Industrial Security Hardening og security i TIA-portalen

Minimér truslen på dit OT-system





Dagens vært

Morten Kromann, Technology Specialist

(පීපී

<u>(</u>ଜି

平

Agenda

Hardening Hvad er det Hvor kan jeg få hjælp Hvad kan man med Siemens produkter



Hardening - hvad er det? IEC 62443-2-3

Security hardening in the context of patch management is the implementation of security controls and the removal of components, features and privileges that are not required.

Security hardening does not replace patch management, it reduces the applicable patches by removing unnecessary software, which then does not need to be patched and possibly limits the effects of certain exploits.

For more information on security hardening for IACS refer to the platform product supplier documentation, the IACS product supplier, IEC 62443-2-4 [2], U.S. National Security Agency (NSA) security guides [28] and other security resources.

IEC 62443-2-4

NOTE Hardening guides provided by the suppliers of the control system and other components used in the Automation Solution may be included in or referenced by the service provider's hardening guide.



Hardening - hvor kan jeg få hjælp?

https://support.industry.siemens.com

SIEMENS

Always at your service! Industry Online Support – 25 years



Security with SIMATIC

controller









The Industrial Security Concept from Siemens: Plant security based on IEC 62443

- Plant physical access
 - protection
- Processes and guidelines
- Security service
 protecting production
 plants







Network security

System integrity



The Industrial Security Concept from Siemens: Network security based on IEC 62443

- Cell protection
- Secured communication
- Firewalls and VPN



Network security



The Industrial Security Concept from Siemens: System Integrity based on IEC 62443

- System hardening measures
- Patch-Management
- Authentication and access

protection





System Integrity: Communication Integrity



IEC 62443-3-3 – SR 1.2 SL2

"The control system shall provide the capability to identify and authenticate all software processes and devices."

IEC 62443-3-3 - SR 4.1 SL1

The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

Controller

TIA Portal

HMI

 \sim



TIA Portal: Certificate Manager What is the use of certificates and keys?



Certificates and keys are essential for authentication and secure communication

Secure Engineering/HMI communication with TIA Portal V17

<u>TLS*-based</u> protection of communication between S7-Controllers and Engineering Stations with TIA Portal or HMI-Stations



- ✓ TLS 1.3
- ✓ Individual certificates
- ✓ End-to-end encryption
- Optional additional protection
 - Helps prevent data theft, manipulation, or sabotage

*) TLS - Transport Layer Security

Secure OPC UA Integrated security mechanisms





OPC UA Security



Selectable security policies in Controller and Clients



Device/application authentication based on certificates



Integrity protection and encrypted communication



User authentication and restricted access to PLC tags

Certificate Management via OPC UA for S7-1500 GDS Support

Certificate management is now possible through OPC UA Global Discovery Server - GDS

- Certificate update at runtime
- Support of Certificate Revocation Lists CRLs
- Access protection for certificate management

Benefits

- Install or update the OPC UA server certificate during runtime
- Implement security concepts based on short validity period
- Revoke certificates during runtime
- Restrict access when employees leave the company or when the system is compromised



SIMATIC S7 CPU: Encrypted Communication Secure Open User Connection

Build your own protocol based on TLS



SIMATIC S7 CPU: Encrypted Communication Webserver with https

Activate the webserver

- Activate the webserver (disabled by default) and restrict the access to only HTTPS (secure http)
- Insert users with different access levels for the webserver
- Create a certificate for the webserver
- Download the project to the PLC, make sure that the system time of the PLC is set correctly

TIA Portal project







SIMATIC S7 CPU: Encrypted Communication Webserver with https

Call integrated webserver of the PLC

- When you call the webserver for the first time you will get a warning – because the PC doesn't trust the certificate of the PLC (nor its CA)
- Solution: add the CA into the "Trusted Root Certification Authorities" folder of the PC



connection meenanisms	
Certificate manager	Security
Security event	
OPC UA	The global security settings for the certificate manager are not enabled.
 System power supply 	Only limited functionality is available.
Configuration control	The server certificate is used to verify the servers identity when it is accessed and to enable
Connection resources	endpoint security.
Overview of addresses	
Isochronous mode	Server certificate: PLC-2/Webserver-15
 Runtime licenses 	
OPC UA	

