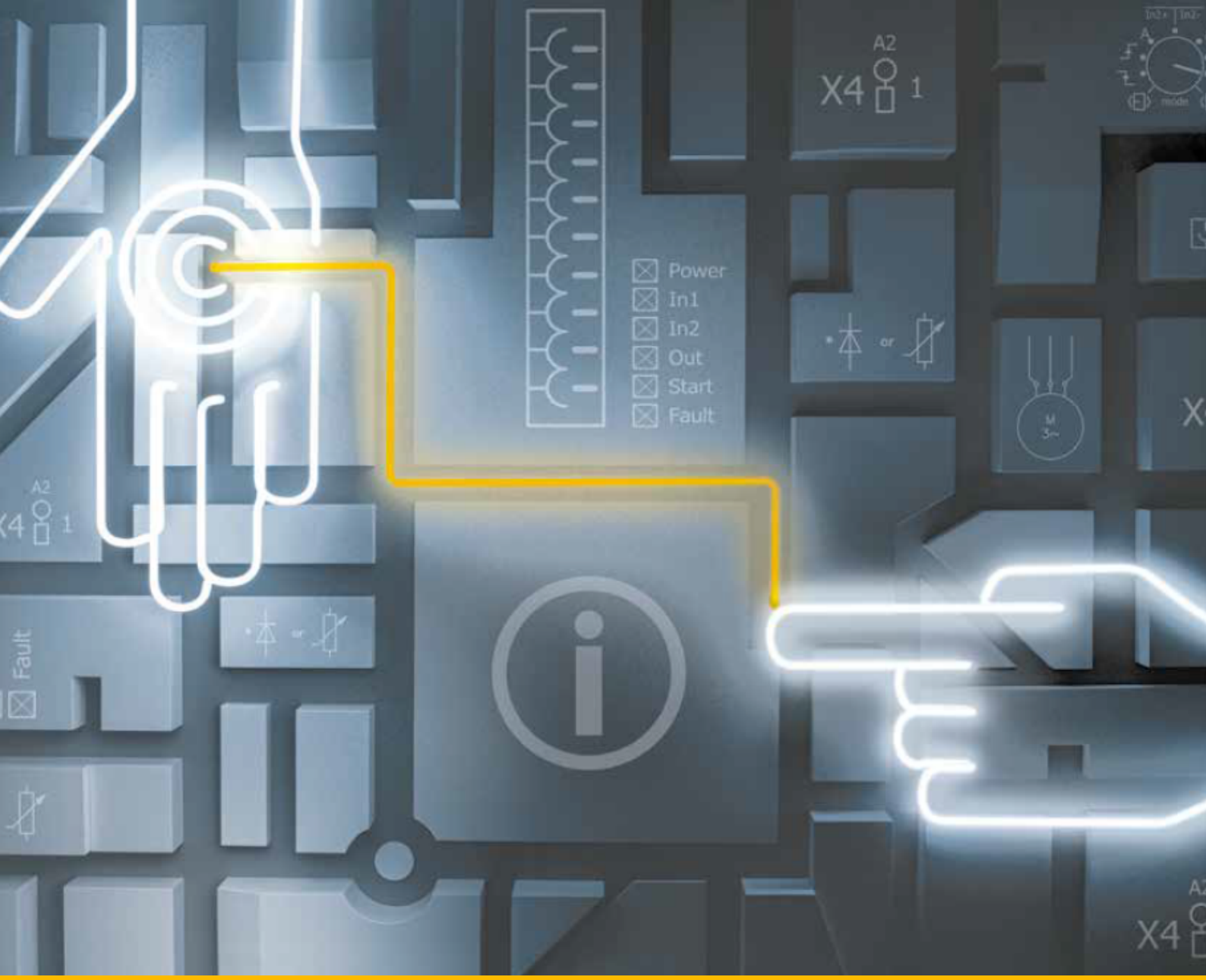

PSS 4000 compliance with IEC 62443-4-2

PILZ
THE SPIRIT OF SAFETY

Operating Manual-1007475-EN-01




This document is a translation of the original document.

