How to configure mGuard devices to cover the functional range of IEC 62443-4-2 in certain aspects

User manual

UM EN MGUARD 62443-4-2

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

UM EN MGUARD 62443-4-2, Revision 01 2019-12-03

This user manual is valid for the following mGuard devices, running firmware 8.6.1 or later

FL MGUARD RS4000 TX/TX (VPN)
FL MGUARD RS4000 TX/TX VPN-M
FL MGUARD RS4000-P
FL MGUARD RS4004 TX/DTX (VPN)
TC MGUARD RS4000 3G VPN
TC MGUARD RS4000 4G VPN
TC MGUARD RS4000 4G VZW VPN
TC MGUARD RS4000 4G ATT VPN

109049_en_01

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 Introduction

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

IEC 62443-4-2 defines security requirements for components used in industrial automation and control systems (IACS). These requirements are called **Component Requirements (CR)** which are close related to the **System Requirements (SR)** defined in IEC 62443-3-3. Both CR and SR are technical requirements derived from the higher level definition of seven **Foundational Requirements (FR)** defined in IEC 62443-1-1.

Component Requirements (CR) and associated Requirement Enhancements (RE) express a component's capability to be used in an IACS with one of the four risk based Security Levels assigned (SL 1 ... SL 4).

In order to achieve a certain Security Level according to IEC 62443-3-3, it is possible to combine components of an automation system in such a way that the overall system meets the desired system requirements (Security Levels).

IEC 62443-4-2 defines the technical components of automation systems on the basis of seven Foundational Requirements (FR) resulting from IEC 62443-1-1:

- identification and authentication control (IAC),
- use control (UC),
- system integrity (SI),
- data confidentiality (DC),
- restricted data flow (RDF),
- timely response to events (TRE), and
- resource availability (RA).

For these, the individual requirements for supporting certain Security Levels at component level (SL-C) are described in the standard.

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

Primarily operators, system integrators and manufacturers active in automation technology.

System integrators can easily determine which components can be used to achieve specific Security Levels. Manufacturers get support in deciding which and how individual components can be combined in an automation system in order to achieve a specific Security Level for the overall system.

1.3 What is a Security Level?

Security Levels (SL) reflect the required set of countermeasures to prevent certain security risks. Four Security Levels SL 1 ... SL 4 are defined, that can be fulfilled by individual security measures. These measures are described in Section 2, “How to configure mGuard devices to cover the functional range of IEC 62443-4-2”.

1.4 Do mGuard devices cover the functional range of the IEC 62443-4-2?

mGuard devices are used in certified security automation solutions (IACS). The devices have not yet been formally certified as single components because product development took place before the publi0cation of IEC 62443-4-1 (Secure product development lifecycle requirements), which is a prerequisite for product certification according to IEC 62443-4-2.

The Security Levels (SL) according IEC 62443-4-2 that could be achieved through the use of mGuard device are listed in Table 1-1.

Table 1-1 Security Levels (SL) according to IEC 62443-4-2 that could be achieved through the use of mGuard devices. FR = Foundational Requirements, CR = Component Requirements, NDR = Network device requirements green = could be achieved, blue = not applicable, white = cannot be achieved

