10 aktive Sitzungen bestehen, werden weitere Login-Versuche abgelehnt.	

Security-Level	Erfüllung	Links
CR 2.8 Prüfbare Ereignisse		
SL 2	Das Gerät erzeugt automatisch lokale sicherheitsrelevante Ereignisdatensätze (Log-Einträge). Die erzeugten Log-Einträge können vom Gerät abgerufen und an einen Syslog-Server übertragen werden. Die Log-Einträge können auch von Benutzern mit der Benutzerrolle "Audit" gelesen werden. **Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Siehe CR 1.2	Siehe CR 1.2
CR 2.9 Speicherkapazität für Ereignisdatensätze		
SL 2	**Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Siehe CR 1.2 **Maßnahme 2 (Extern)** Der externe Syslog-Server muss ausreichend Speicherkapazität bereithalten, um die erforderliche Anzahl von Log-Einträgen aufzuzeichnen.	Siehe CR 1.2
CR 2.9 RE1 Warnung, wenn die Speicherkapazität für Ereignisdatensätze erreicht ist		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	

Security-Level	Erfüllung	Links
CR 2.10 Verhalten bei Verarbeitungsfehlern von Ereignisdaten		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Verarbeitung von Ereignisdaten (Audit/Logging) des Gerätes beeinflusst die Hauptfunktion der Prozesse des Gerätes in keiner Weise negativ. Um auf dem externen Log-Server zu prüfen, ob regelmäßig Log-Einträge übertragen werden, wird ca. alle 30 Minuten ein Log-Eintrag „UPTIME“ erstellt und an den Syslog-Server gesendet. Der Log-Eintrag zeigt die jeweils aktuelle Uptime des mGuard-Gerätes (z. B. 2024-11-06_09:20:00.90770 uptime-audit: -------- UPTIME: 29 min --------)	
	Maßnahme 1 (Intern/Extern) Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Siehe CR 1.2	Siehe CR 1.2
CR 2.11 Zeitstempel		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät erstellt automatisch Zeitstempel für jedes Log-Ereignis in den zugehörigen Log-Dateien. Die im mGuard-Gerät erzeugten Zeitstempel werden mit der systemweiten Zeitquelle synchronisiert.	
CR 2.11 RE1 Zeitsynchronisierung		
SL 2	**Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss mit einem zuverlässigen NTP-Server synchronisiert werden, um die korrekte Zeit zu kennen und zu verwenden. Siehe CR 1.2	Siehe CR 1.2

Security-Level	Erfüllung	Links
CR 2.12 Nichtabstreitbarkeit		
SL 2	Das Gerät erzeugt automatisch lokale sicherheitsrelevante Ereignisdatensätze (Log-Einträge). Die An- und Abmeldung eines Benutzers sowie jede Aktion, die ein Benutzer auf dem Gerät ausführt, werden unter Nennung des Benutzernamens und der zugewiesenen Rolle in einem Log-Eintrag dokumentiert. Um festzustellen, ob ein bestimmter menschlicher Benutzer eine bestimmte Aktion auf dem mGuard-Gerät ausgeführt hat, müssen ein externer RADIUS-Server verwendet und Log-Einträge analysiert werden. **Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss einen Remote-Authentifizierungs- und einen Remote-Syslog-Server zur Authentifizierung sowie zur Speicherung und Verwaltung der erzeugten Ereignisdatensätze (Log-Einträge) verwenden. Siehe CR 1.1 und CR 1.2 **Maßnahme 2 (Extern)** Der RADIUS-Server muss so konfiguriert werden, dass jedem Benutzer mit der Fähigkeit, das mGuard-Gerät zu konfigurieren, ein eindeutiger Benutzername zugeordnet ist. **Maßnahme 3 (Intern/Extern)** Prüfen Sie die sicherheitsrelevanten Ereignisdatensätze (Log-Einträge), um von Benutzern durchgeführte Aktionen zu analysieren.	Siehe CR 1.1 Siehe CR 1.2 Logging >> Einstellungen >> Einstellungen (UM: 11.1.1)

3.3 FR 3 - Systemintegrität (SI)

Die Integrität der Komponente sicherstellen, um nicht autorisierte Manipulation oder Modifizierung zu
verhindern.