Privacy error	× +	-		×
← → C ▲ Not secure	https://10.11.33.18	☆	θ	

A

Your connection is not private

Attackers might be trying to steal your information from **10.11.33.18** (for example, passwords, messages, or credit cards). <u>Learn more</u>

NET::ERR_CERT_AUTHORITY_INVALID

ADVANCED

BACK TO SAFETY



Industrial Security Communication processors: Secured to Ethernet



Feature / function

Secured in-rack Ethernet connection to SIMATIC S7-1200 or S7-1500

Integrated security functionalities:

- Stateful Packet Inspection Firewall
- Virtual Private Network (VPN)
- Clock synchronization (NTP secure)
- Secured web server access (HTTPS)
- Transmission of network analysis information with SNMP V3

Integration **in SINEMA Remote Connect** (from Firmware Version V3.1)

- Integrated engineering by means of:
- STEP 7 in TIA Portal

Benefit

Network protection and segmentation without additional security components and secured connection to a **Telecontrol** control center with TeleControl Server Basic

Protection of critical networks against:

- unauthorized network access
- o espionage or data manipulation

Convenient central administration and auto configuration of remote access

Central configuration of the communication processor



System Integrity User Management Component



IEC 62443-3-3 - SR 1.3 SL1

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.

IEC 62443-3-3 - SR 1.3 RE1 SL3

The control system shall provide the capability to support unified account management.



UMC Server



Cooperation of User Management and Access Control UMAC and TIA Portal Option UMC

UMAC: User Management and Access Control

- o Built-in functionality in TIA Portal
- Allows personalized access to TIA Portal projects
- Define project users, roles, rights and assign them



UMC: User Management Component

- Extends UMAC by optional use
- Manages users/groups outside TIA Portal projects
- Import of needed UMC users/groups into TIA Portal projects
- Assigning project roles to them
- Authenticates UMC users' logins afterwards



TIA Portal Options – System-wide user management UMC

UMC = User Management Component

- Maintenance of users/user groups of a system
- Creation of setup on STEP7/WinCC DVD2
- Project-independent setup with 1... n computers
- Windows users/groups can be imported
- Authentication of login input at runtime

Benefits

- Maintenance of users only once for the system, not multiply across projects or even locally for a product
- UMC users/groups can be imported into projects
- Basis for efficient administration of personalized security in the system
- UMC can be used optionally



HMI & WinCC: User Management Central User Management

SIMATIC Logon

- Users can be handled centrally for all HMI/ WinCC Systems by use of SIMATIC Logon Server
- Comfort Panels, WinCC Runtime Advanced and Professional can be connected
- Can be connected to existing Microsoft Active Directory Domain



Conoral	
Change initial	-
Change Initial password:	
Change logoπ time.	
Enable limit for logon attempts:	
Number of Incorrect logon attempts:	
Logon only with password:	
Hierarchy level	
Group-specific rights for user administration:	
Password	
Freble persuand estinat	
Enable password aging: Password validity (devely	
Prewerning time (days):	7
Pessword generations	
rassword generations.	
Password complexity	
Must include special characters:	
Must include number:	
Minimum password length:	3
SIMATIC Logon	
Enable SIMATIC Logon	
Apply user administration from	
	• Windows domain
	O Windows computer
Server data	
Server name:	
Port number:	16389
Windows domain:	



System Integrity Access Protection and authentication

IEC IEC

IEC 62443-3-3 – SR 2.1 SL2

The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.

IEC 62443-3-3 - SR 2.6 RE 2 SL2

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.





SIMATIC S7 CPU: Online Access Protection of the CPU Different authorization levels



SIMATIC S7 CPU: Online Access Protection of the CPU Deactivate access in the program (multi-factor authentication)

Can the access to the PLC be completely forbidden even if access level password is known?

- Scenario: service technician working on a PLC
- Access to other PLC shall be impossible
- Use function block ENDIS_PW to deactivate all access
- Block could be triggered by key switch, timer,...





