Industrial Security
Hardening og security i TIA-portalen

Minimér truslen på dit OT-system

SIEMENS

Dagens vært

Morten Kromann, Technology Specialist

SIEMENS

Agenda

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

SIEMENS

Hardening - hvad er det?

IEC 62443-2-3

B.8.5 Security hardening

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.

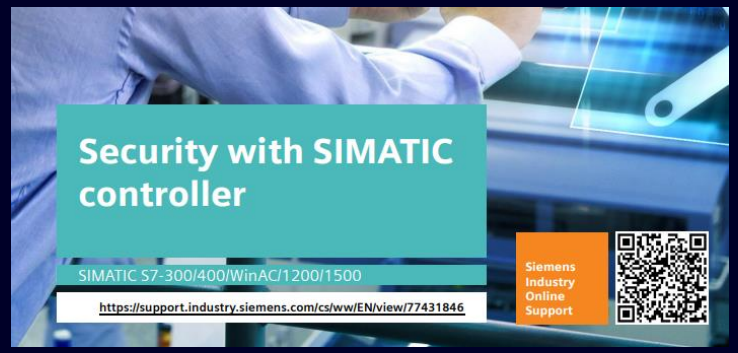
IEC 62443-2-4

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.

SIEMENS

Hardening - hvor kan jeg få hjælp?

https://support.industry.siemens.com



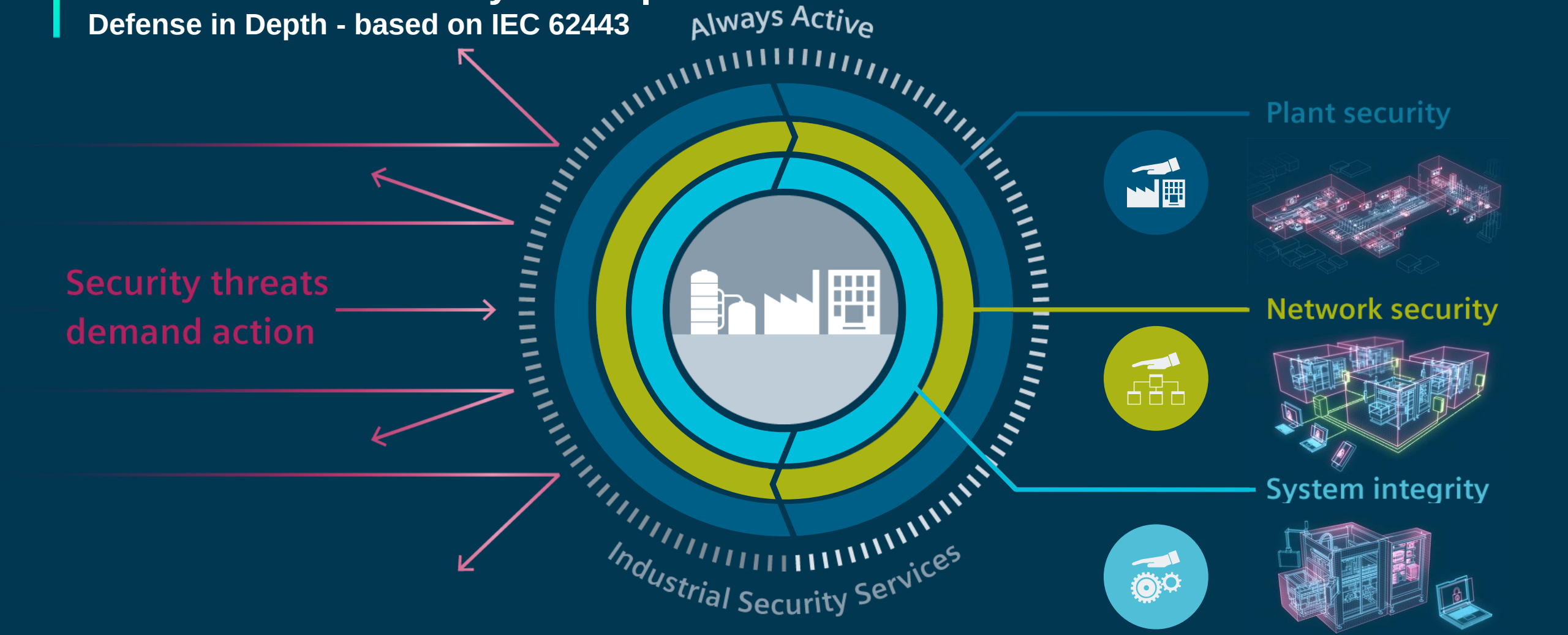
SIEMENS

Always at your service!
Industry Online Support – 25 years

SIEMENS

The Industrial Security Concept from Siemens:

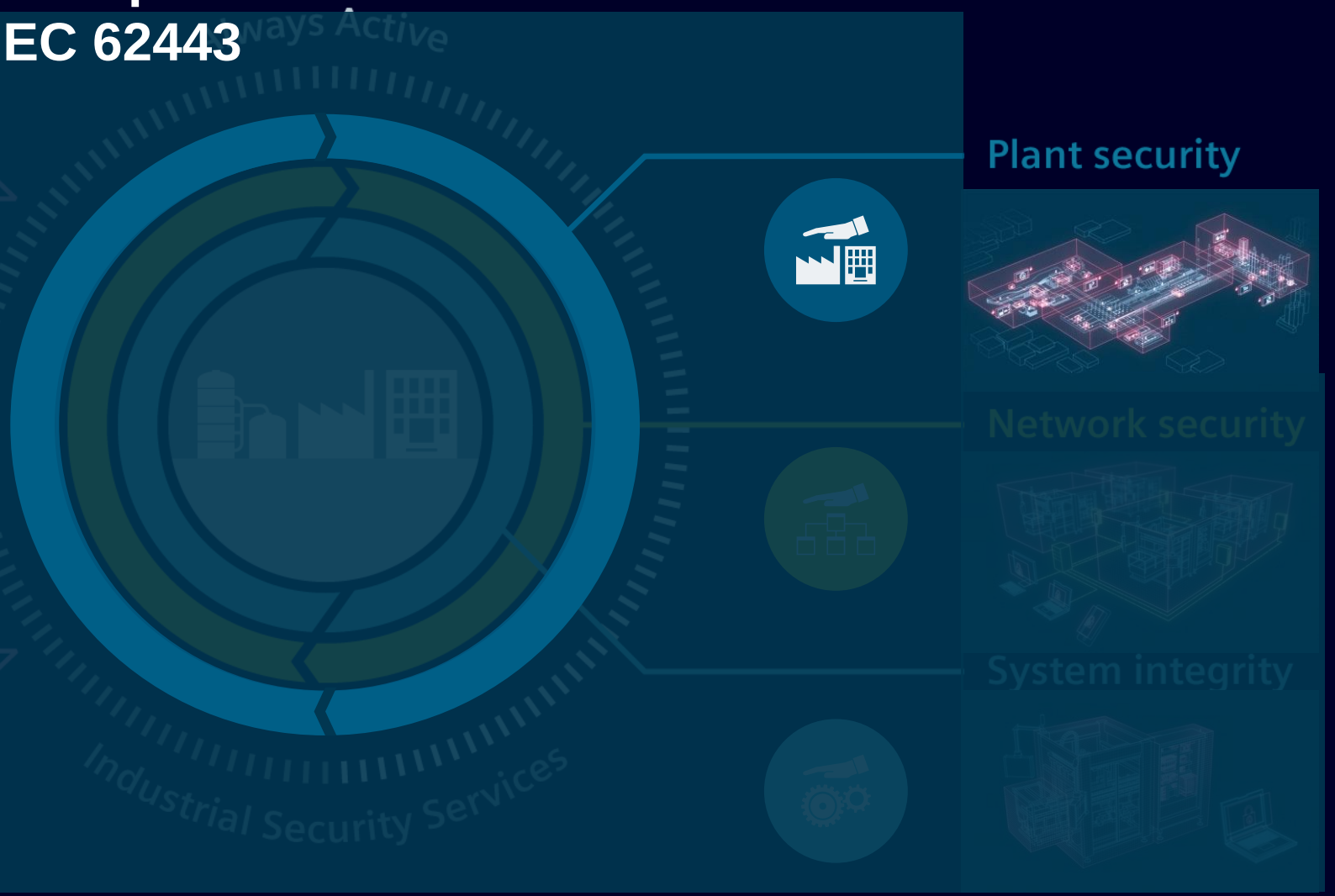
Defense in Depth - based on IEC 62443



SIEMENS

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

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



SIEMENS

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

- Cell protection
- Secured communication
- Firewalls and VPN

SIEMENS

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

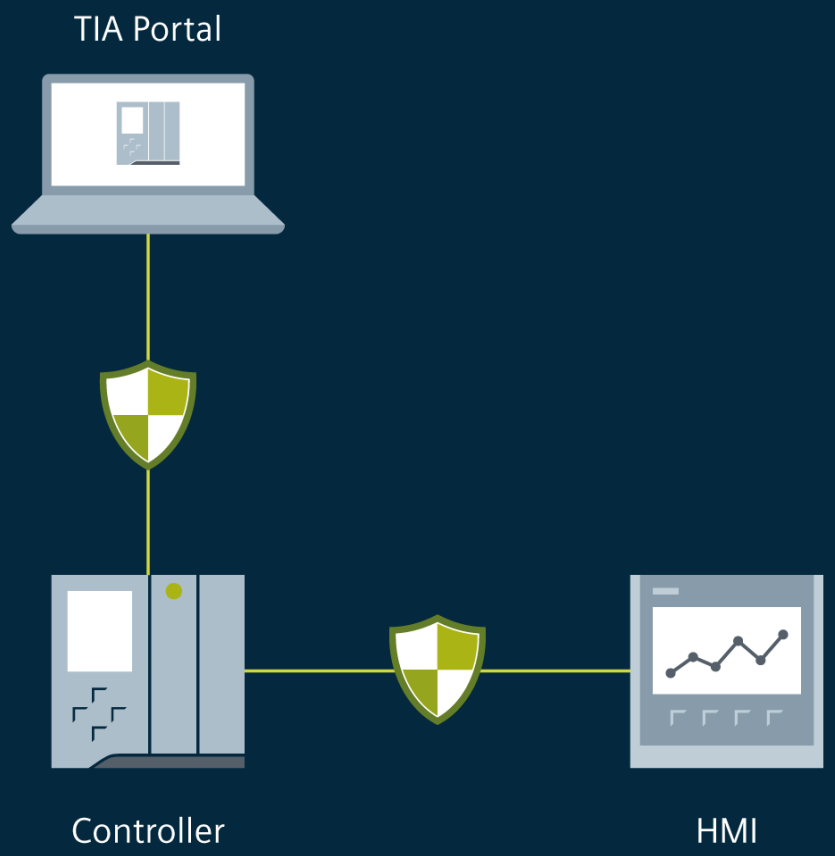
- System hardening measures
- Patch-Management
- Authentication and access protection

SIEMENS

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."