Where unavoidable, for reasons of readability, the masculine form has been selected when formulating this document. We do assure you that all persons are regarded without discrimination and on an equal basis.

All rights to this documentation are reserved by Pilz GmbH & Co. KG. Copies may be made for the user's internal purposes. Suggestions and comments for improving this documentation will be gratefully received.

CECE®, CHRE®, CMSE®, INDUSTRIAL PI®, Leansafe®, MYZEL®, PAS4000®, PAScal®, PASconfig®, Pilz®, PIT®, PMCprimo®, PMCprotego®, PMCtendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries.

SD means Secure Digital

1 PSS 4000 compliance with IEC 62443-4-2

This document applies to all PSS 4000-exclusive devices from PSS 4000 firmware version 1.30.0 onwards.

The products comply with Security Levels 1 and 2.

As soon as PSS 4000 firmware version 1.30.0 is released, you will find a description of the implemented and required external security measures in the automation system PSS 4000 in the Safety and Security Manual PSS 4000, under "Security measures".

Abbreviation/ Symbol	Meaning
CR	Component Requirement
EDR	Embedded Device Requirement
FR	Foundational Requirement
HDR	Host Device Requirement
ID	Identifier from IEC 62443-4-2
NDR	Network Device Requirement
RE	Requirement Enhancement
SAR	Software Application Requirement
SL	Security Level The requirement must be met in order to achieve the stated Security Level(s).
✔	Security measure implemented, product meets the requirement
✔▪	Required external security measure, must be implemented by the user
✖	Requirement is not met.
N/A	The requirement is not applicable.

FR 1 - Identification and authentication control

ID	Requirement	Met	Note	SL
CR 1.1	Human user identification and authentication	✔	Human users can access a PSS 4000 device via the PAS4000 programming interface or via an OPC UA Client. User authentication has been implemented for both interfaces as part of user management.	≥ 1
CR 1.1 RE 1	Unique identification and authentication	✔	A separate user account can be created for each user.	≥ 2
CR 1.1 RE 2	Multifactor authentication for all interfaces	✖	---	≥ 3

ID	Requirement	Met	Note	SL
CR 1.2	Software process and device identification and authentication	✔	A PSS 4000 device can use its device certificate to identify and authenticate itself to other components and to human users' Clients. This concerns the following interfaces: ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p If the implemented security measures are used and the required external security measures are in place (see the PSS 4000 Safety and Security Manual), then no identification or authentication vis-à-vis other components is required for process data communication (SafetyNET p, PROFINET, EtherNet/IP, IP connections). If the implemented security measures are used and the required external security measures are in place (see the PSS 4000 Safety and Security Manual), then no identification or authentication vis-à-vis other components is required for the I/O data from electronic modules.	≥ 2
CR 1.2 RE 1	Unique identification and authentication	✔	The device certificate uniquely identifies and authenticates a PSS 4000 device.	≥ 3
CR 1.3	Account management	✔	There is a local user management system in which user and device accounts are managed.	≥ 1
CR 1.4	Identifier management	✔	The user and device accounts contain unique identifiers for users and devices.	≥ 1

ID	Requirement	Met	Note	SL
CR 1.5	Authenticator management	✔	▸ In its factory settings, a default user is set up with a predefined username and password. ▸ The default user's password must be changed before any other action is taken. ▸ Trusted certificates, user accounts and passwords may be changed at any time. ▸ Communication via the PAS4000 programming interface or via OPC UA is encrypted. ▸ Passwords are stored encrypted. Accounts can either be saved internally on the PSS 4000 device or on the SD card. In the second case, you have the option of encrypting the SD card. ▸ Passwords may only be changed by authenticated and authorised users.	≥ 1
CR 1.5 RE 1	Hardware security for authenticators	✘	---	≥ 3
NDR 1.6	Wireless access management	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NDR 1.6 RE 1	Unique identification and authentication	N/A	Not applicable because the requirement only applies to network components.	≥ 2
CR 1.7	Strength of password-based authentication	✔	The user can configure a password policy.	≥ 1
CR 1.7 RE 1	Password generation and lifetime restrictions for human users	✘	---	≥ 3
CR 1.7 RE 2	Password lifetime restrictions for all users (human, software process or device)	✘	---	4
CR 1.8	Public key infrastructure certificates	✔	Supported to the extent required for the following interfaces: ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p	≥ 2
CR 1.9	Strength of public key-based authentication	✔	Supported to the extent required.	≥ 2
CR 1.9 RE 1	Hardware security for public key-based authentication	✘	---	≥ 3

