IEC 62443-4-2-compliant configuration of the FL MGUARD product family

User Manual

User manual

IEC 62443-4-2-compliant configuration of the FL MGUARD product family

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

This manual is valid for:

Please observe the associated manuals for the listed items (documents: 110191_en_xx, 110192_en_xx, 110193_en_xx). The manuals and further user documentation can be found at phoenixcontact.com. Enter one of the item numbers listed here in the search field.

Designation	Item No.
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_en_04

Phoenix Contact GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 Introduction

In order to comply with the IEC 62443 standard, several requirements must be met at different levels. A level refers to the devices that are to be used in an IEC 62443 environment.

This document describes how mGuard devices running at least the mGuard 10.5 firmware must be configured, as well as organizational measures to meet the requirements of the IEC 62443-4-2 standard.

The mGuard 10 firmware was developed using the IEC 62443-4-1 certified “PxCCS Development Process” of PHOENIX CONTACT Cyber Security GmbH.

1.1 What does the IEC 62443-4-2 standard stand for?

The IEC 62443-4-2 standard defines security requirements for components used in industrial automation and control systems (IACS).

These requirements are called **component requirements (CR)** and are closely related to the **system requirements (SR)** that are defined in IEC 62443-3-3. Both CR and SR are technical requirements derived from the overarching definition of the seven **foundational requirements (FR)** defined in IEC 62443-1-1.

Foundational requirements (FR):

1. Identification and authentication control (IAC)
2. Use control (UC)
3. System integrity (SI)
4. Data confidentiality (DC)
5. Restricted data flow (RDF)
6. Timely response to events (TRE)
7. Resource availability (RA)

Individual component requirements (CR) are assigned to the foundational requirements in the IEC 62443-4-2 standard. Fulfillment of the component requirements (CR) and any associated enhancements (requirement enhancements [RE]) leads to classification in one of four security levels (SL).

The degree of fulfillment of the component requirements (CR) thus expresses the ability of a component to be used in an IACS with a certain security level (SL).

It is important to note that components of an automation system can also be combined such that the overall system meets the desired system requirements (SR) in order to achieve a certain security level in accordance with IEC 62443-3-3.It is therefore not necessary for each individual component to achieve the desired security level (SL) for each CR.

1.2 What is a security level?

Security levels (SL) reflect the countermeasures required to prevent certain security risks. Four security levels SL 1 to SL 4 are defined that can be fulfilled by individual security measures. These measures are described in the sections Security context/ security concept and Configuring mGuard devices.

The associated four SLs are defined in the IEC 62443-4-2 standard as follows:

- SL 1: Prevent unauthorized disclosure of information through interception or accidental discovery.
- SL 2: Prevent unauthorized disclosure of information to an entity actively seeking it using simple means with few resources, general skills, and low motivation.
- SL 3: Prevent the unauthorized disclosure of information to an entity actively seeking it using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.
- SL 4: Prevent unauthorized disclosure of information to an entity actively seeking it using sophisticated means with extensive resources, IACS-specific skills, and high motivation.

1.3 Who is the target group of IEC 62443-4-2?

Primarily operators, system integrators, and manufacturers working in automation technology.
System integrators can easily determine which components can be used to achieve certain security levels. Manufacturers receive support in deciding which individual components can be combined in an automation system in order to achieve a certain security level for the overall system.

2 Security context/security concept

2.1 Security concept

In order to achieve reliable security, the defense-in-depth design of automation systems is an important measure in the design and implementation of a process based on the IEC 62443 series of standards.

The implementation of defense-in-depth measures leads to a security architecture in which security is built up in several layers.

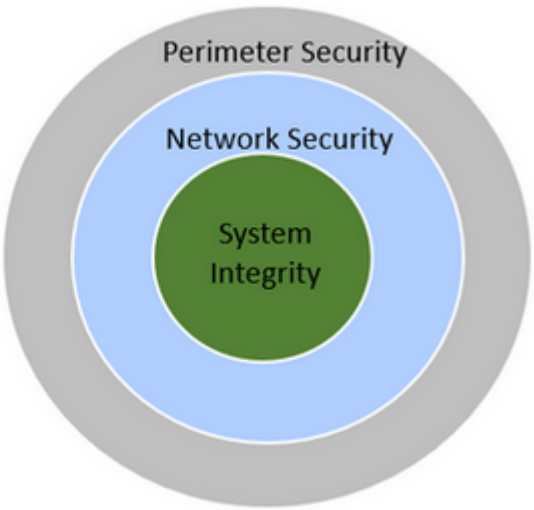
The result is a generic layer architecture that leads to a fully segmented structure for the network layer.The security context (mGuard) describes the security architecture and use cases of mGuard devices.

The mGuard security context results from the combination of technological and organizational measures that together implement the requirements of the IEC 62443-4-2 standard and the philosophy of an integrated security approach.

2.1.1 The defense-in-depth concept

A general defense-in-depth concept consists of three layers:

Figure 2-1 Defense-in-depth concept



2.1.1.1 Perimeter security

Perimeters are the outer boundaries of the network that are protected by physical measures such as fences, doors, physical access control, etc.

2.1.1.2 Network security

This layer contains the company or office zone and a service management zone that are protected by known IT security concepts.

2.1.1.3 System integrity

This layer contains OT devices and applications that are to be protected by IEC 62443 concepts.

2.1.1.4 Phoenix Contact Industrial Security Guideline

The increasing interconnection of systems, components, and devices as well as the growing amount of data to be transmitted and stored result in a higher risk of cyberattacks.

The logical consequence of this must be a high prioritization of the best possible protection against cyberattacks, threats, and misuse or incorrect use and manipulation of data.