Security-Level	Erfüllung	Links
CR 3.1 Kommunikationsintegrität		
SL 2	Das mGuard-Gerät ermöglicht den Fernzugriff auf seine Konfigurationsoberfläche (WBM) über verschlüsselte SSL/HTTPS- oder VPN-Protokolle. Solche Protokolle enthalten Mechanismen zur Gewährleistung der Integrität der übertragenen Daten.	
CR 3.1 RE1 Authentifikation der Kommunikation		
SL 2	**Maßnahme 1 (Intern/Extern)** Die Kommunikation mit externen Komponenten, wie z. B. Remote-Authentifizierungs-, NTP- oder Syslog-Servern, muss über eine zertifikatsbasierte IPsec VPN-Verbindung erfolgen. Das mGuard-Gerät muss sich gegenüber dem externen Kommunikationspartner über X.509-Zertifikate identifizieren und authentifizieren. Siehe CR 1.1 und CR 1.2	Siehe CR 1.1 Siehe CR 1.2
CR 3.3 Verifikation der IT-Sicherheitsfunktionalität		
SL 2	Auf dem mGuard-Gerät ist es jederzeit möglich, den bestimmungsgemäßen Betrieb von Sicherheitsfunktionen zu überprüfen, indem Ereignisdatensätze (Log-Dateien) in Hinblick auf Konfigurationsänderungen, Anwendung von Firewall-Regeln, Anmeldeerfolg oder -misserfolg und die Nutzung von IPsec-VPN-Verbindungen analysiert werden. **Maßnahme 1 (Intern/Extern)** Die Funktionalität der mGuard-Firewall kann jederzeit getestet werden, indem ein spezielles Paket gesendet wird, das auf eine entsprechende Firewall-Regel passt, die das Paket verwirft und protokolliert. Aktivieren Sie die Funktion "Log" bei allen konfigurierten Firewall-Regeln.	
	Maßnahme 2 (Intern/Extern) Siehe CR 1.1 und CR 1.2	Siehe CR 1.1 Siehe CR 1.2

Security-Level	Erfüllung	Links
	Maßnahme 3 (Intern/Extern) Log-Dateien können im WBM des Gerätes oder auf dem externen Syslog-Server analysiert werden.	**Logging >> Logs ansehen (UM: 11.2)**
	Maßnahme 4 (Intern) Konfigurierte Firewall-Regeln können im WBM des Gerätes analysiert werden. Konfigurierte IPsec VPN-Verbindungen können im WBM des Gerätes analysiert werden. Zugangsregeln zum NTP-Server, Web-Server, SNMP-Server und SSH-Server des Gerätes können im WBM des Gerätes analysiert werden. Aktivieren Sie die Funktion "Log" bei allen konfigurierten Firewall-Regeln.	Netzwerksicherheit >> Paketfilter (UM: 7.1) IPsec VPN >> Verbindungen >> (Editieren) >> Firewall (UM: 8.2.4) Sonstige: (UM: Kap. 4.1.2, Kap. 4.1.3, Kap. 4.2.2, Kap. 4.6.1)
	Die Funktionalität von aufgebauten IPsec-VPN-Verbindungen wird im WBM und in den Log-Dateien des mGuard-Gerätes (und des Syslog-Servers) angezeigt.	IPsec VPN >> IPsec-Status (UM: 8.4)
CR 3.4 Software- und Informationsintegrität		
SL 2	Firmware-Updates werden vom Gerät unterstützt. Die Software, die per Update oder Flash-Mechanismus auf das Gerät hochgeladen wird, ist kryptografisch signiert. Die Signatur wird auf dem Gerät geprüft, um sicherzustellen, dass nur vom Hersteller freigegebene Software auf dem Gerät installiert wird. Konfigurationsprofile können auf dem Gerät erstellt, auf das Gerät hoch- und vom Gerät heruntergeladen werden. Die Konfigurationsprofile können mithilfe von Zertifikaten digital signiert werden, um die Authentizität und Integrität der Konfigurationsprofile sicherzustellen. Auf entsprechend konfigurierten Geräten ist es nur noch möglich, signierte Konfigurationsprofile, auf das Gerät hochzuladen. **Maßnahme 1 (Intern/Extern)** Die Funktion "Signierte Konfigurationsprofile aktivieren" muss aktiviert werden. Nur Konfigurationsprofile (atv-Profile und ECS-Dateien), die durch ein mGuard-Maschinenzertifikat kryptografisch signiert sind, dürfen auf das mGuard-Gerät hoch-	Verwaltung >> Konfigurationsprofile (UM: 4.5) Authentifizierung >> Zertifikate (UM: 6.4)

