SIEMENS

SIMATIC
S7-1500/ET 200MP, S7-1500R/H, SIMATIC Drive Controller, SIMATIC S7-1500 Software Controller, ET 200SP, ET 200pro

Product Information about Syslog Messages

Product Information

Introduction

Scope of validity of the product information

This product information supplements the documentation for SIMATIC S7-1500/ET 200MP, S7-1500R/H, SIMATIC Drive Controller, SIMATIC S7-1500 Software Controller, ET 200SP, ET 200pro.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For more information on industrial cybersecurity measures that may be implemented, please visit (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (https://new.siemens.com/global/en/products/services/cert.html).

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Product Information about Syslog Messages
A5E53245873-AB, 11/2024

Table of Contents

Chapter 1. Event Details

1.1. SE_LOCAL_SUCCESSFUL_LOGON

ID	1
Parameter	fct, result
Description	Valid credentials provided by local logon.
Comment	Successful login of on-site-user, e.g. PLC Display user.
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Informational

1.2. SE_LOCAL_UNSUCCESSFUL_LOGON

ID	2
Parameter	fct, result, errReason
Description	Wrong user name or wrong password (credentials) provided by local logon.
Comment	Unsuccessful login of on-site-user, e.g. PLC Display user.
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Error

1.3. SE_NETWORK_SUCCESSFUL_LOGON

ID	3
Parameter	fct
Description	Valid credentials provided by remote logon.
Comment	This event indicates a successful login of a remote user.
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Informational

1.4. SE_NETWORK_UNSUCCESSFUL_LOGON

ID	4
Parameter	fct, errReason
Description	Wrong user name or wrong password (credentials) provided by remote logon.
Comment	This event indicates a failed login attempt of a remote user.
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Error

1.5. SE_LOGOFF

ID	5
Parameter	fct, errReason
Description	User session ended - logout.
Comment	A user is logged out.
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Informational

1.6. SE_DEFAULT_USER_AUTHENTICATION_USED

ID	6
Parameter	fct, result
Description	User logged in with default user name and password.
Comment	Default user credentials are used for session creation, e.g. the 'Anonymous' user.
Requirement	SR 1.5 - Authenticator management
Severity	Informational

1.7. SE_ACCESS_PWD_ENABLED

ID	11
Parameter	fct, resource, result
Description	Password protection was enabled for some resource.
Comment	The password for a protection level is enabled, e.g. by PLC Display.
Requirement	SR 1.3 - Account management
Severity	Notice

1.8. SE_ACCESS_PWD_DISABLED

ID	12
Parameter	fct, resource, result
Description	Password protection was disabled for some resource.
Comment	The password for a protection level is disabled, e.g. by user program.
Requirement	SR 1.3 - Account management
Severity	Notice

1.9. SE_ACCESS_PWD_CHANGED

ID	13
Parameter	fct, errReason, result
Description	User changed his password.
Comment	The password for a given user is changed.
Requirement	SR 1.3 - Account management
Severity	Notice

1.10. SE_ACCESS_GRANTED

ID	19
Parameter	fct, functionRight, result
Description	Restricted access was granted for an user.
Comment	Access is granted to this user to perform a service.
Requirement	SR 2.1 - Authorization enforcement
Severity	Informational

1.11. SE_ACCESS_DENIED

ID	20
Parameter	fct, functionRight
Description	Restricted access was denied for an user.
Comment	Due to lack of rights the access is denied to this user to perform a service.
Requirement	SR 2.1 - Authorization enforcement
Severity	Error

1.12. SE_ACCESS_DENIED_NUMBER_OF_CONCURRENT_SESSIONS_EXCEEDED

ID	51
Parameter	fct, result
Description	When the maximum number of concurrent sessions is exceeded, this event will be raised.
Comment	A login attempt failed due to limited resources. Severity "Error" is used for all products listed in this Product Information
Requirement	SR 2.7 - Concurrent session control
Severity	Warning

1.13. SE_CRITICAL_DEVICE_STARTED

ID	52
Parameter	fct, resource
Description	(Initial) start-up of a critical device.
Comment	An application or component is started (e.g. the Webserver or OPCUA-Server).
Requirement	SR 2.8 RE 1 - Centrally managed, system-wide audit trail
Severity	Notice