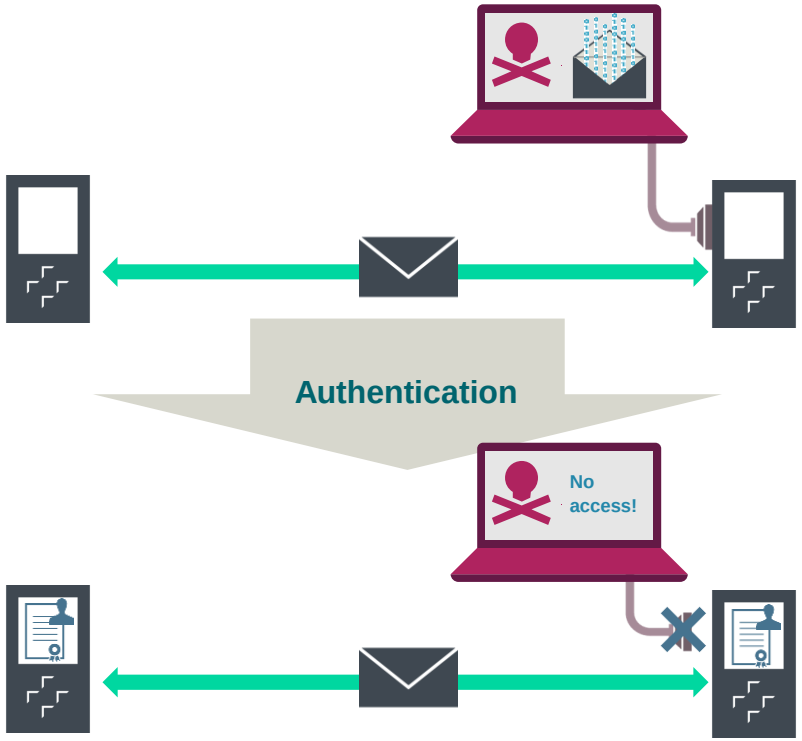
IEC 62443-3-3 – SR 4.1 SL1
The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.