Security-Level	Erfüllung	Links
	bzw. heruntergeladen werden. Der Import und Export von unsignierten Konfigurationsprofilen ist nicht erlaubt.	
CR 3.4 RE1 Authentizität der Software und der Informationen		
SL 2	Firmware-Updates werden vom Gerät unterstützt. Die Software, die per Update oder Flash-Mechanismus auf das Gerät hochgeladen wird, ist kryptografisch signiert. Die Signatur wird auf dem Gerät geprüft, um sicherzustellen, dass nur vom Hersteller freigegebene Software auf dem Gerät installiert wird. Konfigurationsprofile können auf dem Gerät erstellt, auf das Gerät hoch- und vom Gerät heruntergeladen werden. Die Konfigurationsprofile können mithilfe von Zertifikaten digital signiert werden, um die Authentizität und Integrität der Konfigurationsprofile sicherzustellen. Auf entsprechend konfigurierten Geräten ist es nur noch möglich, signierte Konfigurationsprofile, auf das Gerät hochzuladen. **Maßnahme 1 (Intern/Extern)** Die Funktion "Signierte Konfigurationsprofile aktivieren" muss aktiviert werden. Nur Konfigurationsprofile (atv-Profile und ECS-Dateien), die durch ein mGuard-Maschinenzertifikat kryptografisch signiert sind, dürfen auf das mGuard-Gerät hoch- bzw. heruntergeladen werden. Der Import und Export von unsignierten Konfigurationsprofilen ist nicht erlaubt.	Verwaltung >> Konfigurationsprofile (UM: 4.5) Authentifizierung >> Zertifikate (UM: 6.4)
CR 3.4 RE2 Automatisierte Meldung von IT-Sicherheitsverstößen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 3.5 Eingabevalidierung		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Eingaben werden streng auf zulässige Werte und die minimale und maximale Länge geprüft.	

Security-Level	Erfüllung	Links
CR 3.6 Vorbestimmte Zustände der Ausgänge		
SL 2	**Maßnahme 1 (Intern/Extern)** Der Ausgang des mGuard-Gerätes darf nicht in einen Automatisierungsprozess eingebunden werden, kann aber zur Signalisierung verwendet werden.	
CR 3.7 Fehlerbehandlung		
SL 2	**Wird vom Gerät automatisch erfüllt.** Im Fehlerfall liefert das mGuard-Gerät keine Informationen, die von Angreifern für einen Angriff auf das IACS ausgenutzt werden könnten. Einzelheiten sind den Log-Einträgen zu entnehmen.	**Logging >> Logs ansehen (UM: 11.2)** Siehe CR 1.2
CR 3.8 Sitzungsintegrität		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät bietet Mechanismen zum Schutz der Integrität von Sitzungen.	
CR 3.9 Schutz von Prüfinformationen		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die auf dem Gerät gespeicherten Ereignisdatensätze (Log-Einträge) sind automatisch vor unbefugtem Zugriff, Veränderung und Löschung geschützt. Ein unbefugter Zugriff auf das Gerät ist nicht möglich – insbesondere nicht während des Betriebs, der Ruhezeit oder des Transports. Die Informationen können nur von authentifizierten Benutzern gelesen werden. **Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Siehe CR 1.2	Siehe CR 1.2

3.4 FR 4 - Vertraulichkeit der Daten (DC)

Die Vertraulichkeit der Informationen in Kommunikationskanälen und Datenspeichern wird sichergestellt, um
sich vor jeder unbefugten Offenlegung zu schützen.

Security-Level	Erfüllung	Links
CR 4.1 Vertraulichkeit von Informationen		
SL 2	Das mGuard-Gerät muss wie in diesem Dokument beschrieben konfiguriert werden. Es müssen sichere Verschlüsselungs- und Hash-Algorithmen verwendet werden (wie im mGuard-Anwenderhandbuch UM DE FW MGUARD10 / Dokument-ID: 110191_de_xx beschrieben). **Maßnahme 1 (Intern/Extern)** Die Kommunikation mit externen Komponenten, wie z. B. Remote-Authentifizierungs-, NTP- oder Syslog-Servern, muss über eine zertifikatsbasierte IPsec VPN-Verbindung erfolgen. Das mGuard-Gerät muss sich gegenüber dem externen Kommunikationspartner über X.509-Zertifikate identifizieren und authentifizieren. Siehe CR 1.1 und CR 1.2 **Maßnahme 1 (Intern)** Es müssen sichere Verschlüsselungs- und Hash-Algorithmen verwendet werden, wie im Anwenderhandbuch beschrieben.	**Sichere Verschlüsselung (UM: 3.1)**
CR 4.2 Dauerhaftigkeit von Informationen		
SL 2	**Maßnahme 1 (Intern)** Um alle Daten auf dem Gerät sicher und unwiderruflich zu löschen, muss der Smart-Mode „Das Gerät außer Betrieb nehmen (Decommissioning Mode)“ ausgeführt werden.	Siehe Anwenderhandbuch UM DE HW FL MGUARD 2000/4000 (110192_de_xx), Kapitel „Smart-Mode“ >> „Das Gerät außer Betrieb nehmen (Decommissioning Mode)“, unter phoenixcontact.com/product/<Artikelnummer>
CR 4.2 RE1 Löschen gemeinsam genutzter Speicherressourcen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	