Security Levels (SL)							
FR 1 1 2 3 4	**FR 2** 1 2 3 4	**FR 3** 1 2 3 4	**FR 4** 1 2 3 4	**FR 5** 1 2 3 4	**FR 6** 1 2 3 4	**FR 7** 1 2 3 4
CR 1.1 1 2 3 4	CR 2.1 1 2 3 4	CR 3.1 1 2 3 4	CR 4.1 1 2 3 4	CR 5.1 1 2 3 4	CR 6.1 1 2 3 4	CR 7.1 1 2 3 4
CR 1.2 1 2 3 4	CR 2.2 1 2 3 4	CR 3.2 (**NDR**) 1 2 3 4	CR 4.2 1 2 3 4	CR 5.2 (**NDR**) 1 2 3 4	CR 6.2 1 2 3 4	CR 7.2 1 2 3 4
CR 1.3 1 2 3 4	CR 2.3 N/A	CR 3.3 1 2 3 4	CR 4.3 1 2 3 4	CR 5.3 (**NDR**) 1 2 3 4		CR 7.3 1 2 3 4
CR 1.4 1 2 3 4	CR 2.4 (**NDR**) N/A	CR 3.4 1 2 3 4		CR 5.4 N/A		CR 7.4 1 2 3 4
CR 1.5 1 2 3 4	CR 2.5 1 2 3 4	CR 3.5 1 2 3 4				CR 7.5 N/A
CR 1.6 (**NDR**) 1 2 3 4	CR 2.6 1 2 3 4	CR 3.6 N/A				CR 7.6 1 2 3 4
CR 1.7 1 2 3 4	CR 2.7 1 2 3 4	CR 3.7 1 2 3 4				CR 7.7 1 2 3 4
CR 1.8 1 2 3 4	CR 2.8 1 2 3 4	CR 3.8 1 2 3 4				CR 7.8 1 2 3 4
CR 1.9 1 2 3 4	CR 2.9 1 2 3 4	CR 3.9 1 2 3 4				
CR 1.10 1 2 3 4	CR 2.10 1 2 3 4	CR 3.10 (**NDR**) 1 2 3 4				
CR 1.11 1 2 3 4	CR 2.11 1 2 3 4	CR 3.11 (**NDR**) N/A				
CR 1.12 1 2 3 4	CR 2.12 1 2 3 4	CR 3.12 (**NDR**) N/A				
CR 1.13 (**NDR**) 1 2 3 4	CR 2.13 (**NDR**) 1 2 3 4	CR 3.13 (**NDR**) N/A				
CR 1.14 N/A		CR 3.14 (**NDR**) 1 2 3 4				

2 How to configure mGuard devices to cover the functional range of IEC 62443-4-2

According to IEC 62443-4-2 the mGuard device is classified as a network device. Therefore, the corresponding **Network Device Requirements (NDR)** are required for **Component Requirements (CR)** 1.6, 1.13, 2.4, 2.13, 3.2, 3.10, 3.11, 3.12, 3.13, 3.14, 5.2, and 5.3.

Color code: green = could be achieved, blue = not applicable, red = cannot be achieved

References to the related sections in the mGuard User Manual have been added (UM: <Section>).

The user manual (UM EN MGUARD / Document ID: 105661_en_xx) can be downloaded in the Phoenix Contact Web Shop at phoenixcontact.net/product/2200515.

2.1 FR 1 – Identification and authentication control

Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.

2.1.1 CR 1.1 – Human user identification and authentication

Table 2-1 CR 1.1 – Human user identification and authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	By default, the mGuard device requires authentication via password for every user interface (SSH, SSL, SNMP or serial console) each time a user logs on. The password for the user can be configured at: **Authentication >> Administrative Users >> Password** (UM: 7.1.1) To avoid insecure authentication, SNMP should be disabled in: **Management >> SNMP >> Query** (UM: 4.6.1)
Reaching SL 2	Additionally required: To reach SL 2, the mGuard device must additionally use an external RADIUS server for unique identification and authentication. The RADIUS server is normally managed by an IT department. It must be ensured that the connection to the RADIUS server is carried out via a VPN tunnel. The integration of an external RADIUS server can be configured at: **Authentication >> RADIUS** (UM: 7.3) **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2) Configure the mGuard device to allow RADIUS authentication *as only method for password authentication*.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.1.2 CR 1.2 – Software process and device identification and authentication

Table 2-2 CR 1.2 – Software process and device identification and authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.1.3 CR 1.3 – Account management

Table 2-3 CR 1.3 – Account managemet

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The mGuard device must use an external RADIUS server for unique identification and authentication of the accounts. It must be ensured that the connection to the RADIUS server is carried out via a VPN tunnel. The integration of an external RADIUS server can be configured at: **Authentication >> RADIUS** (UM: 7.3) **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2) Configure the mGuard device to allow RADIUS authentication *as only method for password authentication*.