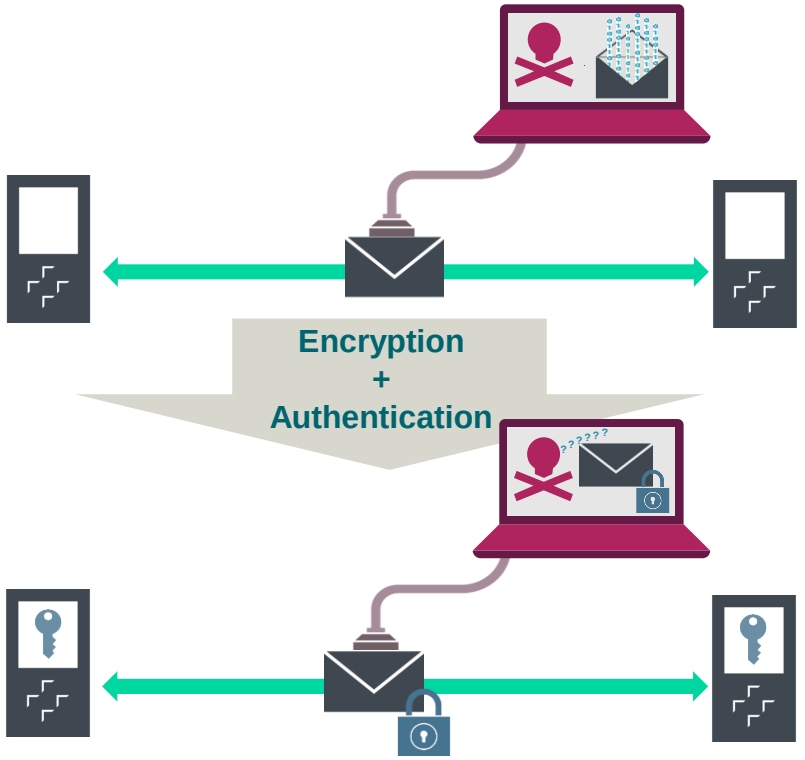
SIEMENS

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

Everyone can establish connection to PLC



Data can be wiretapped and manipulated



Certificates and keys are essential for authentication and secure communication

SIEMENS

Secure Engineering/HMI communication with TIA Portal V17

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

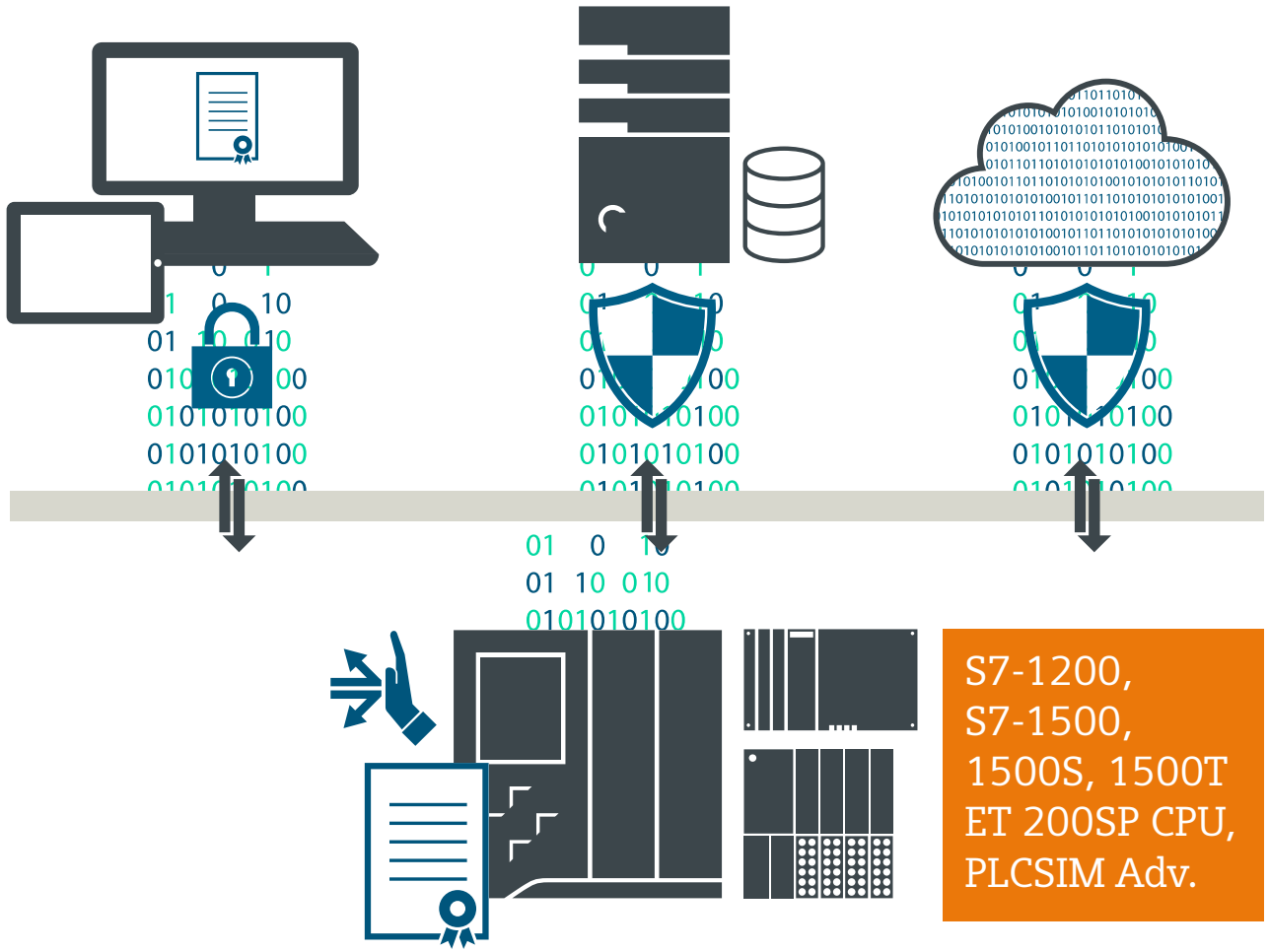
- ✓ TLS 1.3
- ✓ Individual certificates
- ✓ End-to-end encryption
- ✓ Optional additional protection

➢ **Helps prevent data theft, manipulation, or sabotage**

*) TLS - Transport Layer Security

SIEMENS

Secure OPC UA
Integrated security mechanisms



S7-1200,
S7-1500,
1500S, 1500T
ET 200SP CPU,
PLCSIM Adv.