Further general information on cybersecurity can be found in the Phoenix Contact Industrial Security Guideline at:

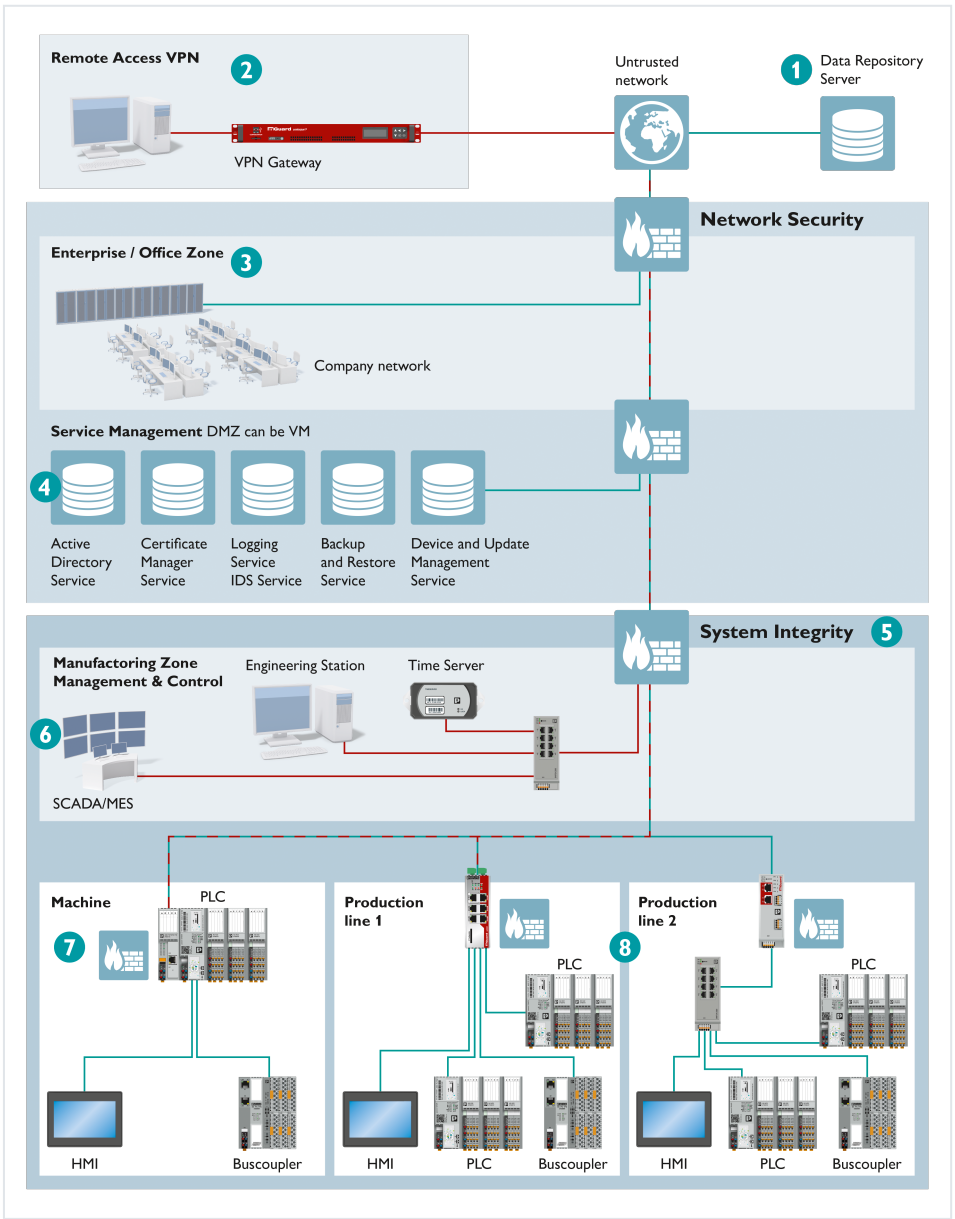
security.plcnext.help/se/Industrial_Security_Guideline/Security_Intro.htm

2.2 Security context (mGuard)

In order to meet the requirements defined in the IEC 62443 series of standards, the device (mGuard) must be used in the intended use cases resulting from the defined security context (use cases). The following figure shows the general security context:

– Blue-green connections represent security mechanisms (e.g., HTTPS).
– Red connections represent virtual private networks (VPNs).

Figure 2-2 The mGuard security concept



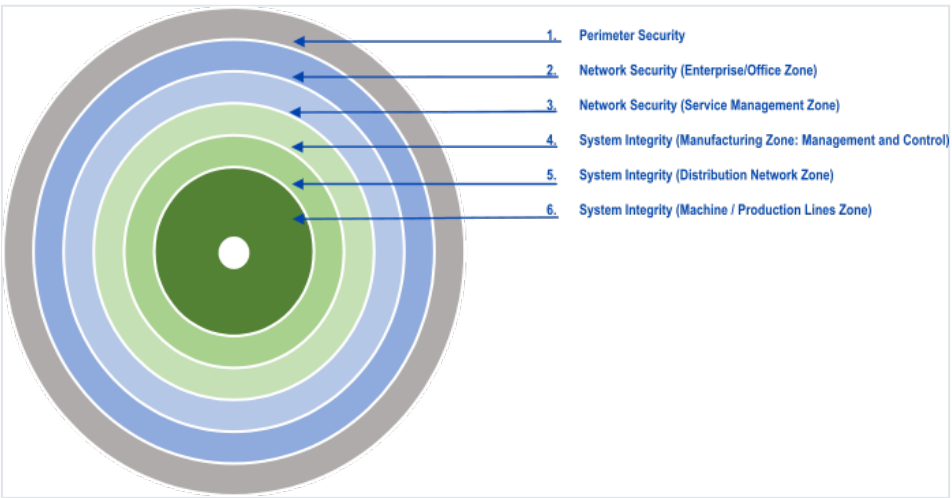
The various levels (zones and lines) are identified by numbers:

Number	Description	Details
1	**Data repository server**	Provides data for patch management/asset management.
2	**VPN server**	Remote maintenance access via VPN
3	**Office zone**	Factory IT, enterprise resource planning (ERP) systems, production control systems. Protected by firewall
4	**Service management zone**	This zone can be regarded as a demilitarized zone (DMZ), as it decouples the ICS networks (zones 5 to 7) from the external network by strictly controlling the flow of information. All communication between the external network and the ICS network must pass through this zone. Implements central user management, patch/update management, and logging. It contains the following infrastructure: • Active Directory/RADIUS server or LDAP server for authentication purposes • Firewall or VPN component (e.g., implemented as a “jump host”) that handles communication with the other zones (conduits)
5	**System integrity**	Factory OT, consisting of zones 6 to 8
6	**Manufacturing zone**	Management, monitoring, and control of the main process and subprocesses. Implements SCADA, time synchronization, and engineering. This zone is made up as follows: • Control center (SCADA = Supervisory Control and Data Acquisition) • NTP server that provides a GPS-based time base for the other devices involved • Ethernet switch • Engineering system (e.g., PLCnext Engineer) • Firewall that handles communication with the other zones (conduits)

7	**Machine level**	Main process that collects and processes the data of the process and the subprocesses. This zone is structured as follows: • PLCnext Control with I/O devices • A firewall and VPN server that handle communication with the other zones (conduits) are integrated into the controller • HMI for control and visualization purposes • Bus coupler
8	**Production line subprocess level**	Executes a specific automation function in a peripheral unit (remote station). This zone is made up as follows: • PLCnext Control, each with decentralized I/O devices connected to the fieldbus • HMI for control and visualization • Ethernet switch • VPN-integrated firewall and/or VPN server **(mGuard security appliance**) that handles communication with the other zones (conduits) • Bus coupler