2.1.4 CR 1.4 – Identifier management

Table 2-4 CR 1.4 – Identifier management

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Local identifier management is supported by the mGuard device itself. It is also possible to delegate the identifier management to an external RADIUS server. The mGuard device supports the identification and authentication via X.509 certificates. Identifier management can be configured at: **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2)

2.1.5 CR 1.5 – Authenticator management

Table 2-5 CR 1.5 – Authenticator management

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	Automatically fulfilled by mGuard devices. a) Passwords for authentication of the users *root* and *admin* are set by default. b) Changes of the default passwords (*root* and *admin*) are displayed via web-based management. c) Passwords and other authentication methods can be changed at any time. d) Passwords are stored in hashed form, their transmission is always encrypted and the typed password is obscured by using bullets (•) instead of characters. If a RADIUS server is used for authentication, it must be ensured that the connection to the RADIUS server is carried out via a VPN tunnel. The integration of an external RADIUS server can be configured at: **Authentication >> RADIUS** (UM: 7.3)
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.1.6 CR 1.6 – Wireless access management (NDR)

Table 2-6 CR 1.6 – Wireless access management (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	A 3G/4G mGuard device can be accessed via its assigned IP address. The login to the device behaves the same as in wired connections. By default, the mGuard device requires authentication via password for every user interface (SSH, SSL, SNMP or serial console) each time a user logs on. Access to the device via the mobile interface can be restricted by the mGuard firewall. The "*access firewall*" can be configured at: **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2)
Reaching SL 2 – 4	Login occurs via SIM card and related PIN.

2.1.7 CR 1.7 – Strength of password-based authentication

Table 2-7 CR 1.7 – Strength of password-based authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	The mGuard device must use an external RADIUS server that posses the capability to enforce configurable password strength. The RADIUS server is normally managed by an IT department. It must be ensured that the connection to the RADIUS server is carried out via a VPN tunnel. The integration of an external RADIUS server can be configured at: **Authentication >> RADIUS** (UM: 7.3) **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2) Configure the mGuard device to allow RADIUS authentication *as only method for password authentication*.
Reaching SL 3 – 4	Additionally required (by the external RADIUS server): – SL 3: Password generation and lifetime restrictions for human users. – SL 4: Password lifetime restrictions for all users (human, software process, or device).

2.1.8 CR 1.8 – Public key infrastructure certificates

Table 2-8 CR 1.8 – Public key infrastructure certificates

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	mGuard devices support X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject. To authenticate remote peers via X.509 certificates, required CA or remote certificates can be used: – CA certificates are certificates issued by a certification authority (CA). CA certificates are used to check whether the certificates shown by peers are authentic. – A remote certificate is a copy of the certificate that is used by a peer to authenticate itself to the mGuard. Certificates can be configured and managed at: **Authentication >> Certificates** (UM: 7.4) **Authentication >> Certificates >> CA Certificates** (UM: 7.4.3) **Authentication >> Certificates >> Remote Certificates** (UM: 7.4.4) PKI support is given for HTTPS/SSH remote access and can be configured at: **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2)

2.1.9 CR 1.9 – Strength of public key-based authentication

Table 2-9 CR 1.9 – Strength of public key-based authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2	mGuard devices support X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject. The supported mechanisms are internationally recognized and proven. Certificates can be configured and managed at: **Authentication >> Certificates** (UM: 7.4)
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.1.10 CR 1.10 – Authenticator feedback

Table 2-10 CR 1.10 – Authenticator feedback

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. The mGuard device provides the capability to obscure feedback of authenticator information during the authentication process.