ID	Requirement	Met	Note	SL
CR 1.10	Authenticator feedback	✔	A PSS 4000 device has no display element and no web application. In the event of a failed authentication attempt, feedback regarding the failure is provided, but no information is disclosed that could assist an attacker. For example, it does not specify whether the authentication failed because of an incorrect password or an unknown user name.	≥ 1
CR 1.11	Unsuccessful login attempts	✔	Supported to the extent required.	≥ 1
CR 1.12	System use notification	N/A	Not applicable because a PSS 4000 device has no display element and no web application.	≥ 1
NDR 1.13	Access via untrusted networks	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NDR 1.13 RE 1	Explicit access request approval	N/A	Not applicable because the requirement only applies to network components.	≥ 3
CR 1.14	Strength of symmetric key-based authentication	N/A	Not applicable because symmetric key-based authentication is not used.	≥ 2
CR 1.14 RE 1	Hardware security for symmetric key-based authentication	N/A	Not applicable because symmetric key-based authentication is not used.	≥ 3

FR 2 - Use control

ID	Requirement	Met	Note	SL
CR 2.1	Authorization enforcement	✔	In user management, permissions are assigned to users indirectly via roles. In each case, users should only be assigned the roles required for their specific task. If a role is no longer required, it can be revoked from a user.	≥ 1
CR 2.1 RE 1	Authorization enforcement for all users (humans, software processes and devices)	✔	Roles are applied equally to human users and to devices/software processes.	≥ 2
CR 2.1 RE 2	Permission mapping to roles	✔	The mapping of permissions to roles can be changed. A user must have the relevant permission to carry out this action. In its factory settings, there is a predefined role, which has permission to manage roles. Note: Roles are not hierarchical. A user can hold several roles at the same time.	≥ 2
CR 2.1 RE 3	Supervisor override	✖	---	≥ 3
CR 2.1 RE 4	Dual approval	✖	---	4

ID	Requirement	Met	Note	SL
CR 2.2	Wireless use control	N/A	Not applicable because PSS 4000 devices do not have any wireless interfaces.	≥ 1
CR 2.3	Use control for portable and mobile devices	N/A	This requirement does not apply to components.	---
SAR 2.4	Mobile code	N/A	Not applicable because the requirement only applies to software applications.	≥ 1
SAR 2.4 RE 1	Mobile code authenticity check	N/A	Not applicable because the requirement only applies to software applications.	≥ 2
EDR 2.4	Mobile code	N/A	Not applicable because PSS 4000 devices do not support mobile code.	≥ 1
EDR 2.4 RE 1	Mobile code authenticity check	N/A	Not applicable because PSS 4000 devices do not support mobile code.	≥ 2
HDR 2.4	Mobile code	N/A	Not applicable because the requirement only applies to host devices.	≥ 1
HDR 2.4 RE 1	Mobile code authenticity check	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 2.4	Mobile code	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NDR 2.4 RE 1	Mobile code authenticity check	N/A	Not applicable because the requirement only applies to network components.	≥ 2
CR 2.5	Session lock	N/A	Not applicable because a PSS 4000 device has no display element and no web application.	≥ 1
CR 2.6	Remote session termination	✔	Supported to the extent required.	≥ 2
CR 2.7	Concurrent session control	✔	Supported to the extent required.	≥ 3
CR 2.8	Auditable events	✔	Supported to the extent required.	≥ 1
CR 2.9	Audit storage capacity	✔	A dedicated memory area is reserved for entries in the diagnostic log. It is used solely for this purpose. The memory area is organised as a ring buffer; i.e. if sufficient memory is no longer available, the oldest entries are overwritten.	≥ 1
CR 2.9 RE 1	Warn when audit record storage capacity threshold reached	✖	---	≥ 3
CR 2.10	Response to audit processing failures	✔	An error when generating a log entry has no impact on other system services.	≥ 1
CR 2.11	Timestamps	✔	We recommend that you synchronise the time with an SNTP Server.	≥ 1
CR 2.11 RE 1	Time synchronization	✔	This is achieved by synchronising the time with an SNTP Server.	≥ 2
CR 2.11 RE 2	Protection of time source integrity	✖	---	4