SIMATIC S7 CPU: HMI communication Secure data access

Restrict accessibility of data

- Not all data needs to be accessed by HMI
- For some data only read access is required
- Threat: HMI developed by third party, tries to access data it should not access
- Solution: Restrict the access to the data granular for each variable

Secure connection

- HMI connection has manipulation detection
- Connection to PLC can be secured by password (see access protection), this password can be stored in the connection settings of the HMI

Name		Data type	Start value	Retain	Accessible from HMI/OPC UA	Writable from HMI/OPC UA
•	Static					
•	REQ	Bool	false			
•	FPW	Bool	false			
•	Ndr	Bool 🔳	false			
•	Error	Bool	false			
•	Status	Word	16#0			

Со	nnections							
	Name	Communication driver	HMI time synchro	nization mode	Station	Partner		
	HMI_Connection_1	SIMATIC S7 1500	None		S71500/ET2	200MP s PLC_1		
	<add new=""></add>	-						
<						>		
Para	ameter Area	pointer						
TP	900 Comfort					Station		
- 1	Interfac	e:						
- J.	ETHERN	NET 📼						
H	/II device			PLC				
	Address:	192.168.0.2			Address:	192.168.0.1		
	Access point: S	70NLINE1		Access password: *****				



HMI & WinCC: User Management Authorization for HMI/SCADA visualization objects/screens

Challenge

- HMI has different screens to operate machine in automatic or manual mode
- Machine might get damaged if operated in manual mode
- Some employees have insufficient training

Solution

Operator

OK

Cancel

Password:

Login User:

- User management for operating the HMI / WinCC •
- Restricted access to the different screens / buttons

Properties

📑 Property list

Securit

Miscellaneous

Animations

 \mathbf{h}

Security

Events

Runtime security

Texts



HMI & WinCC: Secure Access Protect against unauthorized download

Challenge

• Download to HMI during production will interrupt operability of machine when the transfer settings are "automatic"

Solution

- Restrict transfer settings so that during runtime of the HMI no download is possible
- Authorized personal first has to shut down runtime and set HMI to transfer mode
- Recommendation: set transfer settings to manual or off





HMI & WinCC: Secure Access Protection of HMI system settings

Restrict access to the HMI settings

- Assign a password to the HMI settings, further access to the settings will only be possible by entering the password
- Prevents against manipulating the settings, e.g. the transfer settings or others
- If password is lost/compromised, the complete operating system image has to be installed again via SIMATIC ProSave





HMI & WinCC: Secure Access Protect access to sm@rt Server

Challenge

- Remote access to the HMI is needed to operate the machine
- sm@rt Server allows the remote access but has to secured

Solution

- sm@rt Server is deactivated by default
- Set a secure password and restrict the access right ("view only")
- Communication to sm@rt Server can be encrypted
- For remote access from other subnets we recommend to make the sm@rt Server only accessible via VPN





System Integrity: Access Control



IEC 62443-3-3 – SR 1.1 SL4

The control system shall provide the capability to employ **multifactor** authentication for all human user access to the control system.

IEC 62443-3-3 - SR 7.1 RE 2 SL3

The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.



Access Control Reader SIMATIC RF1000

Industrial Security Access control with SIMATIC RFID Card Reader

SIMATIC RFID Card reader

- Protects automation machinery
- Reliably identify operators
- Assign appropriate access rights based on user
- Quick & easy login during operator changeover

RJ45 Locks protect against:

- bypassing approved network procedures
- misuse of unused RJ45 ports
- unauthorized use of unconfigurable(unmanaged) network components







System Integrity: Know-how protection





IEC 62443-3-3 – SR 3.4 SL2

The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

IEC 62443-3-3 – SR 3.4 RE 1 SL3

The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.



SIMATIC S7 CPU: Know-How Protection Protect your engineering know-how!

Know-How Protection

- Set a password for the access
- Without password only the interface of the block (Inputs, Outputs, In-Out, static variables) can be viewed.
- Constants and code can be viewed only by entering the correct password.

Write-Protection

- Set a password for the access
- The block cannot be edited, but everything can be read (including logic).
- Only with the password the write protection can be deactivated to edit the block.







SIMATIC S7 CPU: Know-How Protection Program and data integrity

Check integrity during runtime

- By use of instruction GetChecksum the integrity of the PLC program and data can be checked during runtime
 - Detects manipulation/ unauthorized program changes





SIEMENS

Array[0..7] of Byte

Array[0..7] of Byte

System Integrity: Asset Management



IEC 62443-3-3 - SR 7.3 SL1

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.

