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-AA, 11/2023

Table of Contents

Chapter 1. Event Details

1.1. SE_LOCAL_SUCCESSFUL_LOGON

ID	1
Parameter	fct, result, rhCPU
Description	Valid credentials provided by local logon.
Comment	-
Requirement	SR 1.1 RE 1 - Unique identification and authentication
Severity	Informational

1.2. SE_LOCAL_UNSUCCESSFUL_LOGON

ID	2
Parameter	fct, parameter, result, errReason, rhCPU
Description	Wrong user name or wrong password (credentials) provided by local logon.
Comment	-
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.
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.
Requirement	SR 1.1 RE 1 - Unique identification and authentication

ID	4
Severity	Error

1.5. SE_LOGOFF

ID	5
Parameter	fct, errReason, rhCPU
Description	User session ended - logout.
Comment	This event indicates a terminated user session due to a requested logout.
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	This event indicates a successful login of 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	This event indicates that the protection level has been enabled for particular item.
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	This event indicates that the protection level has been disabled for particular item.
Requirement	SR 1.3 - Account management

ID	12
Severity	Notice

1.9. SE_ACCESS_PWD_CHANGED

ID	13
Parameter	fct, errReason, result
Description	User changed his password.
Comment	This event indicates that the password for a given user has been successfully changed.
Requirement	SR 1.3 - Account management
Severity	Notice

1.10. SE_ACCESS_GRANTED

ID	19
Parameter	fct, functionRight, parameter, result
Description	Restricted access was granted for an user.
Comment	-
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	This event indicates that access to a defined function has been refused due to the lack of the required function right.
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	This event indicates a failed login attempt due to limited resources.
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 or application.
Comment	This event indicates that an application has been started (e.g. web server, OPCUA or PUT/GET-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 or application.
Comment	This event indicates that an application has been stopped (e.g. web server, OPCUA or PUT/GET-Server).
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	This event will only be triggered when a syslog server is configured.
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	This event indicates that a file or a folder is opened.
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	This event indicates that a file or a folder is closed.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.18. SE_DELETE_OBJECT

ID	63
Parameter	fct, resource, result
Description	Delete an object.
Comment	This event indicates that a file, a folder or the user program is deleted or the Simatic Memory Card is formatted.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.19. SE_OBJECT_OPERATION

ID	64
Parameter	fct, resource, resOper, result
Description	Access an object.
Comment	This event indicates that a folder is created, a file or folder is renamed or the file system is browsed.
Requirement	SR 2.12 - Non-repudiation
Severity	Informational

1.20. SE_SESSION_CLOSED

ID	75
Parameter	-
Description	Session closed.
Comment	-
Requirement	SR 3.7 - Error handling
Severity	Informational

1.21. SE_INVALID_SESSION_ID

ID	76
Parameter	-
Description	Session is invalid.
Comment	This event indicates that access to a defined function has been refused due to an invalid Session ID.
Requirement	SR 3.7 - Error handling
Severity	Error

1.22. SE_BACKUP_STARTED

ID	79
Parameter	-
Description	Backup started.
Comment	Start of a backup operation
Requirement	SR 7.3 - Control system backup
Severity	Notice

1.23. SE_BACKUP_SUCCESSFULLY_DONE

ID	80
Parameter	-
Description	Backup finished.
Comment	This event indicates that an online backup finished successfully.
Requirement	SR 7.3 - Control system backup
Severity	Notice

1.24. SE_BACKUP_FAILED

ID	81
Parameter	-
Description	Backup failed.
Comment	This event indicates that an online backup creation 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	This event indicates that restoration of an online backup file 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	This event indicates that restoration of an online backup file failed.
Requirement	SR 7.4 - Control system recovery and reconstitution
Severity	Error

1.27. SE_SECURITY_CONFIGURATION_CHANGED

ID	94
Parameter	fct, result
Description	Security configuration data changed.
Comment	This event indicates that an security-relevant configuration change has been performed for the given application (e.g. download of user configuration).
Requirement	SR 7.6 - Network and security configuration settings
Severity	Notice