ID	Requirement	Met	Note	SL
CR 2.12	Non-repudiation	✔	For each action, the diagnostic log records the user who requested the action. The only exception is the reset button, as a physical control element.	≥ 1
CR 2.12 RE 1	Non-repudiation for all users	✖	---	4
EDR 2.13	Use of physical diagnostic and test interfaces	N/A	Not applicable because PSS 4000 devices (head modules and electronic modules) do not have any externally accessible diagnostic or test interfaces.	≥ 2
EDR 2.13 RE 1	Active monitoring	N/A	Not applicable because PSS 4000 devices (head modules and electronic modules) do not have any externally accessible diagnostic or test interfaces.	≥ 3
HDR 2.13	Use of physical diagnostic and test interfaces	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
HDR 2.13 RE 1	Active monitoring	N/A	Not applicable because the requirement only applies to host devices.	≥ 3
NDR 2.13	Use of physical diagnostic and test interfaces	N/A	Not applicable because the requirement only applies to network components.	≥ 2
NDR 2.13 RE 1	Active monitoring	N/A	Not applicable because the requirement only applies to network components.	≥ 3

FR 3 - System integrity

ID	Requirement	Met	Note	SL
CR 3.1	Communication integrity	✔	The following communication interfaces support cryptographic methods for integrity protection during communication: ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p The following communication interfaces use check sums for integrity protection during communication: ▸ Process data communication via SafetyNET p ▸ ProfiNET ▸ Ethernet/IP If the implemented security measures are used and the required external security measures are in place (see the PSS 4000 Safety and Security Manual), then integrity protection via cryptographic methods is not required for process data communication (SafetyNET p, PROFINET, EtherNet/IP, IP connections, I/O data from electronic modules).	≥ 1
CR 3.1 RE 1	Communication authentication	✔	The following communication interfaces support cryptographic methods for authenticity verification during communication ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p If the implemented security measures are used and the required external security measures are in place (see the PSS 4000 Safety and Security Manual), then authenticity verification via cryptographic methods is not required for process data communication (SafetyNET p, PROFINET, EtherNet/IP, IP connections, I/O data from electronic modules).	≥ 2
SAR 3.2	Protection from malicious code	N/A	Not applicable because the requirement only applies to software applications.	≥ 1

ID	Requirement	Met	Note	SL
EDR 3.2	Protection from malicious code	✔	It is only possible to install new firmware on a PSS 4000 device (head module and electronic module). The installation or execution of unauthorised firmware is prevented by the following measures: ▸ When a head module's firmware is updated, the signature of the new firmware is verified. When an electronic module's firmware is updated, the signature of the new firmware is verified. ▸ Each time a PSS 4000 device is started, the head module's firmware signature is verified.	≥ 1
HRD 3.2	Protection from malicious code	N/A	Not applicable because the requirement only applies to host devices.	≥ 1
HDR 3.2 RE 1	Protection from malicious code	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 3.2	Protection from malicious code	N/A	Not applicable because the requirement only applies to network components.	≥ 1
CR 3.3	Security functionality verification	✔	Tests can be performed to verify the security measures that have been implemented. These tests can verify the following: ▸ The expected system reaction (e.g. action performed or rejected). ▸ When a test is verifying the error reaction, the expected security entry(ies) in the diagnostic log.	≥ 1
CR 3.3 RE 1	Security functionality verification during normal operation	✘	---	4
CR 3.4	Software and information integrity	✔	Encrypting the SD card provides integrity and authenticity protection for the entire configuration.	≥ 1
CR 3.4 RE 1	Authenticity of software and information	✔	See CR 3.4	≥ 2
CR 3.4 RE 2	Automated notification of integrity violations	✘	---	≥ 3
CR 3.5	Input validation	✔	Configuration data and external I-data (input data that comes from the system sections for external communication, e.g. from EtherNet/IP) is verified.	≥ 1
CR 3.6	Deterministic output	✔	If the values for outgoing process data can no longer be determined, they are marked as invalid and overwritten with safe values.	≥ 1