1.14. SE_CRITICAL_DEVICE_STOPPED

ID	53
Parameter	fct, resource
Description	Shut down of a critical device.
Comment	An application or component is stopped (e.g. the Webserver or OPCUA-Server). Severity "Notice" is used for all products listed in this Product Information
Requirement	SR 2.8 RE 1 - Centrally managed, system-wide audit trail
Severity	Alert

1.15. SE_AUDIT_EVENTS_OVERWRITTEN

ID	56
Parameter	fct
Description	Ring buffer is full. Audit Trail starts to overwrite old events.
Comment	Events are overwritten and were not transferred to a syslog server. Information is lost. This event will only be triggered when a syslog server is configured. Severity "Error" is used for all products listed in this Product Information
Requirement	SR 2.10 - Response to audit processing failures
Severity	Alert

1.16. SE_OPEN_RESOURCE

ID	61
Parameter	fct, resource, result
Description	Open the handle of an object.
Comment	A file or folder is opened for read or write access.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.17. SE_CLOSE_RESOURCE

ID	62
Parameter	fct, resource
Description	Close the handle of an object.
Comment	A file or folder is closed after read or write access.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.18. SE_DELETE_OBJECT

ID	63
Parameter	fct, resource, result
Description	Delete an object.
Comment	An object is deleted (details in parameters) or the memory card is formatted.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.19. SE_OBJECT_OPERATION

ID	64
Parameter	fct, resource, newState, resOper, result
Description	Access an object.
Comment	An operation (see parameter fct) is executed on an object (see parameter resource).
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.20. SE_SESSION_CLOSED

ID	75
Parameter	-
Description	Session closed.
Comment	A session is closed.
Requirement	SR 3.8 - Session integrity
Severity	Informational

1.21. SE_INVALID_SESSION_ID

ID	76
Parameter	-
Description	Session is invalid.
Comment	An invalid session ID is detected.
Requirement	SR 3.8 - Session integrity
Severity	Error

1.22. SE_BACKUP_STARTED

ID	79
Parameter	-
Description	Backup started.
Comment	Creation of a backup file is started.
Requirement	SR 7.3 - Control system backup
Severity	Notice

1.23. SE_BACKUP_SUCCESSFULLY_DONE

ID	80
Parameter	-
Description	Backup finished.
Comment	Creation of a backup file is finished successfully.
Requirement	SR 7.3 - Control system backup
Severity	Notice

1.24. SE_BACKUP_FAILED

ID	81
Parameter	-
Description	Backup failed.
Comment	Creation of a backup file failed.
Requirement	SR 7.3 - Control system backup
Severity	Error

1.25. SE_BACKUP_RESTORE_STARTED

ID	85
Parameter	fct, resource, dateAndTime
Description	Restore started.
Comment	Restore of a backup file is started.
Requirement	SR 7.4 - Control system recovery and reconstitution
Severity	Notice

1.26. SE_BACKUP_RESTORE_FAILED

ID	86
Parameter	-
Description	Restore failed.
Comment	Restore of a backup file failed.
Requirement	SR 7.4 - Control system recovery and reconstitution
Severity	Error

1.27. SE_BACKUP_RESTORE_SUCCESSFULLY_DONE

ID	87
Parameter	-
Description	Restore finished.
Comment	Restore of a backup file is finished successfully.
Requirement	SR 7.4 - Control system recovery and reconstitution
Severity	Notice

1.28. SE_SECURITY_CONFIGURATION_CHANGED

ID	94
Parameter	fct, result
Description	Security configuration data changed.
Comment	A security-relevant configuration change is performed for the given application (e.g. certificate management or user configuration).
Requirement	SR 7.6 - Network and security configuration settings
Severity	Notice

1.29. SE_SESSION_ESTABLISHED

ID	95
Parameter	fct, result
Description	A session is created after a successful login from a client.
Comment	A session is established, e.g. when an open secure channel request is processed by OPC UA.
Requirement	-
Severity	Informational

1.30. SE_CFG_DATA_CHANGED

ID	96
Parameter	fct, interface, MACaddress, IPv4Suite, NTPserver, DNSserver, hostName, domainName, PNDeviceName, resource, result, resOper, withMeasurements
Description	Significant configuration changed. E.g. a new project configuration was loaded to the device.
Comment	A configuration change is performed for the given application (e.g. HW-Configuration, DCP commands or DHCP notifications). Detailed information is contained in parameters.
Requirement	-
Severity	Notice