IEC 62443-3-3 - SR 6.1 SL1

The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.





Online Diagnostic & Maintenance Features Integrated Web Server - Diagnostics

SIEMENS	S7-1200 station_1 / PLC	C_1		
				11:27:3
Username				
▶ Start Page	Identification Program protectio	tion Memory		
Diagnostics	Order Identification:			
	Plant designation:		Diagnostics	
 Diagnostic Buffer 	Location identifier:		~	
▶ Module Information	Serial number: SC-E4	E4S21500		_
▶ Communication	Order number:		Identification Program protection Memo	ny
	Hardware: 6ES7 2	7 214-1AG40-0XB0		
► Lag status			Know-how protection:	
Watch tables	Version:			
	Hardware: 1		Know-how protection:	Not present
 Online backup 	Firmware: V04.04	04.00		
▶ Data Logs			Binding:	
▸ User Files			CPU serial number:	No binding
▶ User-defined pages			Memory card serial number:	No binding
▶ File Browser				
			Program copy to memory card:	
			From internal load memory:	Enabled
Introduction				

Online Diagnostic & Maintenance Features Integrated Web Server – Diagnostics Buffer

SIEMENS S7-1200 station_1 / PLC_1

Username Login	Diagno Diagnostic	stic Buffer				information events are re
	Number	Time	Date	Status	Event	recent event
▶ Start Page	1	05:37:23 pm	5/15/2020	Incoming event	High limit exceeded	
	2	05:36:59 pm	5/15/2020	Incoming event	New startup information - Current CPU operating mode: STC)P
 Diagnostics 	3	05:36:58 pm	5/15/2020	Incoming event	Follow-on operating mode change - CPU changes from STC	P to STOP mode
	4	05:36:57 pm	5/15/2020	Incoming event	New startup information - Current CPU operating mode: STC)P
Diagnostic Buffer	5	05:36:54 pm	5/15/2020	Outgoing event	High limit exceeded	
▶ Module Information	6	05:29:47 pm	5/15/2020	Incoming event	High limit exceeded	
F Module Information	7	05:29:39 pm	5/15/2020	Outgoing event	High limit exceeded	
▶ Communication	8	05:29:36 pm	5/15/2020	Incoming event	New startup information - Current CPU operating mode: STC)P
	9	05:29:36 pm	5/15/2020	Incoming event	Communication initiated request: STOP - CPU changes from	n RUN to STOP mode
 Tag status 	10	05:28:50 pm	5/15/2020	Incoming event	High limit exceeded	
	11	05:28:43 pm	5/15/2020	Outgoing event	High limit exceeded	
 Watch tables 	12	01:31:39 am	1/1/2012	Incoming event	Follow-on operating mode change - CPU changes from STA	RTUP to RUN mode
. Online heeldun	13	01:31:39 am	1/1/2012	Incoming event	Communication initiated request: WARM RESTART - CPU c	hanges from STOP to STARTUP m
 Online backup 	14	01:31:39 am	1/1/2012	Incoming event	New startup information - Current CPU operating mode: STC)P
▶ Data Logs	15	01:31:36 am	1/1/2012	Incoming event	New startup information - Current CPU operating mode: STC)P
	Details:1					
► User Files	Error: High li HVV_ID= 2	imit exceeded ?63, Input channel numbe	er 1			
User-defined pages	Incoming ev	ent				
File Browser						

The 'Diagnostic Buffer' page displays descriptive information for all events in the CPU. Diagnostic events are recorded in a circular buffer. The most recent event is displayed in the top line.

iode



Online Diagnostic & Maintenance Features Integrated Web Server – Online Backup/Restore

SIEMENS

SIMATIC 1200 Station_1 / CPU 1215C

		03:31:42 pm	1/1/2012 PLC Local 💌 English 💌	
Username	Online backup			
Login			Create a healture of the re-	aiaat in the
 Start Page 	Backup PLC:		PLC and/or restore your	PLC from a
▸ Diagnostics			previous backup file.	
▶ Diagnostic Buffer				
 Module Information 	Restore PLC:			
Communication	Browse No file selected.			
▶ Tag status	Restore selected online backup			
 Watch tables 	Status:			
Online backup				
 Data Logs 				
▶ User Files				
▶ User-defined pages				
▶ File Browser				SIEMEN