2.1.11 CR 1.11 – Unsuccessful login attempts

Table 2-11 CR 1.11 – Unsuccessful login attempts

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	mGuard devices have build in mechanisms to: a) delay further login attempts after a number of invalid access attempts, b) throttle SSH/HTTPS (SSL) connections after massive connection attempts. As those mechanisms are build in and not configurable on the mGuard device, the requirements for SL 1 – 4 can only be fulfilled, using an external RADIUS server. The integration of an external RADIUS server can be configured at: **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2)

2.1.12 CR 1.12 – System use notification

Table 2-12 CR 1.12 – System use notification

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	mGuard devices show a configurable system use notification before authentication via SSH/HTTPS. The system use notification can be customized at: **Management >> System Setting >> Host** (UM: 4.1.1)

2.1.13 CR 1.13 – Access via untrusted networks (NDR)

Table 2-13 CR 1.13 – Access via untrusted networks (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	The firewall of the network device access is configured to not allow access from untrusted networks (see “CR 7.6 – Network and security configuration settings” on page 28)
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.1.14 CR 1.14 – Strength of symmetric key-based authentication

Table 2-14 CR 1.14 – Strength of symmetric key-based authentication

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The mGuard device allows to use *Pre-shared keys* (PSK) for symmetric authentication of VPN connections. Beyond that, the mGuard does not use symmetric key-based authentication. It must be ensured that the *"Authentication method" PSK* is not used for authentication in VPN connections. X.509 certificates must be used for authentication instead. Authentication in VPN connections can be configured at: **IPsec VPN >> Connections >> (Edit) >> Authentication** (UM: 10.2.3)

2.2 FR 2 – Use Control

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

2.2.1 CR 2.1 – Authorization enforcement

Table 2-15 CR 2.1 – Authorization enforcement

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	The implemented user roles of mGuard devices and therefore related user rights and permissions can be assigned to human users.
Reaching SL 2	Additionally required: (1) User roles and related rights and permissions can be assigned to human users, software processes and devices. (2) With the help of the user role "*netadmin*", write permissions to each variable can be given to or withdrawn. The authorization levels for the users *netadmin* and *audit* relate to access rights with the mGuard device manager (FL MGUARD DM UNLIMITED).
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.2.2 CR 2.2 – Wireless use control

Table 2-16 CR 2.2 – Wireless use control

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	For outgoing wireless communication, mGuard devices can use the 3G or 4G standard, which cannot be influenced. If communication takes place over this route, the same mechanisms and protocols are used as for a wire-bound connection. For incoming wireless communication, the firewall of the mGuard device can be used on mobile connections (Interface: "External 2"). Firewall rules can be configured at: **Network Security >> Packet Filter >> Incoming Rules** (UM: 8.1.1)

2.2.3 CR 2.3 – Use control for portable and mobile devices

Table 2-17 CR 2.3 – Use control for portable and mobile devices

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Not applicable. There is no component level requirement associated with IEC 62443-3-3 SR 2.3.

2.2.4 CR 2.4 – Mobile code (NDR)

Table 2-18 CR 2.4 – Mobile code (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Not applicable. The mGuard device does not use mobile code technologies as defined in the standard.

2.2.5 CR 2.5 – Session lock

Table 2-19 CR 2.5 – Session lock

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatic session timeout is available for access via SSH (Command Line Interface), HTTPS (Web-based management) and for access via serial interface. The automatic session timeout for HTTPS (Web-based management) is set to the default value (90 minutes) and configurable by the user. Session timeout for Web-based management (HTTPS) can be configured at: **Management >> Web Settings >> General** (UM: 4.2.1)

2.2.6 CR 2.6 – Remote session termination

Table 2-20 CR 2.6 – Remote session termination

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The mGuard device automatically terminates active sessions, initiated via SSH (Command Line Interface), HTTPS (Web-based management) and serial interface after a predefined time. The automatic session timeout for HTTPS (Web-based management) is set to the default value (90 minutes) and configurable by the user. Session timeout for Web-based management (HTTPS) can be configured at: **Management >> Web Settings >> General** (UM: 4.2.1)