Security-Level	Erfüllung	Links
CR 4.2 RE2 Verifikation der Löschung		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 4.3 Verwendung von Verschlüsselung		
SL 2	Das mGuard-Gerät erzwingt kryptografische Mechanismen für die Geräteverwaltung über öffentliche Netzwerke, z. B. über die Protokolle HTTPS oder VPN. **Maßnahme 1 (Intern)** Es dürfen nur sichere Verschlüsselungsmaßnahmen sowie sichere Verschlüsselungs- und Hash-Algorithmen verwendet werden. Diese werden im WBM gekennzeichnet und im Anwenderhandbuch beschrieben: – ISAKMP SA (Schlüsselaustausch) – Verschlüsselung: AES-256 – Hash/Prüfsumme: SHA-256, -384, -512 – Diffie-Hellman: 2048 Bit oder höher – IPsec-SA (Datenaustausch) – Verschlüsselung: AES-256 – Hash/Prüfsumme: SHA-256, -384, -512 – Perfect Forward Secrecy (PFS) – 2048 Bit oder höher	**Sichere Verschlüsselung (UM: 3.1)**

3.5 FR5- Eingeschränkter Datenfluss (RDF)

Das Automatisierungssystem in Zonen und Conduits aufteilen, um einen unnötigen Datenfluss zu verhindern.

Security-Level	Erfüllung	Links
CR 5.1 Netzaufteilung		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Segmentierung von Netzwerken ist eine der Kernfunktionen der mGuard-Geräte und wird über deren Router- und Firewall-Funktionalitäten umgesetzt. Mit Hilfe der vorhandenen Netzwerkschnittstellen kann die Segmentierung von Netzwerken durchgeführt werden. **Maßnahme 1 (Intern)** Die Einstellungen der Netzwerkschnittstellen können konfiguriert werden.	Netzwerk (UM: 5)
	Maßnahme 2 (Intern) Firewall-Einstellungen können konfiguriert werden.	Netzwerksicherheit >> Paketfilter (UM: 7.1)
CR 5.4 Partitionierung von Anwendungen		
SL 2	Es gibt keine Anforderungen auf Komponentenebene in Verbindung mit IEC 62443-3-3 SR 5.4	

3.6 FR 6 - Rechtzeitige Reaktion auf Ereignisse (TRE)

Auf Sicherheitsverletzungen wird reagiert, indem die zuständige Behörde informiert wird, der erforderliche
Nachweis des Verstoßes gemeldet wird und zeitnah zur Entdeckung von Vorfällen Korrekturmaßnahmen
getroffen werden.

Security-Level	Erfüllung	Links
CR 6.1 Zugriffsmöglichkeit auf Ereignisprotokolle		
SL 2	Ereignisdatensätze (Log-Einträge) können auf dem mGuard-Gerät über das Web-based Management (WBM) und auf dem Remote-Syslog-Server ausgewertet werden. **Maßnahme 1 (Intern/Extern)** Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Die gespeicherten Log-Dateien können auf dem Remote-Syslog-Server ausgewertet werden. Siehe CR 1.2	**Logging >> Logs ansehen (UM: 11.2)** Siehe CR 1.2
CR 6.1 RE1 Programmgesteuerter Zugriff auf Ereignisprotokolle		
SL 2	Ereignisdatensätze (Log-Einträge) können auf dem mGuard-Gerät über das Web-based Management (WBM) und auf dem Remote-Syslog-Server ausgewertet werden.	**Logging >> Logs ansehen (UM: 11.2)** Siehe CR 1.2
CR 6.2 Kontinuierliche Überwachung		
SL 2	**Maßnahme 1 (Intern/Extern)** Um Sicherheitsverletzungen zu erfassen, müssen die Ereignisdatensätze (Log-Einträge) analysiert werden. Ereignisdatensätze (Log-Dateien) können über das WBM des mGuard-Gerätes oder auf dem Remote-Syslog-Server ausgewertet werden.	**Logging >> Logs ansehen (UM: 11.2)**
	Maßnahme 2 (Intern/Extern) Das mGuard-Gerät muss einen Remote-Syslog-Server verwenden, um die erzeugten Ereignisdatensätze (Log-Einträge) zu speichern und zu verwalten. Ferngespeicherte Log-Dateien können auf dem Remote-Syslog-Server ausgewertet werden. Siehe CR 1.2	Siehe CR 1.2