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

SIEMENS

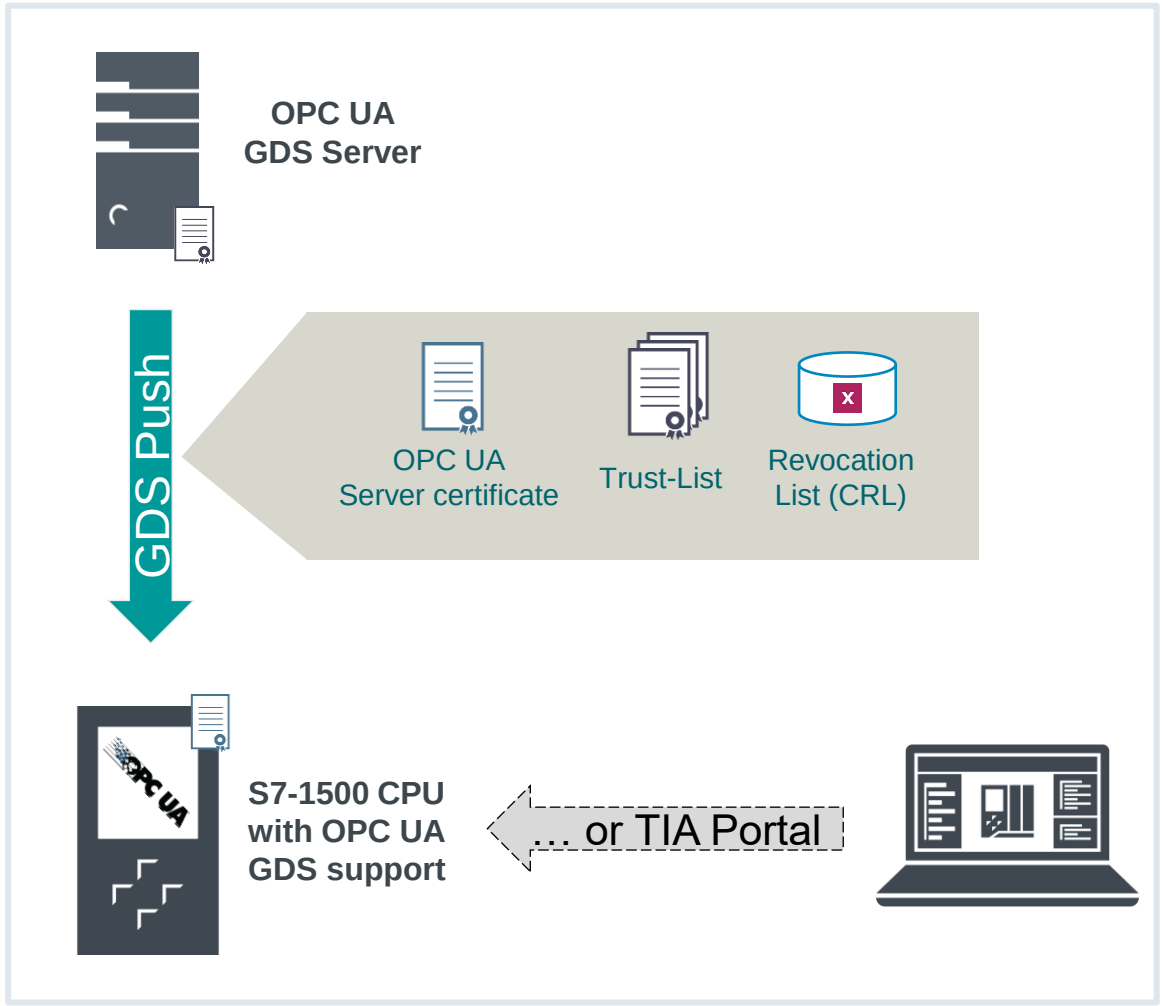
Certificate Management via OPC UA for S7-1500
GDS Support

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

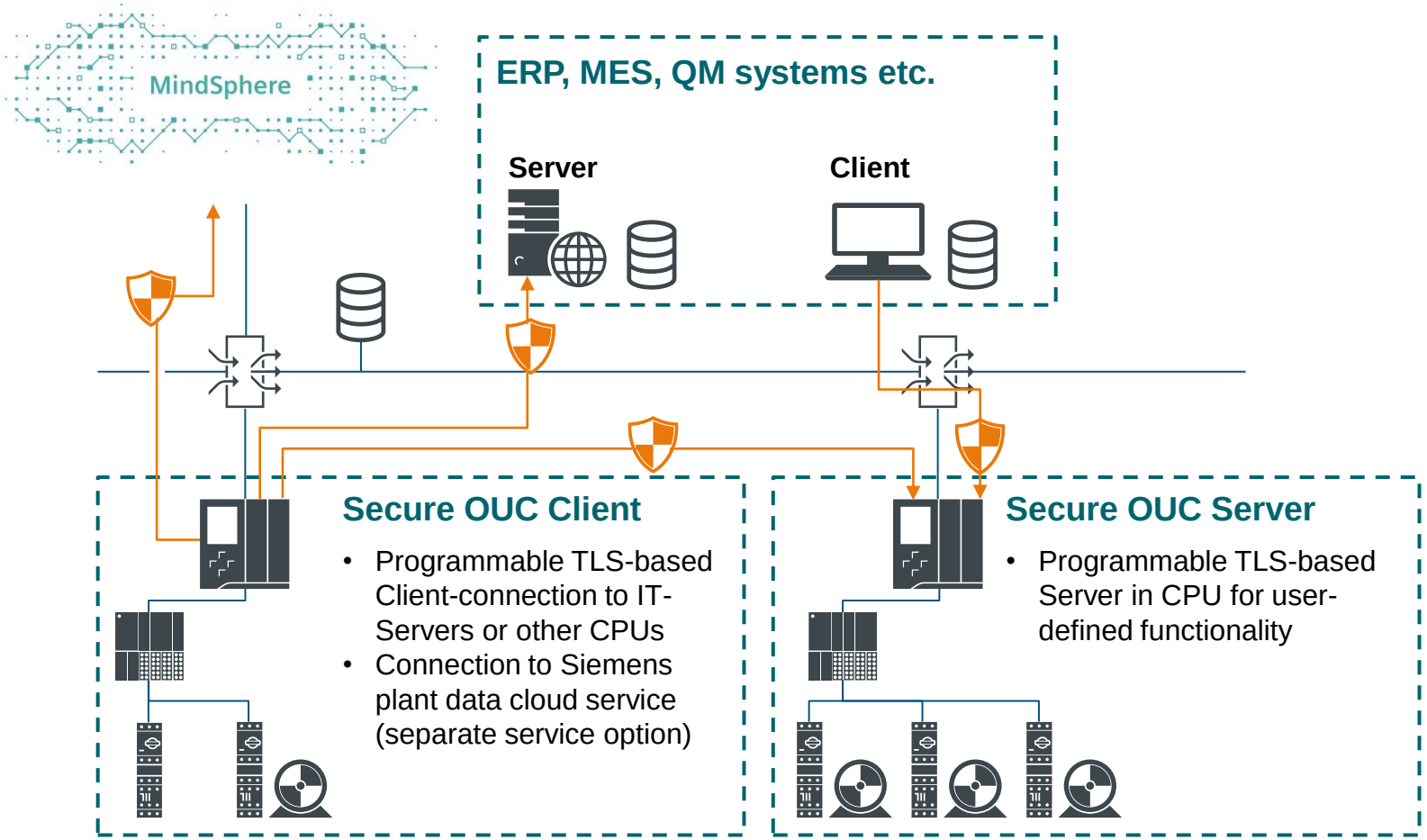
- Install or update the OPC UA server certificate during runtime
- Implement security concepts based on short validity period
- Revoke certificates during runtime
- Restrict access when employees leave the company or when the system is compromised