2.2.7 CR 2.7 – Concurrent session control

Table 2-21 CR 2.7 – Concurrent session control

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 3 – 4	The number of concurrent sessions via the web interface (HTTPS) is limited to only one. For the SSH interface, the number of access instances for administrative user roles (*admin, netadmin, audit,* and *mobile*) can be limited individually. The user *root* always has unrestricted access. It is possible to disable remote access via the SSH interface for the user *root.* Limiting concurrent sessions via the SSH interface can be configured at: **Management >> System Settings >> Shell Access** (UM: 4.1.3)

2.2.8 CR 2.8 – Auditable events

Table 2-22 CR 2.8 – Auditable events

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The mGuard device automatically generates audit records relevant to security. The logs are also readable by the user role *audit*. **Individual audit reports** a – f: The audit records, generated by the mGuard device are *Syslog* conform. Log files can be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2) Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) It must be ensured that the connection to the Syslog server is carried out via a VPN tunnel.

2.2.9 CR 2.9 – Audit storage capacity

Table 2-23 CR 2.9 – Audit storage capacity

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	Automatically fulfilled by mGuard devices. Even if the maximum size for the log file is reached, the running applications are not effected and keep running.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.2.10 CR 2.10 – Response to audit processing failures

Table 2-24 CR 2.10 – Response to audit processing failures

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. The audit and logging event of mGuard devices are not able to influence the main function of the processes.

2.2.11 CR 2.11 – Timestamp

Table 2-25 CR 2.11 – Timestamp

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Automatically fulfilled by mGuard devices. The mGuard device automatically creates time stamps for every log event in the related log files.
Reaching SL 2 – 3	Additionally required: The created time stamps in mGuard devices are synchronized with the system wide time source that might be synchronized via NTP.
Reaching SL 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.2.12 CR 2.12 – Non-repudiation

Table 2-26 CR 2.12 – Non-repudiation

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	To determine if a given human user took a particular action on the mGuard device, an external RADIUS server has to be used. The RADIUS server must be configured in a way, that each user role with the ability to configure the mGuard device, e.g. *admin* or *root*, is allocated to only one human user. Particular actions of the user roles (human users) can be analyzed in the mGuard log files. The integration of an external RADIUS server can be configured at: **Management >> System Settings >> Shell access** (UM: 4.1.3) **Management >> Web Settings >> Access** (UM: 4.2.2) Log files can be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2) Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) It must be ensured that the connection to the Syslog server is carried out via a VPN tunnel.

2.2.13 CR 2.13 – Use of physical diagnostic and test interfaces (NDR)

Table 2-27 CR 2.13 – Use of physical diagnostic and test interfaces (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2	The mGuard devices protects against unauthorized use of the physical factory diagnostic and test interface(s). The test interfaces are only accessible after disassembly of the device housing.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3 FR 3 – System integrity

Ensure the integrity of the component to protect against unauthorized manipulation or modification.

2.3.1 CR 3.1 – Communication integrity

Table 2-28 CR 3.1 – Communication integrity

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	mGuard devices allow remote access to its configuration interfaces via encrypted SSH (command line interface), SSL/HTTPS (web-based management) or VPN protocols. Such protocols include mechanisms to assure integrity of transmitted data. The services "NTP" and "Remote logging/Syslog" must be carried out via a VPN tunnel. **NTP server** Allowing access to the NTP server only via VPN connection can be configured at: **Management >> System Settings >> Time and Date** (UM: 4.1.2) **Remote logging** Using Remote logging/Syslog only via VPN connection is explained at: **Logging >> Settings >> Settings** (UM: 15.1.1) **Configuring VPN connections** VPN connections can be configured at: **IPsec VPN >> Connections** (UM: 10.2, 10.2.2) For other services of the mGuard device that might not be able to provide sufficient communication integrity, the following applies: If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.
Reaching SL 2 – 4	Additionally required: The authenticity of received information during communication can be ensured by using X.509 certificates. Access to configuration interfaces can be configured at: **Management >> Web Settings >> Access** (UM: 4.2.2) **Management >> System Settings >> Shell Access** (UM: 4.1.3) Authentication in VPN connections can be configured at: **IPsec VPN >> Connections >> (Edit) >> Authentication** (UM: 10.2.3) It must be ensured that the *"Authentication method" PSK* is not used for authentication in VPN connections. X.509 certificates must be used for authentication instead.