3.7 FR 7 - Verfügbarkeit der Ressourcen (RA)

Die Verfügbarkeit der Komponenten wird bei einer Beeinträchtigung oder Blockierung wesentlicher Dienste
sichergestellt.

Security-Level	Erfüllung	Links
CR 7.1 Schutz vor Denial-of-Service-Ereignissen		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät hält wesentliche Funktionen aufrecht, wenn es aufgrund eines DoS-Ereignisses in einem beeinträchtigten Modus arbeitet. **Maßnahme 1 (Intern)** DoS-Schutz kann teilweise konfiguriert werden.	Netzwerksicherheit >> DoS-Schutz (UM: 7.3)
CR 7.1 RE1 Verwaltung der Kommunikationslast durch eine Komponente		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät hält wesentliche Funktionen aufrecht, wenn es aufgrund eines DoS-Ereignisses in einem beeinträchtigten Modus arbeitet. **Maßnahme 1 (Intern)** DoS-Schutz kann teilweise konfiguriert werden.	Netzwerksicherheit >> DoS-Schutz (UM: 7.3)
CR 7.2 Ressourcenmanagement		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät begrenzt automatisch die Nutzung von Ressourcen durch Sicherheitsfunktionen zum Schutz vor Ressourcenerschöpfung.	
CR 7.3 Datensicherung im Automatisierungssystem (Backup)		
SL 2	Die aktuelle Konfiguration des mGuard-Gerätes kann als Konfigurationsprofil (atv-Profil und ECS-Datei) gespeichert werden, das vom Gerät heruntergeladen werden kann. Diese Funktion ist unabhängig von anderen Systemfunktionen und beeinträchtigt den normalen Betrieb nicht.	Verwaltung >> Konfigurationsprofile (UM: 4.5)

Security-Level	Erfüllung	Links
CR 7.3 RE1 Verifikation der Integrität der Datensicherung		
SL 2	Importierte Konfigurationen werden streng validiert, einschließlich der Beziehungen zwischen Variablen. Konfigurationsprofile (atv-Profile und ECS-Dateien) können erstellt, verwaltet und hoch- bzw. heruntergeladen werden. Die Konfigurationsprofile können mit einem mGuard-Maschinenzertifikat kryptographisch signiert werden. Dies geschieht, um die Authentizität und Integrität der Konfigurationsprofile zu gewährleisten. **Maßnahme 1 (Intern/Extern)** Die Funktion "Signierte Konfigurationsprofile aktivieren" muss aktiviert werden. Nur Konfigurationsprofile (atv-Profile und ECS-Dateien), die durch ein mGuard-Maschinenzertifikat kryptografisch signiert sind, dürfen auf das mGuard-Gerät hoch- bzw. heruntergeladen werden. Der Import und Export von unsignierten Konfigurationsprofilen ist nicht erlaubt.	Verwaltung >> Konfigurationsprofile (UM: 4.5) Authentifizierung >> Zertifikate (UM: 6.4)
CR 7.4 Wiederherstellung des Automatisierungssystems		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das mGuard-Gerät bietet die Möglichkeit, nach einer Störung oder einem Ausfall in einen bekannten sicheren Zustand (den zuletzt gespeicherten Zustand) zurückversetzt zu werden und diesen wiederherzustellen.	
CR 7.5 Notstromversorgung		
SL 2	Es gibt keine Anforderungen auf Komponentenebene in Verbindung mit IEC 62443-3-3 SR 7.5	