Online Diagnostic & Maintenance Features Integrated Web Server – Data Logs

SIEMENS SIMATIC 1200 Station_1 / CPU 1215C

						03:33:48 pm 1/1/2012	2 PLC Local 💌 English 💌
Username	Data Logs						
Login							😂 <u>Off</u> 📕
	Name	Size	Changed	Active	Delete	Retrieve and clear	
 Start Page 	Production_Data.csv	835	07:56:12 pm 12/31/2011	Yes	×		
▶ Diagnostics							The 'Data Logs' page allows you to
 Diagnostic Buffer 							system memory of the CPU. This
 Module Information 							can either be in the integrated CPU
▸ Communication							memory or the optional SD Card.
▶ Tag status							
 Watch tables 							
 Online backup 							
→ Data Logs							
▶ User Files							
▶ User-defined pages							
							SIEMENS

Online Diagnostic & Maintenance Features Integrated Web Server – File Browser

			04:21:03 pm 1/1/	2012 <mark>PLC</mark>	CLocal 💌	English 💌	
Username	File Browser						
Login						🔀 <u>Off</u> 昌	
▶ Start Page	SIMATIC 1200 Station_1						
▶ Diagnostics	Name	Size	Changed	Delete	Rename		
, Diagnostics	Recines		06:00:00 pm 12/31/2011				The "File Browser" page allows
 Diagnostic Buffer 			00.00.00 pm 12/01/2011				you to access system-generated
► Module Information	Directory operations:						files such as recipes and data logs
Communication							files.
▶ Tag status							
 Watch tables 							
▶ Online backup							
 Data Logs 							
▶ User Files							
 User-defined pages 							
▶ File Browser							SIEMENS

SIMATIC Automation Tool



Uses (No TIA Portal Required)

- File browsing
- Firmware updates
- Program/Project download
- IP Address changes
- Backup/restore PLC / HMI programs
- And more...



Scalable versions

- 1) Free 21-day trial license
- 2) Basic version
- 3) Advanced version
- 4) API SDK unlimited use version

SIMATIC Automation Tool V4.0 Advanced – Scheduler

Scheduler operations:

- Read service data
- Set time
- Export diagnostics buffer
- Create full backup
- Export data log(s)
- Firmware update

Scheduler settings:

- Date
- Time
- Frequency
- Run Once
- Every Day/Every Week/Every 2 Weeks/Every Month/Every Year

M SIMATIC Automation Tool										_ 0 1
File Edit View Operation	ns Options To	ools Help). <i>(</i> 14	li - @- 🖬 Dukdube	100 USB 2.0 Fast Ethernet Adapte	r.TCPIP.Auto.1 V			SIMATI	Automation Tool
Set IP Address Set PROFINET No	ane Program Updat	e Fimware Up	date	Restore from Backup Card Brows	er Scheduler Getting Stated					
				Use the icon to set the start date and time	Use the icon to set the start date and time	Use the icon to set the start date and time	Use the icon to set the start date and time	Use the icon to set the start date and time	Use the icon to set the start date and time	
Device	IP Address	CPU Passwo	d	Read Service Data	Set Time	Device Diagnostics	Full Backup	Read Data Logs	Firmware Update	New Firmware Version
thei_1	192,168.0.8									
• PLC_1	X1: 192.168.2.10		0							
PLC_2	X1: 192.168.2.12	*******	0							
PLC_3	x1: 192.168.2.20		0							
🕶 🛄 im 155-6 pn M	192.168.2.100									
* 🤰 Local modules										
DI 5x24VDC HF	1									V02.00.02



(පීපී

平

Kontakt

Morten Kromann morten.kromann@siemens.com



SIEMENS

WEBINARER MED INSPIRATION, VIDEN OG VÆRDI

Industry Information Live

Tilmeld dig, se og gense på www.siemens.dk/di-webinarer





Tilmeld dig på www.siemens.dk/di-tilmeld-nyheder

Du finder også vores nyheder på www.siemens.dk/di-nyheder

NYHEDSBREVE TIL INDUSTRIEN UDKOMMER 8-10 GANGE OM ÅRET

Industry Information News TIPS OG TRICKS PÅ YOUTUBE

Industry Information Demo

Find hurtigt playlisten og abonner via www.siemens.dk/di-demo