SIEMENS

SIMATIC S7 CPU: Encrypted Communication
Secure Open User Connection

Build your own protocol based on TLS



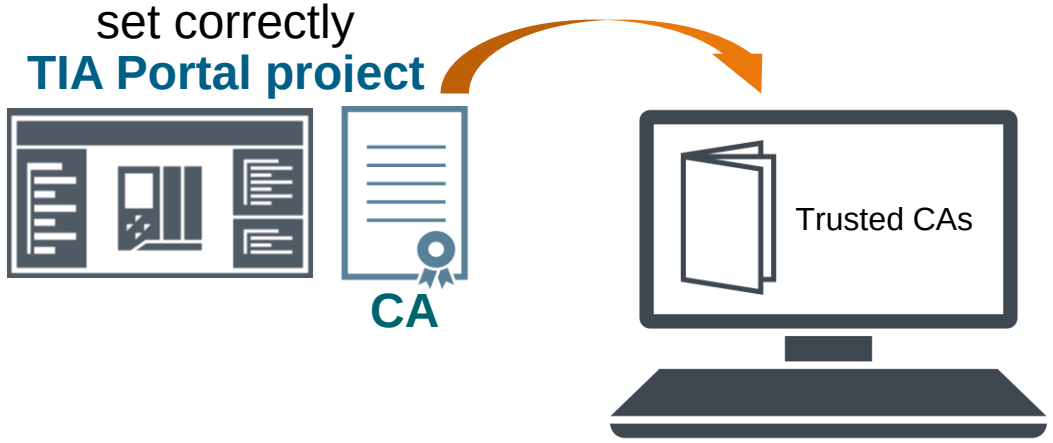
- Allows own HTTPS or FTPS communication (e.g. for production data)
- Secure Communication (TLS) for own customer defined communication
- Certificate based authentication of server and client (optionally)