Security-Level	Erfüllung	Links
CR 7.6 Netzwerk- und IT-Sicherheitseinstellungen		
SL 2	Die Firewall des mGuard-Gerätes ist so konfiguriert, dass sie den Zugriff aus nicht vertrauenswürdigen Netzwerken nicht zulässt. Der Zugriff auf das Gerät ist standardmäßig nur über die internen Netzwerkschnittstellen (LAN) möglich. Alle von außen zugänglichen Dienste können durch Firewall-Einstellungen grundsätzlich eingeschränkt werden. Standardmäßig sind nur die wichtigsten Dienste aktiviert. Bei Denial-of-Service-Angriffen (DoS-Angriffe) wird nur die Quell-IP des Angreifers zurückgewiesen, um den autorisierten Zugriff dennoch zu ermöglichen. **Maßnahme 1 (Intern/Extern)** Firewall-Einstellungen können konfiguriert werden.	Verwaltung >> Systemeinstellungen >> Zeit und Datum (UM: 4.1.2) Verwaltung >> Systemeinstellungen >> Shell-Zugang (UM: 4.1.3) Verwaltung >> Web-Einstellungen >> Zugriff (UM: 4.2.2) Verwaltung >> SNMP >> Abfrage (UM: 4.6.2)
CR 7.6 RE1 Maschinenlesbare Berichte über die momentanen IT-Sicherheitseinstellungen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
CR 7.7 Geringste Funktionalität		
SL 2	Der Zugriff auf das Gerät ist standardmäßig nur über die internen Netzwerkschnittstellen (LAN) möglich. Alle von außen zugänglichen Dienste können durch Firewall-Einstellungen grundsätzlich eingeschränkt werden. Standardmäßig sind nur die wichtigsten Dienste aktiviert. **Maßnahme 1 (Intern)** Firewall-Einstellungen können konfiguriert werden.	Verwaltung >> Systemeinstellungen >> Zeit und Datum (UM: 4.1.2) Verwaltung >> Systemeinstellungen >> Shell-Zugang (UM: 4.1.3) Verwaltung >> Web-Einstellungen >> Zugriff (UM: 4.2.2) Verwaltung >> SNMP >> Abfrage (UM: 4.6.2)

Security-Level	Erfüllung	Links
CR 7.8 Verzeichnis der Komponenten eines Automatisierungssystems		
SL 2	**Wird vom Gerät automatisch erfüllt.** Informationen über die installierte Firmware-Version des mGuard-Gerätes sowie die zugrundeliegenden Pakete werden im WBM des Gerätes angezeigt. **Maßnahme 1 (Intern)** Der Komponentenbestand des Gerätes kann analysiert werden.	Verwaltung >> Update >> Übersicht (UM: 4.4.1)

3.8 Anforderungen an Netzwerkkomponenten (NDR)

Security-Level	Erfüllung	Links
NDR 1.6 Verwaltung drahtloser Zugriffsverfahren		
SL 2	Die Anforderung entfällt, da das mGuard-Gerät über keine Funkschnittstelle verfügt.	
NDR 1.13 Zugriff über nicht vertrauenswürdige Netzwerke		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Firewall des Netzwerkgerätes ist so konfiguriert, dass sie den Zugriff aus nicht vertrauenswürdigen Netzwerken nicht zulässt. Standardmäßig ist der HTTPS-Zugriff auf das mGuard-Gerät nur über die internen Netzwerkschnittstellen (LAN) möglich. Bei Bedarf kann er für weitere, individuell eingeschränkte Netzwerke erlaubt werden. **Maßnahme 1 (Intern)** Siehe CR 7.6	Siehe CR 7.6
NDR 1.13 RE1 Ausdrückliche Genehmigung von Zugriffsanforderungen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
NDR 2.4 Mobiler Code		
SL 2	**Nicht zutreffend**. Das mGuard-Gerät verwendet keine der in der Norm definierten mobilen Code-Technologien.	
NDR 2.4 RE1 Authentizitätsprüfung von mobilen Codes		
SL 2	**Nicht zutreffend**. Das mGuard-Gerät verwendet keine der in der Norm definierten mobilen Code-Technologien.	
NDR 2.13 Nutzung von physikalischen Diagnose- und Prüfschnittstellen		
SL 2	**Wird vom Gerät automatisch erfüllt.** Das Gerät verfügt über keine physikalischen Diagnose- und Prüfschnittstellen.	
NDR 2.13 RE1 Aktive Überwachung		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	