2.3.2 CR 3.2 – Protection from malicious code (NDR)

Table 2-29 CR 3.2 – Protection from malicious code (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. All executable code loaded onto the device via update or flash mechanism is cryptographically signed.

2.3.3 CR 3.3 – Security functionality verification

Table 2-30 CR 3.3 – Security functionality verification

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 3	On the mGuard device it is possible to verify the intended operation of security functions at any time by analyzing the log files for configuration changes, application of firewall rules, usage of VPN connections. **Logging** Log files can be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2) Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) Remote logging/Syslog must be carried out via a VPN tunnel (see Section 2.3.1). **Firewall** The functionality of the mGuard firewall can be tested at any time by sending a special packet matched by an appropriate firewall rule that drops and logs the packet. The DPI modules can also be tested likewise. Firewall rules and respective logging can be configured at: **Network Security >> Packet Filter** (UM: 8.1) **IPsec VPN >> Connections >> (Edit) >> Firewall** (UM: 10.2.4) **OpenVPN Client >> Connections >> (Edit) >> Firewall** (UM: 11.1.5) **Network >> GRE Tunnel >> (Edit) >> Firewall** (UM: 10.6.2) **Other:** UM: Ch. 3.1.2, Ch. 3.1.3, Ch. 4.2.2, Ch. 4.6.1, Ch. 6.3.2, Ch. 6.3.4, CH. 12.1) **VPN connections** The functionality of established VPN connections are displayed in the Web UI and log files of the mGuard device. VPN connections can be analyzed at: **IPsec VPN >> IPsec Status** (UM: 10.4)
Reaching SL 4	Additionally required: The mGuard device provides the capability to support verification of the intended operation of security functions during normal operations (see above).

2.3.4 CR 3.4 – Software and information integrity

Table 2-31 CR 3.4 – Software and information integrity

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3.5 CR 3.5 – Input validation

Table 2-32 CR 3.5 – Input validation

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	Automatically fulfilled by mGuard devices. All input values are validated. Several external testing institutions have performed *Penetration-Tests* on the product. No gaps were found.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3.6 CR 3.6 – Deterministic output

Table 2-33 CR 3.6 – Deterministic output

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The output of the mGuard device shall not be connected to an automation process but it can be used for signaling. Service contacts (I/O) can be configured at: **Management >> Service I/O** (UM: 4.8) Beyond this the requirement does not apply to mGuard devices. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3.7 CR 3.7 – Error handling

Table 2-34 CR 3.7 – Error handling

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	In case of an error condition, the mGuard device does not provide information that could be exploited by adversaries to attack the IACS. Details can be seen in the log files. Log files can be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2) Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) Remote logging/Syslog must be carried out via a VPN tunnel (see Section 2.3.1).

2.3.8 CR 3.8 – Session integrity

Table 2-35 CR 3.8 – Session integrity

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	Automatically fulfilled by mGuard devices. The mGuard device provides mechanisms to protect the integrity of communications sessions.

2.3.9 CR 3.9 – Protection of audit information

Table 2-36 CR 3.9 – Protection of audit information

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 3	The audit information 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 or transit. Information can only be read by authenticated users.
Reaching SL 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3.10 CR 3.10 – Support for updates (NDR)

Table 2-37 CR 3.10 – Support for updates (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Firmware update is a supported function. The functionality of the device is interrupted in this case. Thus the device shall only be used for essential functions in a redundant setup.
Reaching SL 2 – 4	Additionally required: The update files are signed by PKCS#7 signatures and hashed. This is done to ensure authenticity and integrity of the update files.