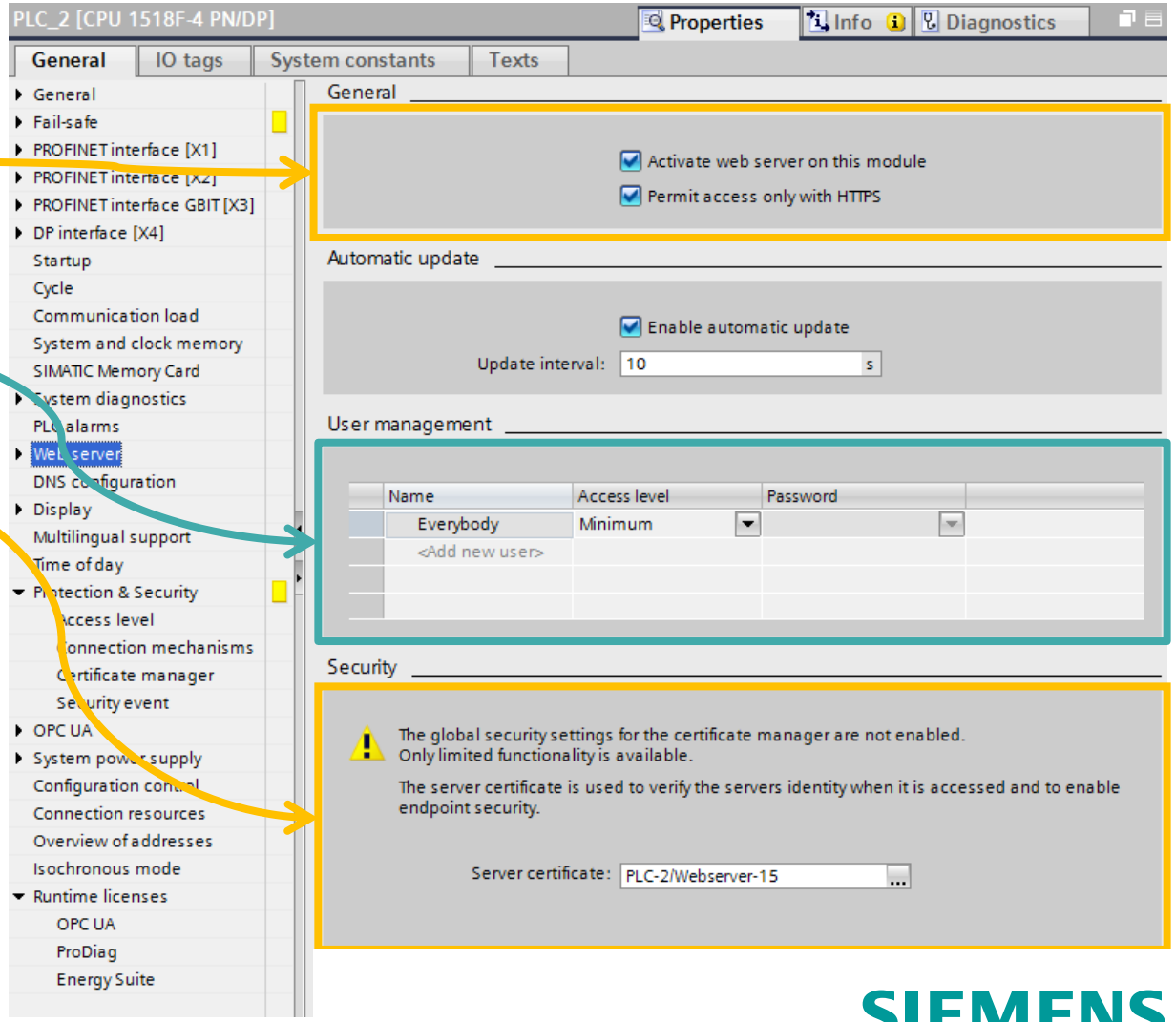
SIEMENS

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



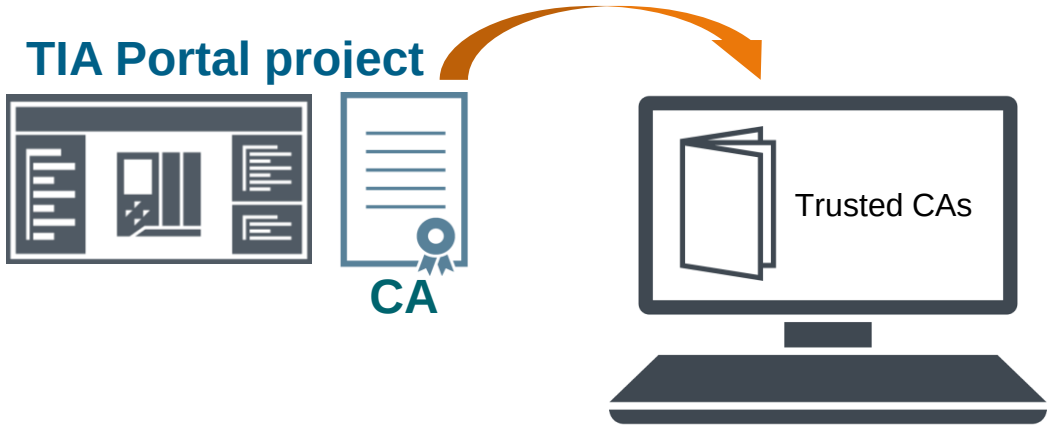


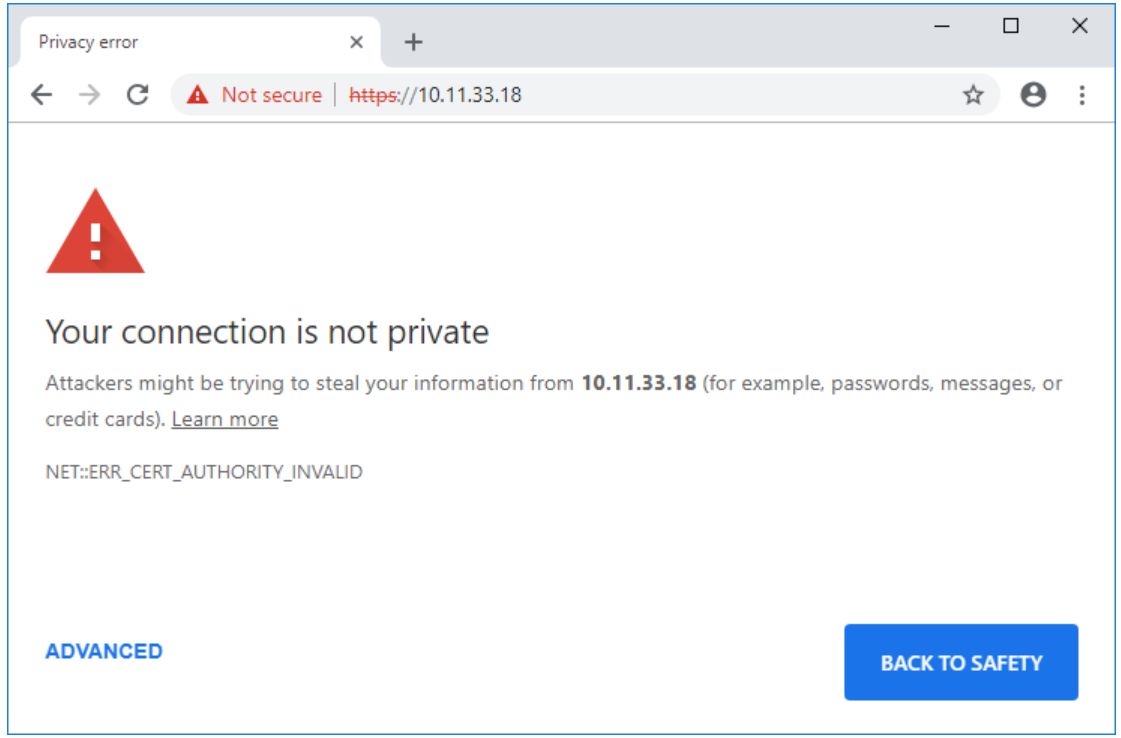
SIEMENS

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





SIEMENS

Industrial Security
Communication processors: Secured to Ethernet

CP 1243-1 CP 1543-1

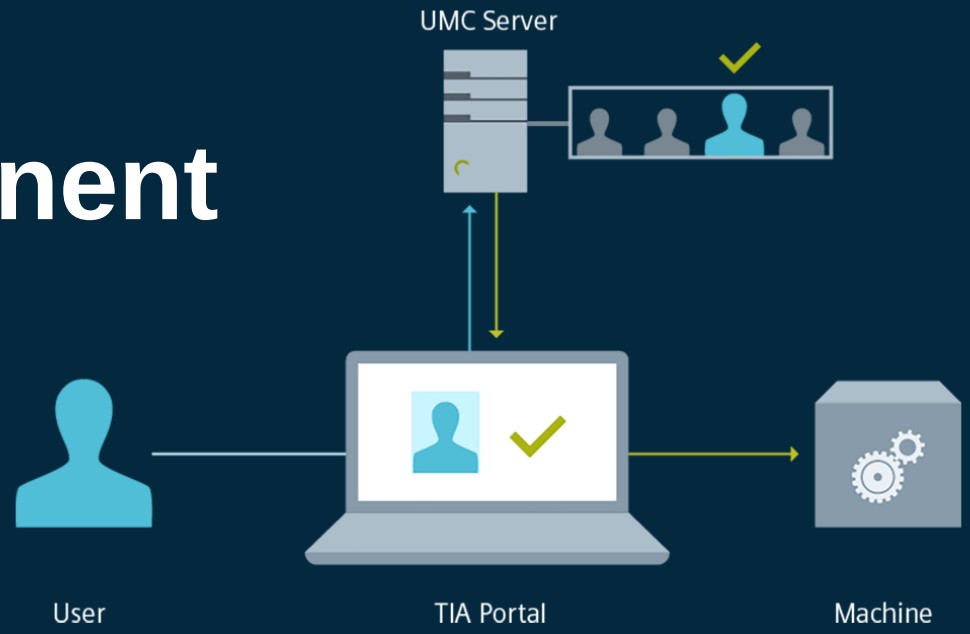
Feature / function	Benefit
Secured in-rack **Ethernet connection** to **SIMATIC S7-1200 or S7-1500**	**Network protection** and **segmentation** without additional security components and secured connection to a **Telecontrol control center** with TeleControl Server Basic