The mGuard security context is based on the defense-in-depth concept and offers six security levels (zones/conduits):

Figure 2-3 Defense-in-depth concept (security levels)



Perimeter security – the outer layer

Access protection for the company network through the following measures:

- Physical isolation
- Digital isolation through network segmentation
- Logical access controls
- Use of specially configured firewalls. The specified firewall must correspond to the identified threats and vulnerabilities
- VPN or other security measures for remote access
- Documentation of all remote access points

Network security layers

Protection of the factory network, consisting of the company network zone and the service management zone, which is regarded as a demilitarized zone (DMZ). Possible measures are:

- Identification of all network devices and hosts
- Analysis of logs/traffic
- Verification of wireless communication/traffic
- Analysis of switch/router configurations

Measures in the DMZ:

- OS check for vulnerabilities
- OS patch management
- Preventing the use of USB or removable media in the control room
- Restriction of connection to external computers

System integrity – the inner layers

Measures for SCADA applications:

- Monitoring the network for plain-text transmission and use of encryption
- Ensuring the use of individual user accounts
- Restricted access to the desktop

Measures for control subnetworks at machine/production line level (main process and subprocesses):

- Wired vs. wireless communication
- Ethernet vs. serial communication
- Recording of data traffic on Ethernet connections

Measures for field controls:

- Ethernet vs. serially connected devices
- Ethernet devices tested for vulnerabilities in the laboratory
- Manufacturer’s default passwords removed

2.2.1 Security context (use cases)

The mGuard security routers are designed for zone protection in production facilities. They can be used to separate production cells or automation cells from the production network in the system integrity layer. See the red outline in the previous figure.

To meet the requirements, organizational measures and local/internal settings on the mGuard device as well as settings on external supporting systems are required.

The following measures are mandatory in order to meet the requirements specified in the IEC 62443-4-2 standard.

2.2.1.1 Organizational measures

1. The mGuard device must be configured by personnel who have been trained in security and the requirements of the IEC 62443-4-2 standard.
2. Protected by the perimeter, the mGuard device must be installed in a restricted-access control cabinet in the production plant to which only qualified personnel have access.
3. The use and configuration of the mGuard device are aimed exclusively at users who are familiar with the relevant security concepts of automation technology and the applicable standards and other regulations, in particular the IEC 62443 series of standards.
4. The higher-level networks must be secured in accordance with the defense-in-depth principle and the requirements of the IEC 62443 series of standards.
5. The mGuard device must not be used for process control.

2.2.1.2 Internal measures that are only configured on the device

6. Access to the mGuard device via the SSH and SNMP protocols must be disabled. Only human users may log in to web-based management (WBM) of the device.
7. The “root” access to the device must not be used. Only users with the user roles “admin” and “audit” may log in to the device.
8. Only configuration profiles that are cryptographically signed by an mGuard machine certificate may be downloaded from or uploaded to the mGuard device.

2.2.1.3 Internal and external measures in relation to external support systems

9. An external or remote authentication server must be used. The mGuard device uses the external authentication server as a client for authentication. It is up to the customer to decide which available and suitable authentication server is used and operated.
   The authentication server must provide at least the following functions:

- Detection of invalid login attempts
- Temporary locking out of users after a certain number of invalid login attempts

10. A remote log server (syslog server) must be used. The remote log files must be continuously evaluated.
11. To connect the mGuard device to external authentication, NTP, and syslog servers, certificate-based IPsec VPN connections must be used.
    1. The use of pre-shared keys (PSK) in these VPN connections is not permitted.
    2. The use of weak encryption and hash algorithms in these VPN connections is not permitted.The following encryption and hash algorithms must be used as a minimum:AES-256/SHA-512/Diffie-Hellman = 2048 bits or higher/PFS = 2048 bits or higher

3 Configuring mGuard devices

In order to meet the requirements defined in the IEC 62443-4-2 standard, the device must be used in the intended use cases resulting from the defined security context (see Security context). For this purpose, several functions of the device (mGuard) require clear and compulsory configuration in accordance with certain specifications.
The following sections will guide you through the requirements and describe which settings must be made on the mGuard device in order to meet the requirements in accordance with IEC 62443-4-2.

The document refers both to the web-based management menu (WBM menu), in which the settings are made, and to the corresponding sections in the user documentation.References to the corresponding sections in the mGuard user manual “Web-based management”
(110191_en_xx) have been added --> (UM:<section>).
The user manual (UM EN MGUARD10/document ID: 110191_en_xx) and further documentation are available for download in the Phoenix Contact Web Shop at phoenixcontact.net/product/1357875 in the “Download --> Manual” section.

3.1 FR 1 – Identification and authentication control (IAC)

Identify and authenticate all users (human users, software processes, and devices) before
they are granted access to the system or equipment.

Security-Level	Fulfillment	Links
CR 1.1Human user identification and authentication		
SL 2	In order to securely authenticate human users when they log in to web-based management (WBM), the mGuard device must establish a connection to an external authentication server using the RADIUS protocol.	
	Measure 1 (internal) Login via SSH and SNMP is not permitted and must be prevented on the mGuard device.To do this, the following functions must be **disabled** on the device**(deselect check boxes**): – Enable SSH remote access – Allow SSH login as user root	Management >> System Settings >> Shell Access (UM: 4.1.3)
CR 1.1 RE1 Unique identification and authentication		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. The external authentication server must carry out and provide the unique	

Security-Level	Fulfillment	Links
	identification and authentication of each user.	
	Measure 2 (internal/external) Integrate an external authentication server.	Authentication >> RADIUS (UM: 6.3)
	Measure 3 (internal) Activate RADIUS authentication for access via WBM. The mGuard device must be configured to allow RADIUS authentication “As only method for password authentication”.	Management >> Web Settings >> Access (UM: 4.2.2)
	Measure 4 (internal/external) Manage certificates for secure communication via IPsec VPN with external servers.	Authentication >> Certificates (UM: 6.4)

	Measure 5 (internal/external)
	Configure a certificate-based, secure IPsec VPN connection to the external server.
	Only secure encryption measures and secure encryption and hash algorithms may be used. These are identified in WBM and described in the user manual:
	
	IPsec VPN
	– ISAKMP SA (Key Exchange)
	  – Encryption: AES-256
	  – Hash/checksum: SHA-256, -384, -512
	  – Diffie-Hellman: 2048 bit or higher
	– IPsec SA (Data Exchange)
	  – Encryption: AES-256
	  – Hash/checksum: SHA-256, -384, -512
	– Perfect Forward Secrecy (PFS)
	  – 2048 bit or higher
		IPsec VPN >> Connections (UM: 8.2, 8.2.2, 8.2.3)
		Secure encryption (UM: 3.1)

CR 1.1 RE2 Multifactor authentication for all interfaces		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 1.2 Software process and device identification and authentication		
SL 2	The mGuard device is able to identify itself and authenticate itself to every other component (software application, embedded devices, host devices, and network devices).	