1.28. SE_SESSION_ESTABLISHED

ID	95
Parameter	fct, result
Description	-
Comment	The event is created when OPC UA has processed an open secure channel request.
Requirement	-
Severity	-

1.29. SE_CFG_DATA_CHANGED

ID	96
Parameter	fct, interface, IPv4Suite, NTPserver, DNSserver, hostName, domainName, PNDeviceName, resource, result, resOper, withMeasurements
Description	-
Comment	This event indicates a change of the PLC configuration data.
Requirement	-
Severity	-

1.30. SE_USER_PROGRAM_CHANGED

ID	97
Parameter	fct, result
Description	-
Comment	This event indicates software program change.
Requirement	-
Severity	-

1.31. SE_OPMOD_CHANGED

ID	98
Parameter	fct, oldState, newState
Description	-
Comment	This event indicates that the operating mode has been changed.
Requirement	-
Severity	-

1.32. SE_FIRMWARE_LOADED

ID	99
Parameter	fct, result
Description	Firmware successfully loaded.
Comment	-
Requirement	-
Severity	-

1.33. SE_FIRMWARE_ACTIVATED

ID	100
Parameter	fct, oldState, newState
Description	-
Comment	Firmware successfully activated.
Requirement	-
Severity	-

1.34. SE_SYSTEMTIME_CHANGED

ID	101
Parameter	fct
Description	-
Comment	This event indicates that the system time has been changed.
Requirement	-
Severity	-

1.35. SE_OPMOD_CHANGE_INITIATED

ID	102
Parameter	newState, rhCPU
Description	A client (e.g. TIA-Portal) initiated a change of the operating state of the CPU. Please be aware that additional operating modes (e.g. RUN_REDUNDANT) exist on R/H CPUs. Since multiple clients can initiate such a change not all changes are really executed.
Comment	This event indicates that an application has initiated an operating mode change request.
Requirement	-

ID	102
Severity	Notice

1.36. SE_SECURITY_STATE_CHANGE

ID	105
Parameter	fct, result
Description	-
Comment	A component inside PLC changed the security state. Security may have lowered down, for example to allow an initial configuration (e.g. provisioning mode in OPC UA).
Requirement	-
Severity	-

1.37. SE_DEVICE_STARTUP

ID	106
Parameter	fct, result
Description	-
Comment	The device is started up and provides the previous shut down reason in the details.
Requirement	-
Severity	-

1.38. SE_TIME_SYNCHRONIZATION

ID	201
Parameter	fct, result
Description	-
Comment	This event indicates that time synchronisation started, stopped or got lost.
Requirement	-
Severity	-

1.39. SE_DEVICE_CONNECTED

ID	301
Parameter	fct, interface
Description	USB device or SD card was connected, but not mounted.

ID	301
Comment	External device (SMC, USB) has been connected.
Requirement	-
Severity	-

1.40. 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	-

1.41. 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	This event indicates a terminated user session due to a session timeout.
Requirement	-
Severity	-

Chapter 2. Parameter Details

2.1. dateAndTime

Description: date and time

2.2. devProduct

Description: Device Product Name

2.3. devVendor

Description: Device Vendor Name

2.4. DNSserver

Description: DNS server addresses

2.5. domainName

Description: domain name

2.6. errReason

Description: error reason

2.7. evt

Description: Test functions event

2.8. fct

Description: Function executed in PLC

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. job

Description: Test functions job

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: Result of an operation

2.21. resource

Description: object or file name

2.22. result

Description: Result of an executed function

2.23. rhCPU

Description: inside the R/H system the event is initiated locally on this or neighbour CPU

2.24. service

Description: system service name

2.25. sessionID

Description: Contains an identifier that allows the reader of the syslog to determine related syslog events

2.26. spt

Description: source port (UDP/TCP)