ID	Requirement	Met	Note	SL
CR 3.7	Error handling	✔	Users who do not have the appropriate authorisation cannot access the diagnostic log. Security-related information requires additional permissions.	≥ 1
CR 3.8	Session integrity	✔	The requirement is supported to the extent required for the following interfaces: ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p If the implemented security measures are used and the required external security measures are in place (see the PSS 4000 Safety and Security Manual), no session integrity measures are required for process data communication (SafetyNET p, PROFINET, EtherNet/IP, IP connections).	≥ 2
CR 3.9	Protection of audit information	✔	The information to be protected is in the diagnostic log. The diagnostic log is stored internally within the device. For read access to the log, a user must have the required permissions. To clear the diagnostic log, a user must have additional permission.	≥ 2
CR 3.9 RE 1	Audit records on write-once media	✖	---	4
EDR 3.10	Support for updates	✔	The user can update the firmware on PSS 4000 devices (head modules and electronic modules).	≥ 1
ERD 3.10 RE 1	Update authenticity and integrity	✔	When a head module's firmware is updated, the signature of the new firmware is verified. When an electronic module's firmware is updated, the signature of the new firmware is verified.	≥ 2
HDR 3.10	Support for updates	N/A	Not applicable because the requirement only applies to host devices.	≥ 1
HRD 3.10 RE 1	Update authenticity and integrity	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 3.10	Support for updates	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NRD 3.10 RE 1	Update authenticity and integrity	N/A	Not applicable because the requirement only applies to network components.	≥ 2

ID	Requirement	Met	Note	SL
EDR 3.11	Physical tamper resistance and detection	✔▪	The SD card in a PSS 4000 device can be protected against easy removal or exchange, as described in the operating manual. The user must prevent tampering through physical access to the PSS 4000 device by implementing external measures in accordance with their risk assessment.	≥ 2
ERD 3.11 RE 1	Notification of a tampering attempt	✖	---	≥ 3
HDR 3.11	Physical tamper resistance and detection	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
HRD 3.11 RE 1	Notification of a tampering attempt	N/A	Not applicable because the requirement only applies to host devices.	≥ 3
NDR 3.11	Physical tamper resistance and detection	N/A	Not applicable because the requirement only applies to network components.	≥ 2
NRD 3.11 RE 1	Notification of a tampering attempt	N/A	Not applicable because the requirement only applies to network components.	≥ 3
EDR 3.12	Provisioning product supplier roots of trust	✔	Supported to the extent required.	≥ 2
HDR 3.12	Provisioning product supplier roots of trust	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 3.12	Provisioning product supplier roots of trust	N/A	Not applicable because the requirement only applies to network components.	≥ 2
EDR 3.13	Provisioning asset owner roots of trust	✔	The user can store the following "roots of trust" on the PSS 4000 device: ▸ Key for encrypting the SD card ▸ Trust List containing the lists Trusted Certs, Trusted CRLs, Issuer Certs and Issuer CRLs Changes to the "roots of trust" are subject to user management. The "roots of trust" are stored directly on the PSS 4000 device. The encryption key for the SD card is stored internally; there is no read function. If required, the Trust List can be stored on the SD card. On the SD card, the Trust List is protected if the SD card is encrypted and user management is used to grant access exclusively to authorised users.	≥ 2
HDR 3.13	Provisioning asset owner roots of trust	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 3.13	Provisioning asset owner roots of trust	N/A	Not applicable because the requirement only applies to network components.	≥ 2