Security-Level	Fulfillment	Links
	Measure 1 (internal) Use of the SSH and SNMP protocols is not permitted and must be prevented on the mGuard device.To do this, the following functions must be **disabled** on the device**(deselect check boxes**): – Enable SSH remote access – Allow SSH login as user root	Management >> System Settings >> Shell Access (UM: 4.1.3)
CR 1.2 RE1 Unique identification and authentication		
SL 2	Communication with external components, such as remote authentication, NTP, or syslog servers, must take place via a certificate-based IPsec VPN connection. The mGuard device must identify and authenticate itself to the external communication partner using X.509 certificates	
	Measure 2 (internal/external) Manage certificates for secure communication via IPsec VPN with external servers.	Authentication >> Certificates (UM: 6.4)

	Measure 3 (internal/external)
	Configure a certificate-based, secure IPsec VPN connection to the external server.
	Only secure encryption measures and secure encryption and hash algorithms may be used. These are identified in WBM and described in the user manual:
	
	IPsec VPN
	– ISAKMP SA (Key Exchange)
	  – Encryption: AES-256
	  – Hash/checksum: SHA-256, -384, -512
	  – Diffie-Hellman: 2048 bit or higher
	– IPsec SA (Data Exchange)
	  – Encryption: AES-256
	  – Hash/checksum: SHA-256, -384, -512
	– Perfect Forward Secrecy (PFS)
	  – 2048 bit or higher
		IPsec VPN >> Connections (UM: 8.2, 8.2.2, 8.2.3)
		Secure encryption (UM: 3.1)

Security-Level	Fulfillment	Links
	Measure 4 (internal/external) See CR 1.1	See CR 1.1
	Measure 5 (internal/external) Integrate a remote syslog server via a secure IPsec VPN connection.	Logging >> Settings >> Settings (UM: 11.1.1)
	Measure 6 (internal/external) Integrate a remote NTP server via a secure IPsec VPN connection.	Management >> System Settings >> Time and Date (UM: 4.1.2)
CR 1.3 Account management		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. The external authentication server must carry out and provide the unique identification and authentication of each user. **Measure 1 (internal/external)** See CR 1.1	See CR 1.1
CR 1.4 Identifier management		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. The external authentication server must carry out and provide the unique identification and authentication of each user. **Measure 1 (internal/external)** See CR 1.1	See CR 1.1
CR 1.5 Authenticator management		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. The external authentication server must carry out and provide the unique identification and authentication of each user. **Measure 1 (internal/external)** See CR 1.1	See CR 1.1

Security-Level	Fulfillment	Links
	Measure 2 (internal/external) The default passwords for the users “admin” and “root” on the device must be changed. The “root” access to the mGuard device must not be used. Create and use only secure and complex passwords as described by the National Institute of Standards and Technology (NIST) (pages.nist.gov/800-63-3/sp800-63b.html).	Authentication >> Administrative Users (UM: 6.1)
CR 1.5 RE1 Hardware security for authenticators		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 1.7 Strength of password-based authentication		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. **Measure 1 (internal/external)** See CR 1.1 **Measure 2 (external)** The external authentication server must be able to enforce a configurable password strength. Create and use only secure and complex passwords as described by the National Institute of Standards and Technology (NIST) (pages.nist.gov/800-63-3/sp800-63b.html).	See CR 1.1 Authentication >> Administrative Users (UM: 6.1)
CR 1.7 RE1 Password generation and lifetime restrictions for human users		
SL 3	Use of the device at SL 3 level is not considered in this document.	

Security-Level	Fulfillment	Links
CR 1.8 Public key infrastructure certificates		
SL 2	mGuard devices support X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and filtering option by subject. The supported mechanisms are recognized and proven worldwide. PKI support applies, e.g., to the configuration of certificate-based IPsec VPN connections. **Measure 1 (external)** The certificates must be created and managed by the customer (asset owner) (e.g., using third-party software tools such as XCA [hohnstaedt.de/xca]) and uploaded to the mGuard device. **Measure 2 (internal/external)** The required CA or remote certificates can be used to authenticate peers via X.509 certificates: – CA certificates are certificates issued by a certification authority (CA). CA certificates are used to verify the authenticity of certificates shown by peers. – A remote certificate is a copy of the certificate with which a peer identifies itself to the mGuard device.	Authentication >> Certificates (UM: 6.4) Authentication >> Certificates >> CA Certificates (UM: 6.4.3) Authentication >> Certificates >> Remote Certificates (UM: 6.4.4) See CR 1.1
CR 1.9 Strength of public key-based authentication		
SL 2	mGuard devices support X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and filtering option by subject. The supported mechanisms are recognized and proven worldwide. **Measure 1 (external)** The certificates must be created and managed by the customer (asset owner) (e.g., using third-party software tools such as XCA [hohnstaedt.de/xca]) and uploaded to the mGuard device. **Measure 2 (internal/external)** See CR 1.8	Authentication >> Certificates (UM: 6.4) See CR 1.8

Security-Level	Fulfillment	Links
CR 1.9 RE1 Hardware security for public key-based authentication		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 1.10 Authenticator feedback		
SL 2	**Automatically met by the device.** The mGuard device obscures feedback of authenticator information during the authentication process. This includes entered passwords, displayed error messages, and log files.	
CR 1.11 Unsuccessful login attempts		
SL 2	To securely authenticate human users, the mGuard device must establish a connection to an external authentication server using the RADIUS protocol. **Measure 1 (internal/external)** See CR 1.1 **Measure 2 (external)** The detection of invalid login attempts and the temporary locking out of users after a certain number of invalid login attempts must be carried out by the external authentication server. The external authentication server must be configured accordingly.	See CR 1.1
CR 1.12 System use notification		
SL 2	The mGuard device displays a configurable system notification before authentication via WBM (HTTPS). **Measure 1 (internal)** The system notification can be customized.	Management >> System Settings >> Host (UM: 4.1.1)

Security-Level	Fulfillment	Links
CR 1.14 Strength of symmetric key-based authentication		
SL 2	The mGuard device allows the use of pre-shared keys (PSK) for symmetric authentication of VPN connections.In addition, the mGuard device does not use authentication based on symmetric keys. **Measure 1 (internal/external)** It must be ensured that the “authentication method” PSK is not used for authentication, especially not for IPsec VPN connections. Instead, X.509 certificates must be used for secure authentication. See CR 1.1	See CR 1.1 IPsec VPN >> Connections (UM: 8.2, 8.2.2, 8.2.3)
CR 1.14 RE1 Hardware security for symmetric key-based authentication		
SL 3	Use of the device at SL 3 level is not considered in this document.	