1.31. SE_USER_PROGRAM_CHANGED

ID	97
Parameter	fct, result, checksum
Description	A program that is executed by the device is modified.
Comment	User program is changed by a download or is being prepared for execution after boot sequence.
Requirement	-
Severity	Notice

1.32. SE_OPMOD_CHANGED

ID	98
Parameter	fct, oldState, newState
Description	Operating mode is changed. This has an impact on the behavior of the device.
Comment	Operating mode of PLC is changed. A separate message informs about the originator of this command.
Requirement	-
Severity	Notice

1.33. SE_FIRMWARE_LOADED

ID	99
Parameter	fct, result
Description	Firmware successfully loaded.
Comment	A firmware is downloaded to PLC.
Requirement	-
Severity	Notice

1.34. SE_FIRMWARE_ACTIVATED

ID	100
Parameter	fct, oldState, newState
Description	Firmware successfully activated after download.
Comment	A firmware is activated after a successful download.
Requirement	-
Severity	Notice

1.35. SE_SYSTEMTIME_CHANGED

ID	101
Parameter	fct
Description	Modification of system time.
Comment	The system time of PLC is changed.
Requirement	-
Severity	Notice

1.36. SE_OPMOD_CHANGE_INITIATED

ID	102
Parameter	newState
Description	A client initiated a change of the operating state of the device.
Comment	A change of the operating mode is initiated. A separate message informs when the change is executed.
Requirement	SR 2.1 RE 1 - Authorization enforcement for all users
Severity	Notice

1.37. SE_RESET_TO_FACTORY

ID	103
Parameter	-
Description	The device is set back to facory settings. All data is set to default values and retentive buffers are empty.
Comment	PLC is reset to factory settings. This command deletes all retentive data on the device and initiates a reboot. It is not guaranteed that the message is sent before reboot to the syslog server. A separate message informs during subsequent boot up about the last reboot reason.
Requirement	SR 4.2 - Information persistence
Severity	Notice

1.38. SE_MEMORY_RESET

ID	104
Parameter	-
Description	A client initiates a reset of the user relevant memory areas.
Comment	Memory reset is performed and deletes all non-retentive data. Operating mode changes caused by this command are reported in separate messages.
Requirement	SR 4.2 - Information persistence
Severity	Notice

1.39. SE_SECURITY_STATE_CHANGE

ID	105
Parameter	fct, result
Description	The device itself or a subcomponent changed an important state.
Comment	An application or component is running in provisioning mode. Security may be lowered down as long as this special mode is active.
Requirement	CR 3.13 - Provisioning product supplier roots of trust
Severity	Notice

1.40. SE_DEVICE_STARTUP

ID	106
Parameter	fct, result
Description	The startup of the device itself (and not components inside) is indicated and provides additional information.
Comment	PLC is booting up after power on or a reboot sequence. The reason for the last shut down reason is given in the parameters.
Requirement	CR 3.14 - Integrity of the boot process
Severity	Notice

1.41. SE_TIME_SYNCHRONIZATION

ID	201
Parameter	fct, result
Description	Internal system time is affected by a change or issue of time synchronization.
Comment	Time synchronization is started, stopped, got lost or has returned.
Requirement	-
Severity	Notice

1.42. SE_DEVICE_CONNECTED

ID	301
Parameter	fct, interface
Description	USB device or SD card was connected, but not mounted.
Comment	A device is connected to PLC, e.g. Simatic memory card.
Requirement	-
Severity	Informational

1.43. SE_DEVICE_DISCONNECTED

ID	304
Parameter	interface
Description	USB device or SD card was disconnected.
Comment	External device (SMC, USB) has been disconnected.
Requirement	-
Severity	Informational

1.44. SE_SESSION_TERMINATED

ID	307
Parameter	fct, errReason
Description	A local or remote session was terminated due to missing operator acknowledgement, timeout or network issues.
Comment	The session to a PLC application is terminated.
Requirement	-
Severity	Notice