Security-Level	Erfüllung	Links
NDR 3.2 Schutz vor Schadcodes		
SL 2	**Wird vom Gerät automatisch erfüllt.** Der gesamte ausführbare Code, der per Update oder Flash-Mechanismus auf das mGuard-Gerät geladen wird, ist kryptografisch signiert. Auf dem Linux-basierten Betriebssystem des mGuard-Gerätes werden Mechanismen, die die Ausführung von schädlichem Code einschränken oder verhindern (Härtung), eingesetzt.	
NDR 3.10 Unterstützung von Updates		
SL 2	**Wird vom Gerät automatisch erfüllt.** Firmware-Updates werden vom Gerät unterstützt.	
NDR 3.10 RE1 Authentizität und Integrität von Updates		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Update-Dateien werden kryptografisch signiert und gehasht. Dies geschieht, um die Authentizität und Integrität der Update-Dateien zu gewährleisten. **Maßnahme 1 (Intern/Extern)** Updates werden regelmäßig zur Verfügung gestellt. Die Website des Herstellers oder andere Informationsquellen müssen regelmäßig auf die Verfügbarkeit von Updates überprüft werden. Verfügbare Updates müssen so schnell wie möglich installiert werden.	

Security-Level	Erfüllung	Links
NDR 3.11 Physikalische Manipulationssicherheit und -erkennung		
SL 2	**Nicht zutreffend**. In dem vorgegebenen Sicherheitskontext hat kein unbefugtes Personal physischen Zugang zu dem Gerät. Darüber hinaus sind das Gehäuse von Hutschienengeräten und die Verpackung von PCI-Karten mit einem manipulationssicheren Siegel für den Transport vom Hersteller zur Anwendung geschützt. **Maßnahme 1 (Intern/Extern)** Vergewissern Sie sich, dass das Siegel intakt ist, bevor Sie das mGuard-Gerät in Betrieb nehmen. Im Falle einer Entfernung/Beschädigung des Siegels würden Teile des Siegels auf dem Gehäuse/der Verpackung verbleiben. Stellen Sie sicher, dass nur befugtes Personal Zugang zum Gehäuse hat.  	Siehe Anwenderhandbuch UM DE HW FL MGUARD 2000/4000 (110192_de_xx), Kapitel „Erstinbetriebnahme“, unter phoenixcontact.com/product/<Artikelnummer>
NDR 3.11 RE1 Meldung eines Manipulationsversuchs		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
NDR 3.12 Bereitstellung von Hersteller-Vertrauensankern		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die mGuard-Geräte sind mit einem öffentlichen Produktschlüssel des Herstellers ausgestattet, um z. B. die Signatur einer Update-Datei zu prüfen. Der öffentliche Schlüssel des Herstellers ist in der Firmware fest kodiert.	
NDR 3.13 Bereitstellung von Betreiber-Vertrauensankern		
SL 2	Das mGuard-Gerät kann vom Betreiber erstellte und verwaltete X.509-Zertifikate verwenden, um IPsec-VPN-Verbindungen sicher zu verschlüsseln, sich als Web-Server gegenüber einer	

Security-Level	Erfüllung	Links
	Gegenstelle zu authentifizieren und um Konfigurationsprofile kryptografisch zu signieren. Damit wird die Authentizität und Integrität von Konfigurationsprofilen, die Identifizierung des Gerätes und die verschlüsselte Kommunikation über IPsec-VPN-Verbindungen gewährleistet. **Maschinenzertifikat:** Das mGuard-Gerät authentifiziert sich gegenüber der Gegenstelle mit einem auf das mGuard-Gerät geladenen Maschinenzertifikat. Das Maschinenzertifikat dient sozusagen als „Ausweisdokument" für das mGuard-Gerät, das der Gegenstelle angezeigt wird. Konfigurationsprofile werden mit dem Maschinenzertifikat signiert. **CA-Zertifikat:** CA-Zertifikate sind Zertifikate von Zertifizierungsstellen (CA). CA-Zertifikate dienen dazu, die von Gegenstellen vorgezeigten Zertifikate auf Echtheit zu überprüfen. **Gegenstellen-Zertifikat:** Ein Gegenstellen-Zertifikat ist die Kopie des Zertifikats, mit dem sich eine Gegenstelle beim mGuard-Gerät ausweist. Die Zertifikate werden vom Kunden (Asset Owner) erstellt und verwaltet und müssen auf das mGuard-Gerät hochgeladen werden. **Maßnahme 1 (Intern/Extern)** Die Zertifikate müssen vom Betreiber (Asset Owner) erstellt und verwaltet (z. B. mithilfe von Software-Tools von Drittanbietern wie XCA [hohnstaedt.de/xca]) und auf das mGuard-Gerät hochgeladen werden.	
	Maßnahme 2 (Intern/Extern) Verwalten Sie Zertifikate, um über IPsec VPN sicher mit externen Servern zu kommunizieren, indem Sie die Roots-of-Trust des Betreibers (Asset Owner) nutzen.	Authentifizierung >> Zertifikate (UM: 6.4)
	Maßnahme 3 (Intern/Extern) Konfigurieren Sie eine zertifikatsbasierte, sichere IPsec-VPN-Verbindung zum externen Server unter Verwendung der Roots-of-Trust des Betreibers (Asset Owner) .	IPsec VPN >> Verbindungen (UM: 8.2, 8.2.2, 8.2.3)