3.2 FR 2 – Use control (UC)

Enforcement of the assigned permissions that allow an authenticated user (human user, software process, or device) to perform the required actions in the component and monitor the use of these permissions.

Security-Level	Fulfillment	Links
CR 2.1 Authorization enforcement		
SL 2	The default roles “admin”, “root”, “netadmin”, and “audit” are configured on the mGuard device.The roles “root” and “netadmin” must not be used.	
CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)		
SL 2	Authorization is enforced for all users. Software processes use the same user, authentication mechanisms, and authorization mechanisms as human users.	

Security-Level	Fulfillment	Links
CR 2.1 RE2 Permission mapping to roles		
SL 2	**Measure 1 (internal/external)** The roles “root” and “netadmin” must not be used. **Measure 2 (internal/external)** The mGuard device must use the RADIUS protocol to connect to an external authentication server. See CR 1.1 **Measure 3 (internal/external)** In order to be able to assign permissions to the authorized users who are managed and authenticated on the authentication server, at least one RADIUS filter (“Group/Filter ID”) must be configured for each role (admin and audit). The authorized users must be assigned the corresponding group/filter IDs on the authentication server such that they receive the role-specific permissions. The following permissions are implemented: – Users with the “admin” role have read and write access to the device. – Users with the “audit” role only have read-only access to the device.	See CR 1.1 Authentication >> Administrative Users >> RADIUS Filters (UM: 6.1.2)
CR 2.1 RE3 Supervisor override		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 2.2 Wireless use control		
SL 2	**Not applicable**. The device does not use any of the wireless technologies defined in the standard.	
CR 2.3 Use control for portable and mobile devices		
SL 2	**Not applicable**. The device does not use any of the portable/mobile devices defined in the standard.	

Security-Level	Fulfillment	Links
CR 2.5 Session lock		
SL 2	**Automatically met by the device.** In the case of access via HTTPS (web-based management), the session can be terminated automatically via a configured timeout (logout after the session has ended). **Measure 1 (internal)** The timeout for the automatic termination of the session is set to a default value (30 minutes) and can be configured.	Management >> Web Settings >> General (UM: 4.2.1)
CR 2.6 Remote session termination		
SL 2	**Automatically met by the device.** After a predefined time, the mGuard device automatically terminates active sessions that were initiated via HTTPS (web-based management). **Measure 1 (internal)** The timeout for the automatic termination of the session is set to a default value (30 minutes) and can be configured.	Management >> Web Settings >> General (UM: 4.2.1)
CR 2.7 Concurrent session control		
SL 2	**Automatically met by the device.** Simultaneous login to the device's web-based management (WBM) is limited to 10 web sessions (HTTPS).As soon as there are 10 active sessions, further login attempts will be rejected.	

Security-Level	Fulfillment	Links
CR 2.8 Auditable events		
SL 2	The device automatically generates local security-relevant event data records (log entries). The generated log entries can be retrieved from the device and transmitted to a syslog server.The log entries can also be read by users with the “audit” user role. **Measure 1 (internal/external)** The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries). See CR 1.2	See CR 1.2
CR 2.9 Audit storage capacity		
SL 2	**Measure 1 (internal/external)** The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries). See CR 1.2 **Measure 2 (external)** The external syslog server must have sufficient storage capacity to record the required number of log entries.	See CR 1.2
CR 2.9 RE1 Warn when audit record storage capacity threshold reached		
SL 3	Use of the device at SL 3 level is not considered in this document.	

Security-Level	Fulfillment	Links
CR 2.10 Response to audit processing failures		
SL 2	**Automatically met by the device.** The processing of the device's event data (audit/logging) in no way negatively affects the main function of the device's processes. To check on the external log server whether log entries are transmitted regularly, an "UPTIME" log entry is created approximately every 30 minutes and sent to the syslog server. The log entry shows the current uptime of the mGuard device (e.g., 2024-11-06_09:20:00.90770 uptime-audit: -------- UPTIME: 29 min --------)	
	Measure 1 (internal/external) The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries). See CR 1.2	See CR 1.2
CR 2.11 Timestamps		
SL 2	**Automatically met by the device.** The mGuard device automatically creates time stamps for each log event in the associated log files. The time stamps generated in the mGuard device are synchronized with the system-wide time source.	
CR 2.11 RE1 Time synchronization		
SL 2	**Measure 1 (internal/external)** The mGuard device must be synchronized with a reliable NTP server in order to know and use the correct time. See CR 1.2	See CR 1.2

Security-Level	Fulfillment	Links
CR 2.12 Non-repudiation		
SL 2	The device automatically generates local security-relevant event data records (log entries). The login and logout of a user and every action that a user performs on the device are documented in a log entry, stating the user name and the assigned role. To determine whether a specific human user has performed a specific action on the mGuard device, an external RADIUS server must be used and log entries analyzed. **Measure 1 (internal/external)** The mGuard device must use a remote authentication server and a remote syslog server for authentication and for storing and managing the generated event data records (log entries). See CR 1.1 and CR 1.2 **Measure 2 (external)** The RADIUS server must be configured such that each user with the ability to configure the mGuard device is assigned a unique user name. **Measure 3 (internal/external)** Check the security-relevant event data records (log entries) to analyze actions performed by users.	See CR 1.1 See CR 1.2 Logging >> Settings >> Settings (UM: 11.1.1)

3.3 FR 3 – System integrity (SI)

Ensure the integrity of the component to prevent unauthorized manipulation or modification.