Chapter 2. Parameter Details

2.1. checksum

Description: overall signature for user program

2.2. dateAndTime

Description: date and time

2.3. devProduct

Description: Device Product Name

2.4. devVendor

Description: Device Vendor Name

2.5. DNSserver

Description: DNS server addresses

2.6. domainName

Description: domain name

2.7. errReason

Description: error reason

2.8. fct

Description: Function

2.9. functionRight

Description: the requested function right

2.10. FWVersion

Description: Firmware Version

2.11. hostName

Description: host name

2.12. interface

Description: interface name

2.13. IPv4Suite

Description: IP v4 Suite

2.14. MACaddress

Description: MAC address

2.15. newState

Description: new state or version

2.16. NTPserver

Description: NTP server addresses

2.17. oldState

Description: old state or version

2.18. PNDeviceName

Description: PROFINET device name

2.19. protocolType

Description: Protocol Type

2.20. resOper

Description: resOper

2.21. resource

Description: object or file name

2.22. result

Description: Result

2.23. sessionID

Description: Session ID

2.24. userMgmt

Description: type of the user authentication

2.25. userName

Description: name of the user

2.26. withMeasurements

Description: withMeasurements

Chapter 3. APP-NAME field content

AppName	Description
Backup/Restore	Software component implementing Online Backup and Restore
Cert-Store	Software component implementing certificate management
DCP-Server	DCP server
DHCP-Client	DHCP client
Display	Display of PLC
FW-Update	Software component managing firmware update
HW-Configuration	Software component managing hardware configuration
Memory-Card	Software component managing Memory Card
Memory-Mgt	Memory management
OPCUA-Server	Software component OPC UA
Operating-Mode-Mgt	Software component managing operating mode changes
PG/HMI-Comm	Software component managing the communication to Engineering system and HMI devices
PLC-Program	Software component for user program execution
PUT-GET-Server	Server for PUT/GET access from a client via unsecured S7 communication
RIB	Software component Real-time information backbone on a SIMATIC IPC with an S7 1500 Software Controller
Syslog	Software component syslog
Test-Functions	Test system for commissioning
Text-Lists	Text list manager
Time-System	Software component responsible for time system
UMAC	User management and access control
Webserver	Software component web server

Chapter 4. Requirements

4.1. CR 3.10 - Support for updates

Description	The support for updates requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15. (Specific information for several device types can be found in EDR 3.10, HDR 3.10 and NDR 3.10)
Source	IEC 62443-4-2:2019

4.2. CR 3.13 - Provisioning product supplier roots of trust

Description	The provisioning product supplier roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15. (Specific information for several device types can be found in EDR 3.13, HDR 3.13 and NDR 3.13)
Source	IEC 62443-4-2:2019

4.3. CR 3.14 - Integrity of the boot process

Description	The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15. (Specific information for several device types can be found in EDR 3.14, HDR 3.14 and NDR 3.14)
Source	IEC 62443-4-2:2019

4.4. SR 1.11 - Unsuccessful login attempts

Description	The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.
Source	IEC 62443-3-3:2013

4.5. SR 1.13 - Access via untrusted networks

Description	The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.
Source	IEC 62443-3-3:2013

4.6. SR 1.1 RE 1 - Unique identification and authentication

Description	The control system shall provide the capability to uniquely identify and authenticate all human users.
Source	IEC 62443-3-3:2013

4.7. SR 1.1 RE 2 - Multifactor authentication for untrusted networks

Description	The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 - Access via untrusted networks).
Source	IEC 62443-3-3:2013

4.8. SR 1.1 RE 3 - Multifactor authentication for all networks

Description	The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.
Source	IEC 62443-3-3:2013

4.9. SR 1.2 - Software process and device identification and authentication

Description	The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.
Source	IEC 62443-3-3:2013

4.10. SR 1.3 - Account management

Description	The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.
Source	IEC 62443-3-3:2013

4.11. SR 1.4 - Identifier management

Description	The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.
Source	IEC 62443-3-3:2013

4.12. SR 1.5 - Authenticator management

Description	The control system shall provide the capability to: h) initialize authenticator content; i) change all default authenticators upon control system installation; j) change/refresh all authenticators; and k) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.
Source	IEC 62443-3-3:2013

4.13. SR 2.1 - Authorization enforcement

Description	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.
Source	IEC 62443-3-3:2013

4.14. SR 2.10 - Response to audit processing failures

Description	The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.
Source	IEC 62443-3-3:2013

4.15. SR 2.12 - Non-repudiation

Description	The control system shall provide the capability to determine whether a given human user took a particular action.
Source	IEC 62443-3-3:2013