2.27. src

Description: source address

2.28. sTSel

Description: source Transport selector

2.29. userName

Description: name of the user

2.30. 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 the 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
ODK	Open Developement Kit
OPCUA-Server	Software component OPC UA
Operating-Mode-Mgt	Software component managing operating mode changes
PLC-Program	Software component for user program execution
PG/HMI-Comm	Software component managing the communication to Engineering system and HMI devices
PUT/GET-Server	Server for PUT/GET access from a client via unsecured S7 communication
Syslog	Software component syslog
RIB	Software component Real-time information backbone on a SIMATIC IPC with an S7 1500 Software Controller
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. 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
SecurityLevel	SL-C 2
Comment	SL-C 2 requires fullfilment of SR 1.1 and SR 1.1 RE 1.

4.2. 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
SecurityLevel	SL-C 3
Comment	SL-C 3 requires fullfilment of SR 1.1, SR 1.1 RE 1 and SR 1.1 RE 2.

4.3. 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
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 1.1, SR 1.1 RE 1, SR 1.1 RE 2 and SR 1.1 RE 3.

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

SecurityLevel	SL-C 4

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
SecurityLevel	SL-C 1

4.6. 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
SecurityLevel	SL-C 2
Comment	Wireless devices are covered in particular by SR 1.6 and SR 2.2 with higher requirements for achiving a similar security level to wired devices.

4.7. 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
SecurityLevel	SL-C 2

4.8. 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
SecurityLevel	SL-C 4

4.9. 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
SecurityLevel	SL-C 2

4.10. 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
SecurityLevel	SL-C 1

4.11. 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
SecurityLevel	SL-C 3
Comment	SL-C 3 requires fullfilment of SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2 and SR 2.1 RE 3.

4.12. 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
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2, SR 2.1 RE 3 and SR 2.1 RE 4.

4.13. 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

SecurityLevel	SL-C 4

4.14. 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
SecurityLevel	SL-C 3
Comment	SR 2.12 RE 1 (SL-C 4) requires determination of users in general (human, softare process, device)

4.15. 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
SecurityLevel	SL-C 2

4.16. 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
SecurityLevel	SL-C 4

4.17. 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
SecurityLevel	SL-C 4

4.18. 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
SecurityLevel	SL-C 4

4.19. 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
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 2.8 and SR 2.8 RE 1

4.20. 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
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 2.9 and SR 2.9 RE 1.

4.21. 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
SecurityLevel	SL-C 2

4.22. 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
SecurityLevel	SL-C 1

4.23. 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
SecurityLevel	SL-C 2

4.24. 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
SecurityLevel	SL-C 2

4.25. 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
SecurityLevel	SL-C 2

4.26. 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
SecurityLevel	SL-C 3

4.27. 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
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 3.9 and SR 3.9 RE 1.

4.28. 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
SecurityLevel	SL-C 1

4.29. 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
SecurityLevel	SL-C 1

4.30. 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
SecurityLevel	SL-C 2
Comment	SL-C 2 requires fullfilment of SR 7.3 and SR 7.3 RE 1.

4.31. SR 7.3 RE 2 - Backup automation

Description	The control system shall provide the capability to automate the backup function based on a configurable frequency.
Source	IEC 62443-3-3:2013
SecurityLevel	SL-C 4
Comment	SL-C 4 requires fullfilment of SR 7.3, SR 7.3 RE 1 and SR 7.3 RE 2.

4.32. 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
SecurityLevel	SL-C 4

4.33. 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
SecurityLevel	SL-C 4

4.34. 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
SecurityLevel	SL-C 2

Chapter 5. Severities

5.1. Emergency

Value	0
Used by	Reserved for SIEM after corelation
Meaning	A 'panic' condition. The most severe messages that prevent continuation of operation, such as immediate system shutdown.

5.2. 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.

5.3. 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.

5.4. 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'.

5.5. 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.

5.6. 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.

5.7. 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).

5.8. Debug

Value	7
Meaning	Reserved value. Currently not used by this document. Info useful to developers for debugging the application, not useful during operations.