2.3.11 CR 3.11– Physical tamper resistance and detection (NDR)

Table 2-38 CR 3.11 – Physical tamper resistance and detection (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The mGuard device itself does not offer physical tamper resistance and detection. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.3.12 CR 3.12 – Provisioning product supplier roots of trust (NDR)

Table 2-39 CR 3.12 – Provisioning product supplier roots of trust (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	Not applicable.

2.3.13 CR 3.13 – Provisioning asset owner roots of trust (NDR)

Table 2-40 CR 3.13 – Provisioning asset owner roots of trust (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	Not applicable.

2.3.14 CR 3.14 – Integrity of the boot process (NDR)

Table 2-41 CR 3.14 – Integrity of the boot process (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.4 FR 4 – Data confidentiality

Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure.

2.4.1 CR 4.1 – Information confidentiality

Table 2-42 CR 4.1 – Information confidentiality

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	If the mGuard device is configured as described in this document and if secure encryption and hash algorithms are used as described in Chapter 2.1 of the mGuard User Manual (UM EN MGUARD / Document ID: 105661_en_xx), SL1 – 2 can be reached. Several external testing institutions have performed *Penetration-Tests* on the product. No gaps were found.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.4.2 CR 4.2 – Information persistence

Table 2-43 CR 4.2 – Information persistence

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2	By flashing the device, all information will be deleted.
Reaching SL 3 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.4.3 CR 4.3 – Use of cryptography

Table 2-44 CR 4.3 – Use of cryptography

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	The device enforces cryptographic mechanisms for device management over public networks e.g. via the protocols HTTPS, SSH or VPN. It must be assured, that secure encryption and hash algorithms are used as describes in the User Manual (UM: 2.1).

2.5 FR 5 – Restricted data flow

Segment the control system via zones and conduits to limit the unnecessary flow of data.

2.5.1 CR 5.1 – Network segmentation

Table 2-45 CR 5.1 – Network segmentation

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. The segmentation of networks is one of the core feature of mGuard devices, using their router and firewall functionalities. Using its two or more network interfaces, segmentation of networks can be easily performed. Network interfaces settings can be configured at: **Network** (UM: 6) Firewall settings can be configured at: **Network Security >> Packet Filter** (UM: 8.1)

2.5.2 CR 5.2 – Zone boundary protection (NDR)

Table 2-46 CR 5.2 – Zone boundary protection (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Automatically fulfilled by mGuard. Basic functionality of the mGuard device. **Network Security >> Packet Filter** (UM: 8.1)
Reaching SL 2	Automatically fulfilled by mGuard devices. Default firewall rules entirely reject any access from the external (untrusted) network. Configured firewall rules should only allow network traffic that is necessary.
Reaching SL 3 – 4	Automatically fulfilled by mGuard devices. The mGuard device protects against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms.

2.5.3 CR 5.3 – General-purpose person-to-person communication restrictions (NDR)

Table 2-47 CR 5.3 – General-purpose person-to-person communication restrictions (NDR)

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Basic functionality of the mGuard device. Firewall rules can be configured at: **Network Security >> Packet Filter** (UM: 8.1)

2.5.4 CR 5.4 – Application partitioning

Table 2-48 CR 5.4 – Application partitioning

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	There is no component level requirement associated with IEC 62443-3-3 SR 5.4

2.6 FR 6 – Timely response to events

Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

2.6.1 CR 6.1 – Audit log accessibility

Table 2-49 CR 6.1 – Audit log accessibility

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	The log files of the device can be analyzed via SSH (console) and HTTPS (web-based management). Log files can be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2)
Reaching SL 3 – 4	Additionally required: Log files can be analyzed remotely using Remote logging/Syslog. Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) Remote logging/Syslog must be carried out via a VPN tunnel (see Section 2.3.1).