Security-Level	Fulfillment	Links
CR 3.1 Communication integrity		
SL 2	The mGuard device allows remote access to its configuration interface (WBM) via encrypted SSL/HTTPS or VPN protocols. Such protocols contain mechanisms to ensure the integrity of the transmitted data.	
CR 3.1 RE1 Communication authentication		
SL 2	**Measure 1 (internal/external)** Communication with external components, such as remote authentication, NTP, or syslog servers, must take place via a certificate-based IPsec VPN connection. The mGuard device must identify and authenticate itself to the external communication partner using X.509 certificates. See CR 1.1 and CR 1.2	See CR 1.1 See CR 1.2
CR 3.3 Security functionality verification		
SL 2	It is possible to verify the intended operation of security functions on the mGuard device at any time by analyzing event data records (log files) with regard to configuration changes, application of firewall rules, login success or failure, and the use of IPsec VPN connections. **Measure 1 (internal/external)** The functionality of the mGuard firewall can be tested at any time by sending a special packet that matches a corresponding firewall rule, which discards and logs the packet. Activate the “Log” function for all configured firewall rules.	
	Measure 2 (internal/external) See CR 1.1 and CR 1.2	See CR 1.1 See CR 1.2

Security-Level	Fulfillment	Links
	Measure 3 (internal/external) Log files can be analyzed in the device's WBM or on the external syslog server.	**Logging >> Browse Local Logs (UM: 11.2)**
	Measure 4 (internal) Configured firewall rules can be analyzed in the device's WBM. Configured IPsec VPN connections can be analyzed in the device's WBM. Access rules to the NTP server, web server, SNMP server, and SSH server of the device can be analyzed in WBM of the device. Activate the "Log" function for all configured firewall rules.	Network Security >> Packet Filter (UM: 7.1) IPsec VPN >> Connections >> (Edit) >> Firewall (UM: 8.2.4) Other: (UM: 4.1.2, 4.1.3, 4.2.2, 4.6.1)
	The functionality of established IPsec VPN connections is displayed in WBM and in the log files of the mGuard device (and the syslog server).	IPsec VPN >> IPsec Status (UM: 8.4)

Security-Level	Fulfillment	Links
CR 3.4 Software and information integrity		
SL 2	Firmware updates are supported by the device. The software that is uploaded to the device via an update or flash mechanism is cryptographically signed. The signature is checked on the device to ensure that only software approved by the manufacturer is installed on the device. Configuration profiles can be created on the device, uploaded to the device, and downloaded from the device.The configuration profiles can be digitally signed using certificates to ensure the authenticity and integrity of the configuration profiles. On devices configured accordingly, it is only possible to upload signed configuration profiles to the device. **Measure 1 (internal/external)** The “Enable signed configuration profiles” function must be enabled. Only configuration profiles (atv profiles and ECS files) that are cryptographically signed by an mGuard machine certificate may be uploaded to or downloaded from the mGuard device.The import and export of unsigned configuration profiles is not permitted.	Management >> Configuration Profiles (UM: 4.5) Authentication >> Certificates (UM: 6.4)
CR 3.4 RE1 Authenticity of software and information		
SL 2	Firmware updates are supported by the device. The software that is uploaded to the device via an update or flash mechanism is cryptographically signed. The signature is checked on the device to ensure that only software approved by the manufacturer is installed on the device. Configuration profiles can be created on the device, uploaded to the device, and downloaded from the device.The configuration profiles can be digitally signed	Management >> Configuration Profiles (UM: 4.5) Authentication >> Certificates (UM: 6.4)

Security-Level	Fulfillment	Links
	using certificates to ensure the authenticity and integrity of the configuration profiles. On devices configured accordingly, it is only possible to upload signed configuration profiles to the device. **Measure 1 (internal/external)** The “Enable signed configuration profiles” function must be enabled. Only configuration profiles (atv profiles and ECS files) that are cryptographically signed by an mGuard machine certificate may be uploaded to or downloaded from the mGuard device.The import and export of unsigned configuration profiles is not permitted.	
CR 3.4 RE2 Automated notification of integrity violations		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 3.5 Input validation		
SL 2	**Automatically met by the device.** The entries are strictly checked for permissible values and the minimum and maximum length.	
CR 3.6 Deterministic output		
SL 2	**Measure 1 (internal/external)** The mGuard device output must not be integrated into an automation process, but can be used for signaling.	
CR 3.7 Error handling		
SL 2	**Automatically met by the device.** In the event of an error, the mGuard device does not provide any information that could be exploited by attackers to attack the IACS. Details can be found in the log entries.	**Logging >> Browse Local Logs (UM: 11.2)** See CR 1.2

Security-Level	Fulfillment	Links
CR 3.8 Session integrity		
SL 2	**Automatically met by the device.** The mGuard device offers mechanisms to protect the integrity of sessions.	
CR 3.9 Protection of audit information		
SL 2	**Automatically met by the device.** The event data records (log entries) stored on the device are automatically protected against unauthorized access, modification, and deletion. Unauthorized access to the device is not possible – especially not during operation, rest periods, or transport. The information can only be read by authenticated users. **Measure 1 (internal/external)** The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries). See CR 1.2	See CR 1.2

3.4 FR 4 – Data confidentiality (DC)

The confidentiality of information on communication channels and data storage systems is ensured in order to
protect against unauthorized disclosure.

Security-Level	Fulfillment	Links
CR 4.1 Information confidentiality		
SL 2	The mGuard device must be configured as described in this document. Secure encryption and hash algorithms must be used (as described in the mGuard user manual UM EN FW MGUARD10/ document ID: 110191_en_xx). **Measure 1 (internal/external)** Communication with external components, such as remote authentication, NTP, or syslog servers, must take place via a certificate-based IPsec VPN connection. The mGuard device must identify and authenticate itself to the external communication partner using X.509 certificates. See CR 1.1 and CR 1.2 **Measure 1 (internal)** Secure encryption and hash algorithms must be used as described in the user manual.	**Secure encryption (UM: 3.1)**
CR 4.2 Information persistence		
SL 2	**Measure 1 (internal)** To securely and irrevocably delete all data on the device, the Smart mode “Taking the device out of operation (Decommissioning Mode)” must be executed.	See user manual UM EN HW FL MGUARD 2000/4000 (110192_en_xx), Section “Smart mode” >> “Taking the device out of operation (Decommissioning Mode)”, at phoenixcontact.com/ product/<item number>
CR 4.2 RE1 Erase of shared memory resources		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 4.2 RE2 Erase verification		
SL 3	Use of the device at SL 3 level is not considered in this document.	

Security-Level	Fulfillment	Links
CR 4.3 Use of cryptography		
SL 2	The mGuard device enforces cryptographic mechanisms for device management via public networks, e.g., via the HTTPS or VPN protocols. **Measure 1 (internal)** Only secure encryption measures and secure encryption and hash algorithms may be used. These are identified in WBM and described in the user manual: – ISAKMP SA (Key Exchange) – Encryption: AES-256 – Hash/checksum: SHA-256, -384, -512 – Diffie-Hellman: 2048 bit or higher – IPsec SA (Data Exchange) – Encryption: AES-256 – Hash/checksum: SHA-256, -384, -512 – Perfect Forward Secrecy (PFS) – 2048 bit or higher	Secure encryption (UM: 3.1)

3.5 FR 5 – Restricted data flow (RDF)

Divide the automation system into zones and conduits to prevent unnecessary data flow.