Security-Level	Erfüllung	Links
	Maßnahme 4 (Intern/Extern) Erstellen und verwalten Sie kryptografisch signierte Konfigurationsprofile unter Verwendung der Roots-of-Trust des Betreibers (Asset Owner) .	Verwaltung >> Konfigurationsprofile (UM: 4.5)
	Maßnahme 5 (Intern/Extern) Authentifizieren Sie den Web-Server des mGuard-Gerätes gegenüber anfragenden Web-Clients über ein selbst erstelltes Maschinenzertifikat bzw. "HTTPS Server-Zertifikat" (unter Verwendung des Roots-of-Trust des Betreibers).	Verwaltung >> Web-Einstellungen >> Zugriff (UM: 4.2.2)
NDR 3.14 Integrität von Boot-Prozessen		
	Wird vom Gerät automatisch erfüllt. Während des Boot-Prozesses, bevor die Kernfunktionen des Gerätes gestartet werden und bevor ein Benutzer mit dem Gerät interagieren kann, wird die Authentizität und Integrität der Dateien des mGuard-Basissystems geprüft. Wird während des Boot-Prozesses festgestellt, dass die Authentizität und Integrität der Dateien auf dem Gerät fehlerhaft oder manipuliert sind, wird der Boot-Prozess abgebrochen. Der Fehler wird über die rot blinkende Geräte-LED PF5 angezeigt (Blink-Rhythmus 500/500 ms). Im Falle von PCI-Karten blinkt die LED FAIL im Rhythmus 500/500).	LED-Statusanzeige und Blinkverhalten (UM: 15.3)
NDR 3.14 RE1 Authentizität des Boot-Prozesses		
SL 2	**Wird vom Gerät automatisch erfüllt.** Während des Boot-Prozesses, bevor die Kernfunktionen des Gerätes gestartet werden und bevor ein Benutzer mit dem Gerät interagieren kann, wird die Authentizität und Integrität der Dateien des mGuard-Basissystems geprüft. Wird während des Boot-Prozesses festgestellt, dass die Authentizität und Integrität der Dateien auf dem Gerät fehlerhaft oder manipuliert sind, wird der Boot-Prozess abgebrochen. Der Fehler wird über die rot blinkende Geräte-LED PF5 angezeigt (Blink-Rhythmus 500/500 ms). Im Falle von PCI-Karten blinkt die LED FAIL im Rhythmus 500/500).	LED-Statusanzeige und Blinkverhalten (UM: 15.3)
NDR 5.2 Schutz der Zonengrenze		

Security-Level	Erfüllung	Links
	Der Schutz von Zonengrenzen ist eine der Hauptfunktionen des mGuard-Gerätes.	
NDR 5.2 RE1 Standardmäßig verweigern, als Ausnahme zulassen		
SL 2	**Wird vom Gerät automatisch erfüllt.** Die Standard-Firewall-Regeln lehnen jeglichen Zugriff aus einem externen (nicht vertrauenswürdigen) Netzwerk vollständig ab. **Maßnahme 1 (Intern)** Konfigurierte Firewall-Regeln sollten nur Netzwerkverkehr zulassen, der notwendig ist.	Netzwerksicherheit >> Paketfilter (UM: 7.1)
NDR 5.2 RE2 Inselbetrieb		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
NDR 5.2 RE3 Im Fehlerfall geschlossen		
SL 3	Eine Verwendung des Geräts auf Ebene SL 3 wird in diesem Dokument nicht betrachtet.	
NDR 5.3 Allgemeine Beschränkung der persönlichen Kommunikation		
SL 2	**Wird vom Gerät automatisch erfüllt.** Beschränkungen der zum allgemeinen Zweck dienlichen Kommunikation von Mensch zu Mensch werden durch die Hauptfunktionen des mGuard-Gerätes abgedeckt. **Maßnahme 1 (Intern)** Firewall-Regeln können konfiguriert werden.	Netzwerksicherheit >> Paketfilter (UM: 7.1)

Phoenix Contact GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Email: info@phoenixcontact.com
phoenixcontact.com

109049_de_04