2.6.2 CR 6.2 – Continuous monitoring

Table 2-50 CR 6.2 – Continuous monitoring

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	To detect security breaches, the log files need to be analyzed at: **Logging >> Browse Local Logs** (UM: 15.2) Remote logging can be configured at: **Logging >> Settings** (UM: 15.1) Remote logging/Syslog must be carried out via a VPN tunnel (see Section 2.3.1).

2.7 FR 7 – Resource availability

Ensure the availability of components against the degradation or denial of essential services.

2.7.1 CR 7.1 – Denial of service protection

Table 2-51 CR 7.1 – Denial of service protection

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Automatically fulfilled by mGuard devices. The mGuard device maintains essential functions when operating in a degraded mode as the result of a DoS event.
Reaching SL 2 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.7.2 CR 7.2 – Resource management

Table 2-52 CR 7.2 – Resource management

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. The mGuard device limits the use of resources by security functions to protect against resource exhaustion.

2.7.3 CR 7.3 – Control system backup

Table 2-53 CR 7.3 – Control system backup

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	The current configuration of the mGuard device can be stored as a configuration profile (ECS file) which can be downloaded from the device. This function is independent of other system functionality and does not affect the normal operations. Configuration profiles can be generated and downloaded at: **Management >> Configuration Profiles** (UM: 4.5)
Reaching SL 2 – 4	There are no functions implemented in mGuard devices that help to reach the designated Security Level. If necessary, compensation would have to be provided by a higher-level system component or by organizational measures.

2.7.4 CR 7.4 – Control system recovery and reconstitution

Table 2-54 CR 7.4 – Control system recovery and reconstitution

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	Automatically fulfilled by mGuard devices. The mGuard device provides the capability to be recovered and reconstituted to a known secure state (the last saved state) after a disruption or failure.

2.7.5 CR 7.5 – Emergency power

Table 2-55 CR 7.5 – Emergency power

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	There is no component level requirement associated with IEC 62443-3-3 SR 7.5.

2.7.6 CR 7.6 – Network and security configuration settings

Table 2-56 CR 7.6 – Network and security configuration settings

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 2	All externally accessible services can be restricted by firewall settings or completely disabled. By default only essential services are enabled. Firewall settings can be configured at: **Network Security >> Packet Filter** (UM: 8.1) In case of Denial of Service (DoS) attacks, only the source IP of the attacker is rejected, to still allow authorized access.
Reaching SL 3 – 4	Additionally required: The current configuration of the device can be exported (ATV file) and read by other applications. Configuration profiles can be generated and downloaded at: **Management >> Configuration Profiles** (UM: 4.5)

2.7.7 CR 7.7 – Least functionality

Table 2-57 CR 7.7 – Least functionality

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1 – 4	All externally accessible services can be restricted by firewall settings or completely disabled. By default only essential services are enabled. Firewall settings can be configured at: **Network Security >> Packet Filter** (UM: 8.1)

2.7.8 CR 7.8 – Control system component inventory

Table 2-58 CR 7.8 – Control system component inventory

How to configure mGuard devices to cover the functional range of IEC 62443-4-2	
Reaching SL 1	Not applicable. There is no requirement defined in 62443-4-2 to reach the security level.
Reaching SL 2 – 4	Information about the installed firmware version of the mGuard device as well as the underlying packets is shown in the web interfaces of the device. The component inventory can be analyzed at: **Management >> Update >> Overview** (UM: 4.4.1)

2.8 NDR – Network Device Requirements

According to IEC 62443-4-2 the mGuard device is classified as a network device. Therefore, the corresponding **Network Device Requirements (NDR)** are required for **Component Requirements (CR)** 1.6, 1.13, 2.4, 2.13, 3.2, 3.10, 3.11, 3.12, 3.13, 3.14, 5.2, and 5.3. The related measures to achieve certain Security levels is described in the respective CRs.

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com **phoenixcontact.com**

109049_en_01
Order No. —01

INSPIRING INNOVATIONS