ID	Requirement	Met	Note	SL
EDR 3.14	Integrity of the boot process	✔	Each time a PSS 4000 device is started, the head module's firmware signature is verified. The integrity of the configuration is guaranteed if the SD card is encrypted and user management is used to grant access exclusively to authorised users.	≥ 1
EDR 3.14 RE 1	Authenticity of the boot process	✔	Supported to the extent required.	≥ 2
HDR 3.14	Integrity of the boot process	N/A	Not applicable because the requirement only applies to host devices.	≥ 1
HDR 3.14 RE 1	Authenticity of the boot process	N/A	Not applicable because the requirement only applies to host devices.	≥ 2
NDR 3.14	Integrity of the boot process	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NDR 3.14 RE 1	Authenticity of the boot process	N/A	Not applicable because the requirement only applies to network components.	≥ 2

FR 4 - Data confidentiality

ID	Requirement	Met	Note	SL
CR 4.1	Information confidentiality	✔	Information at rest: Encrypting the SD card ensures that all data stored there remains confidential. For the following interfaces, the confidentiality of information during transmission is supported to the extent required: ▸ PAS4000 programming interface ▸ OPC UA ▸ Event communication with other PSS 4000 devices via SafetyNET p	≥ 1
CR 4.2	Information persistence	✔	There is a dedicated command that clears the diagnostic log. An original reset clears all the data from a PSS 4000 device, but not the diagnostic log.	≥ 2
CR 4.2 RE 1	Erase of shared memory resources	✖	---	≥ 3
CR 4.2 RE 2	Erase verification	✖	---	≥ 3
CR 4.3	Use of cryptography	✔	Supported to the extent required.	≥ 1

FR 5 - Restricted data flow

ID	Requirement	Met	Note	SL
CR 5.1	Network segmentation	✔	PSS 4000 devices use IP-based communication. For IP networks, infrastructure components that support network segmentation are widely available on the market. Additional options for integration into a segmented network infrastructure are supported via the advanced network configuration.	≥ 1
NDR 5.2	Zone boundary protection	N/A	Not applicable because the requirement only applies to network components.	≥ 1
NDR 5.2 RE 1	Deny all, permit by exception	N/A	Not applicable because the requirement only applies to network components.	≥ 2
NDR 5.2 RE 2	Deny all, permit by exception	N/A	Not applicable because the requirement only applies to network components.	≥ 3
NDR 5.2 RE 3	Fail close	N/A	Not applicable because the requirement only applies to network components.	≥ 3
NDR 5.3	General-purpose person-to-person communication restrictions	N/A	Not applicable because the requirement only applies to network components.	≥ 1

FR 6 - Timely response to events

ID	Requirement	Met	Note	SL
CR 6.1	Audit log accessibility	✔	For read access to the diagnostic log, a user must have the required permissions. To clear the diagnostic log, a user must have additional permission.	≥ 1
CR 6.1 RE 1	Programmatic access to audit logs	✔	Programmatic access is possible via OPC UA.	≥ 3
CR 6.2	Continuous monitoring	✔	The diagnostic list and diagnostic log of a PSS 4000 device (including security entries) can be continuously monitored by an authorised process via OPC UA or by an authorised user. PSS 4000 devices use IP-based communication. IP networks can be monitored for suspicious activity or denial-of-service attacks using standard market tools.	≥ 2