Security-Level	Fulfillment	Links
CR 5.1 Network segmentation		
SL 2	**Automatically met by the device.** Network segmentation is one of the core functions of mGuard devices and is implemented via their router and firewall functionalities. Network segmentation can be carried out using the existing network interfaces. **Measure 1 (internal)** The network interface settings can be configured.	Network (UM: 5)
	Measure 2 (internal) Firewall settings can be configured.	Network Security >> Packet Filter (UM: 7.1)
CR 5.4 Application partitioning		
SL 2	There are no requirements at component level in connection with IEC 62443-3-3 SR 5.4	

3.6 FR 6 – Timely response to events (TRE)

Security breaches are responded to by informing the appropriate authority, reporting the necessary
evidence of the breach, and taking corrective action promptly upon discovery of incidents.

Security-Level	Fulfillment	Links
CR 6.1 Audit log accessibility		
SL 2	Event data records (log entries) can be evaluated on the mGuard device via web-based management (WBM) and on the remote syslog server. **Measure 1 (internal/external)** The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries).The stored log files can be evaluated on the remote syslog server. See CR 1.2	**Logging >> Browse Local Logs (UM: 11.2)** See CR 1.2
CR 6.1 RE1 Programmatic access to audit logs		
SL 2	Event data records (log entries) can be evaluated on the mGuard device via web-based management (WBM) and on the remote syslog server.	**Logging >> Browse Local Logs (UM: 11.2)** See CR 1.2
CR 6.2 Continuous monitoring		
SL 2	**Measure 1 (internal/external)** To record security breaches, the event data records (log entries) must be analyzed. Event data records (log files) can be analyzed via WBM of the mGuard device or on the remote syslog server.	**Logging >> Browse Local Logs (UM: 11.2)**
	Measure 2 (internal/external) The mGuard device must use a remote syslog server to store and manage the generated event data records (log entries). Remotely stored log files can be evaluated on the remote syslog server. See CR 1.2	See CR 1.2

3.7 FR 7 – Resource availability (RA)

The availability of the components is ensured if essential services are impaired or denied.

Security-Level	Fulfillment	Links
CR 7.1 Denial of service protection		
SL 2	**Automatically met by the device.** The mGuard device maintains essential functions when operating in an impaired mode due to a DoS event. **Measure 1 (internal)** DoS protection can be partially configured.	Network Security >> DoS Protection (UM: 7.3)
CR 7.1 RE1 Manage communication load from component		
SL 2	**Automatically met by the device.** The mGuard device maintains essential functions when operating in an impaired mode due to a DoS event. **Measure 1 (internal)** DoS protection can be partially configured.	Network Security >> DoS Protection (UM: 7.3)
CR 7.2 Resource management		
SL 2	**Automatically met by the device.** The mGuard device automatically limits resource usage through security functions to protect against resource exhaustion.	
CR 7.3 Control system backup		
SL 2	The current configuration of the mGuard device can be saved as a configuration profile (atv profile and ECS file), which can be downloaded from the device. This function is independent of other system functions and does not affect normal operation.	Management >> Configuration Profiles (UM: 4.5)
CR 7.3 RE1 Backup integrity verification		
SL 2	Imported configurations are strictly validated, including the relationships between variables. Configuration profiles (atv profiles and ECS files) can be created, managed, and uploaded or downloaded. The configuration profiles can be cryptographically signed with an mGuard machine certificate. This is done to	Management >> Configuration Profiles (UM: 4.5) Authentication >> Certificates (UM: 6.4)

Security-Level	Fulfillment	Links
	ensure the authenticity and integrity of the configuration profiles. **Measure 1 (internal/external)** The “Enable signed configuration profiles” function must be enabled. Only configuration profiles (atv profiles and ECS files) that are cryptographically signed by an mGuard machine certificate may be uploaded to or downloaded from the mGuard device.The import and export of unsigned configuration profiles is not permitted.	
CR 7.4 Control system recovery and reconstitution		
SL 2	**Automatically met by the device.** The mGuard device offers the option of returning to and restoring a known safe state (the last saved state) after a fault or failure.	
CR 7.5 Emergency power		
SL 2	There are no requirements at component level in connection with IEC 62443-3-3 SR 7.5	
CR 7.6 Network and security configuration settings		
SL 2	The mGuard device’s firewall is configured to prevent access from untrusted networks. By default, access to the device is only possible via the internal network interfaces (LAN). All externally accessible services can be restricted by firewall settings. Only the most important services are activated by default. In denial-of-service attacks (DoS attacks), only the attacker’s source IP is rejected in order to enable authorized access. **Measure 1 (internal/external)** Firewall settings can be configured.	Management >> System Settings >> Time and Date (UM: 4.1.2) Management >> System Settings >> Shell Access (UM: 4.1.3) Management >> Web Settings >> Access (UM: 4.2.2) Management >> SNMP >> Query (UM: 4.6.2)
CR 7.6 RE1 Machine-readable reporting of current security settings		
SL 3	Use of the device at SL 3 level is not considered in this document.	
CR 7.7 Least functionality		
SL 2	By default, access to the device is only possible via the internal network interfaces (LAN). All externally	Management >> System Settings >>

Security-Level	Fulfillment	Links
	accessible services can be restricted by firewall settings. Only the most important services are activated by default. **Measure 1 (internal)** Firewall settings can be configured.	Time and Date (UM: 4.1.2) Management >> System Settings >> Shell Access (UM: 4.1.3) Management >> Web Settings >> Access (UM: 4.2.2) Management >> SNMP >> Query (UM: 4.6.2)
CR 7.8 Control system component inventory		
SL 2	**Automatically met by the device.** Information about the installed firmware version on the mGuard device and the underlying packets is displayed in the device's WBM. **Measure 1 (internal)** The device's component inventory can be analyzed.	Management >> Update >> Overview (UM: 4.4.1)

3.8 Network device requirements (NDR)

Security-Level	Fulfillment	Links
NDR 1.6 Wireless access management		
SL 2	The requirement does not apply as the mGuard device does not have a wireless interface.	
NDR 1.13 Access via untrusted networks		
SL 2	**Automatically met by the device.** The network device's firewall is configured to prevent access from untrusted networks. By default, HTTPS access to the mGuard device is only possible via the internal network interfaces (LAN). If required, it can be permitted for other, individually restricted networks. **Measure 1 (internal)** See CR 7.6	See CR 7.6
NDR 1.13 RE1 Explicit access request approval		
SL 3	Use of the device at SL 3 level is not considered in this document.	
NDR 2.4 Mobile code		
SL 2	**Not applicable**. The mGuard device does not use any of the mobile code technologies defined in the standard.	
NDR 2.4 RE1 Mobile code authenticity check		
SL 2	**Not applicable**. The mGuard device does not use any of the mobile code technologies defined in the standard.	
NDR 2.13 Use of physical diagnostic and test interfaces		
SL 2	**Automatically met by the device.** The device has no physical diagnostic and test interfaces.	
NDR 2.13 RE1 Active monitoring		
SL 3	Use of the device at SL 3 level is not considered in this document.	