4.16. SR 2.1 RE 1 - Authorization enforcement for all users

Description	On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.
Source	IEC 62443-3-3:2013

4.17. SR 2.1 RE 3 - Supervisor override

Description	The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence.
Source	IEC 62443-3-3:2013

4.18. SR 2.1 RE 4 - Dual approval

Description	The control system shall support dual approval where an action can result in serious impact on the industrial process.
Source	IEC 62443-3-3:2013

4.19. SR 2.2 - Wireless use control

Description	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.
Source	IEC 62443-3-3:2013

4.20. SR 2.5 - Session lock

Description	The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.
Source	IEC 62443-3-3:2013

4.21. SR 2.6 - Remote session termination

Description	The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.
Source	IEC 62443-3-3:2013

4.22. SR 2.7 - Concurrent session control

Description	The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.
Source	IEC 62443-3-3:2013

4.23. SR 2.8 RE 1 - Centrally managed, system-wide audit trail

Description	The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system-wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).
Source	IEC 62443-3-3:2013

4.24. SR 2.9 RE 1 - Warn when audit record storage capacity threshold reached

Description	The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.
Source	IEC 62443-3-3:2013

4.25. SR 3.1 - Communication integrity

Description	The control system shall provide the capability to protect the integrity of transmitted information.
Source	IEC 62443-3-3:2013

4.26. SR 3.2 - Malicious code protection

Description	The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.
Source	IEC 62443-3-3:2013

4.27. SR 3.4 - Software and information integrity

Description	The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.
Source	IEC 62443-3-3:2013

4.28. SR 3.7 - Error handling

Description	The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.
Source	IEC 62443-3-3:2013

4.29. SR 3.8 - Session integrity

Description	The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.
Source	IEC 62443-3-3:2013

4.30. SR 3.9 - Protection of audit information

Description	The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.
Source	IEC 62443-3-3:2013

4.31. SR 3.9 RE 1 - Audit records on write-once media

Description	The control system shall provide the capability to produce audit records on hardware-enforced write-once media.
Source	IEC 62443-3-3:2013

4.32. SR 4.2 - Information persistence

Description	The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.
Source	IEC 62443-3-3:2013

4.33. SR 7.1 - Denial of service protection

Description	The control system shall provide the capability to operate in a degraded mode during a DoS event.
Source	IEC 62443-3-3:2013

4.34. SR 7.3 - Control system backup

Description	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.
Source	IEC 62443-3-3:2013

4.35. SR 7.3 RE 1 - Backup verification

Description	The control system shall provide the capability to verify the reliability of backup mechanisms.
Source	IEC 62443-3-3:2013

4.36. SR 7.4 - Control system recovery and reconstitution

Description	The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.
Source	IEC 62443-3-3:2013

4.37. SR 7.5 - Emergency power

Description	The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
Source	IEC 62443-3-3:2013

4.38. SR 7.6 - Network and security configuration settings

Description	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.
Source	IEC 62443-3-3:2013

Chapter 5. Severities

5.1. Alert

Value	1
Meaning	System conditions requiring immediate attention. E.g. corrupted system database, insufficient disk space, run out of file descriptors, audit log corrupt / stopped / deleted.

5.2. Critical

Value	2
Meaning	Indicates failure in a primary system. Mostly serious system/application malfunctioning, such as failing hardware (hard device errors) or software. Usually non-recoverable. E.g. H-System not available.

5.3. Error

Value	3
Meaning	Mostly correctable errors, for example errors other than hardware device errors. Continuation of the operation is possible. Usually all error conditions are automatically recoverable. E.g. autentication / autorisation failures, CPU and resource issues, any problems that do not infect 'normal operation'.

5.4. Warning

Value	4
Meaning	Not an error, but indication that an error will occur if action is not taken. E.g. file system 85% full.

5.5. Notice

Value	5
Meaning	Events that are unusual but not error conditions. Change of any authorized security setting. Non-error conditions that might require special handling. E.g. configuration event, commands executed by user (after successful authentication), change of security policy by administrator, activation AV scanner.

5.6. Informational

Value	6
Meaning	Normal operational messages based on valid security policy. E.g. successful autentication / autorisation event, commands executed by user (after successful authentication), firewall has passed a frame (only by special FW-setting).