FR 7 - Resource availability

ID	Requirement	Met	Note	SL
CR 7.1	Denial of service protection	✔	The assured properties with regard to functional safety are maintained even in the event of a DoS attack. DoS impact on incoming process data: A DoS event (on the network or at the sender's end) may mean that incoming process data arrives late or not at all. In this case, the incoming process data is marked as invalid and overwritten with safe values. DoS impact on the PSS 4000 device itself: A DoS event that impacts the PSS 4000 device itself may mean that the device cannot complete its data processing in time. This leads to a major FS error, as a result of which the generated process data is marked as invalid and overwritten with safe values. Note: To guarantee that the PSS 4000 device remains accessible even in DoS situations, it is recommended that you use a firewall that limits the rate of incoming data per destination IP address.	≥ 1
CR 7.1 RE 1	Manage communication load from component	✔	The outgoing data traffic from a PSS 4000 device is determined by the device project. It is not possible for incoming external data traffic to cause the PSS 4000 device to generate additional network messages.	≥ 2
CR 7.2	Resource management	✔	All security functions are limited in terms of the amount of memory they can occupy. For example, the number of configurable user accounts, device accounts and roles is limited.	≥ 1

ID	Requirement	Met	Note	SL
CR 7.3	Control system backup	✔▪	A direct backup function is not currently provided, but users can set this up themselves. The following steps are required: 1. The user must create an archive containing the following data: a) For each PSS 4000 device in the system, the naming data and the encryption key for the SD card. b) For each PSS 4000 device in the system, an image of the SD card that is plugged into the device. The archive must be updated after each change. 2. The user must back up the values of the non-volatile variables at regular intervals during runtime (e.g. by reading them via an OPC Client). The frequency of backups should be based on how often the non-volatile data changes.	≥ 1
CR 7.3 RE 1	Backup integrity verification	✔	The user must ensure and verify the integrity of parts 1.a) and 2. of the backup. By encrypting the SD card, the PSS 4000 device can verify the integrity of the SD card itself.	≥ 2
CR 7.4	Control system recovery and reconstitution	✔	An original reset can be used to restore a PSS 4000 device to its factory settings (secure default); in this case, only the diagnostic log remains on the device. From this point, the device can be reprogrammed or restored from the archive (see CR 7.3).	≥ 1
CR 7.5	Emergency power	N/A	This requirement does not apply to components.	---
CR 7.6	Network and security configuration settings	✔	The recommended settings can be found in the Safety and Security Manual. The current settings can be read via the OPC UA namespace.	≥ 1
CR 7.6 RE 1	Machine-readable reporting of current security settings	✖	---	≥ 3

ID	Requirement	Met	Note	SL
CR 7.7	Least functionality	✔	With regard to configurable functions: ports, protocols or services are only used if the user has configured that function. Essential functions of the PSS 4000 device and its protocols and ports are described in the network data sheet. Using this information, the user can restrict access to these functions through measures at network level.	≥ 1
CR 7.8	Control system component inventory	✔▪	A software bill of materials is available for all Pilz products on request. In PAS4000, a bill of materials listing all the products used in a project's hardware configuration can be exported as a CSV file.	≥ 2

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 400-088-3566
Japan
+81 45 471-2281
South Korea
+82 31 778 3390

Australia and Oceania
Australia
+61 3 95600621
New Zealand
+64 9 6345350

Europe
Austria
+43 1 7986263-444
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Türkiye
+90 216 5775552
United Kingdom
+44 1536 460866

You can reach our international hotline on:
+49 711 3409-222
support@pilz.com

Reporting security vulnerabilities or security incidents
If you would like to report a security vulnerability or a security incident in connection with a Pilz product, please contact our **Pilz Product Security Incident Response Team (PSIRT).**
You can reach us at: www.pilz.com/psirt

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

BLUeCOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

German Standards BRAND OF THE CENTURY 2025

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/linkedin
www.pilz.com/youtube

1007475-EN-01, 2026-07 Printed in Germany
© Pilz GmbH & Co. KG, 2024

CECE, CHRE, CMSE®, IndustrialPI®, Leansafe®, MYZEL®, PAS4000®, PAScal®, PASconfig®, Pilz®, PIT®, PMCprimo®, PMCprotego®, PMCtendo®, PMD®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ
THE SPIRIT OF SAFETY