Security-Level	Fulfillment	Links
NDR 3.2 Protection from malicious code		
SL 2	**Automatically met by the device.** All executable code that is loaded onto the mGuard device via an update or flash mechanism is cryptographically signed. Mechanisms that restrict or prevent the execution of malicious code (hardening) are used on the Linux-based operating system of the mGuard device.	
NDR 3.10 Support for updates		
SL 2	**Automatically met by the device.** Firmware updates are supported by the device.	
NDR 3.10 RE1 Update authenticity and integrity		
SL 2	**Automatically met by the device.** The update files are cryptographically signed and hashed. This is done to ensure the authenticity and integrity of the update files. **Measure 1 (internal/external)** Updates are made available on a regular basis. The manufacturer’s website or other sources of information must be checked regularly for the availability of updates. Available updates must be installed as quickly as possible.	

Security-Level	Fulfillment	Links
NDR 3.11 Physical tamper resistance and detection		
SL 2	**Not applicable**. In the specified security context, no unauthorized personnel have physical access to the device. In addition, the housing of DIN rail devices and the packaging of PCI cards are protected with a tamper-proof seal for transport from the manufacturer to the application. **Measure 1 (internal/external)** Ensure that the seal is intact before operating the mGuard device. If the seal were removed/damaged, parts of the seal would remain on the housing/ packaging. Ensure that only authorized personnel have access to the housing. 	See user manual UM EN HW FL MGUARD 2000/4000 (110192_en_xx), Section “Initial startup”, at phoenixcontact.com/ product/<item number>
NDR 3.11 RE1 Notification of a tampering attempt		
SL 3	Use of the device at SL 3 level is not considered in this document.	
NDR 3.12 Provisioning product supplier roots of trust		
SL 2	**Automatically met by the device.** mGuard devices are equipped with a public product key from the manufacturer, e.g., to check the signature of an update file. The manufacturer’s public key is hard-coded in the firmware.	

Security-Level	Fulfillment	Links
NDR 3.13 Provisioning asset owner roots of trust		
SL 2	The mGuard device can use X.509 certificates created and managed by the operator to securely encrypt IPsec VPN connections, to authenticate itself as a web server to a peer, and to cryptographically sign configuration profiles. This ensures the authenticity and integrity of configuration profiles, identification of the device, and encrypted communication via IPsec VPN connections. **Machine certificate:** The mGuard device authenticates itself to the peer using a machine certificate loaded onto the mGuard device. The machine certificate acts as an “identification document” for the mGuard device, which it shows to the peer. Configuration profiles are signed with the machine certificate. **CA certificate:** CA certificates are certificates issued by a certification authority (CA). CA certificates are used to verify the authenticity of certificates shown by peers. **Remote certificate:** A remote certificate is a copy of the certificate with which a peer identifies itself to the mGuard device. The certificates are created and managed by the customer (asset owner) and must be uploaded to the mGuard device. **Measure 1 (internal/external)** The certificates must be created and managed by the operator (asset owner) (e.g., using third-party software tools such as XCA [hohnstaedt.de/xca]) and uploaded to the mGuard device.	
	Measure 2 (internal/external) Manage certificates to communicate securely with external servers via IPsec VPN by using the asset owner’s roots of trust.	Authentication >> Certificates (UM: 6.4)

Security-Level	Fulfillment	Links
	Measure 3 (internal/external) Configure a certificate-based, secure IPsec VPN connection to the external server using the asset owner's roots of trust.	IPsec VPN >> Connections (UM: 8.2, 8.2.2, 8.2.3)
	Measure 4 (internal/external) Create and manage cryptographically signed configuration profiles using the asset owner's roots of trust.	Management >> Configuration Profiles (UM: 4.5)
	Measure 5 (internal/external) Authenticate the mGuard device's web server to requesting web clients using a self-created machine certificate or "HTTPS server certificate" (using the operator's root of trust).	Management >> Web Settings >> Access (UM: 4.2.2)
NDR 3.14 Integrity of the boot process		
	Automatically met by the device. During the boot process, before the core functions of the device are started and before a user can interact with the device, the authenticity and integrity of the files of the mGuard base system are checked. If it is determined during the boot process that there is a problem with the authenticity and integrity of the files on the device (faulty/ manipulated), the boot process is aborted. The error is indicated by the red flashing device LED PF5 (flashing rhythm 500/500 ms).	LED status indicator and flashing behavior (UM: 15.3)
NDR 3.14 RE1 Authenticity of the boot process		
SL 2	**Automatically met by the device.** During the boot process, before the core functions of the device are started and before a user can interact with the device, the authenticity and integrity of the files of the mGuard base system are checked. If it is determined during the boot process that there is a problem with the authenticity and integrity of the files on the device (faulty/ manipulated), the boot process is aborted. The error is indicated by the red flashing device LED PF5 (flashing rhythm 500/500 ms).	LED status indicator and flashing behavior (UM: 15.3)

Security-Level	Fulfillment	Links
NDR 5.2 Zone boundary protection		
	The protection of zone boundaries is one of the main functions of the mGuard device.	
NDR 5.2 RE1 Deny all, permit by exception		
SL 2	**Automatically met by the device.** The standard firewall rules completely reject any access from an external (untrusted) network. **Measure 1 (internal)** Configured firewall rules should only allow network traffic that is necessary.	Network Security >> Packet Filter (UM: 7.1)
NDR 5.2 RE2 Island mode		
SL 3	Use of the device at SL 3 level is not considered in this document.	
NDR 5.2 RE3 Fail close		
SL 3	Use of the device at SL 3 level is not considered in this document.	
NDR 5.3 General purpose, person-to-person communication restrictions		
SL 2	**Automatically met by the device.** Restrictions on person-to-person communication for general purposes are covered by the main functions of the mGuard device. **Measure 1 (internal)** Firewall rules can be configured.	Network Security >> Packet Filter (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_en_04