Integrated **security functionalities:** ○ 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	**Protection of critical networks** against: ○ unauthorized network access ○ espionage or data manipulation
Integration **in SINEMA Remote Connect** (from Firmware Version V3.1)	Convenient **central administration and auto configuration** of remote access
Integrated engineering by means of: ○ STEP 7 in TIA Portal	**Central configuration** of the communication processor

SIEMENS

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.

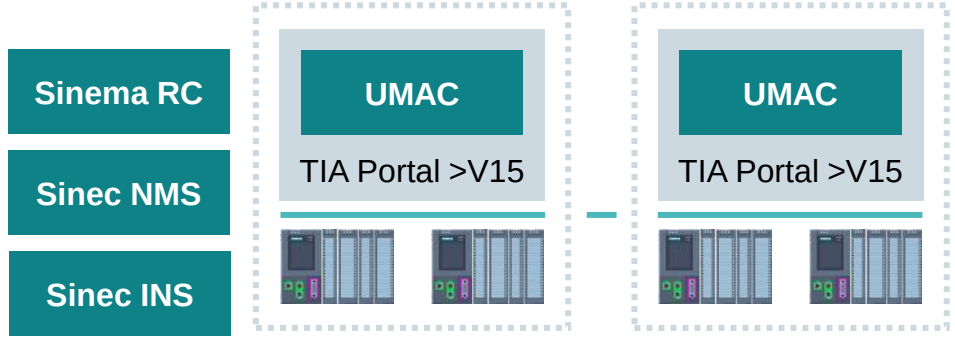


SIEMENS

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

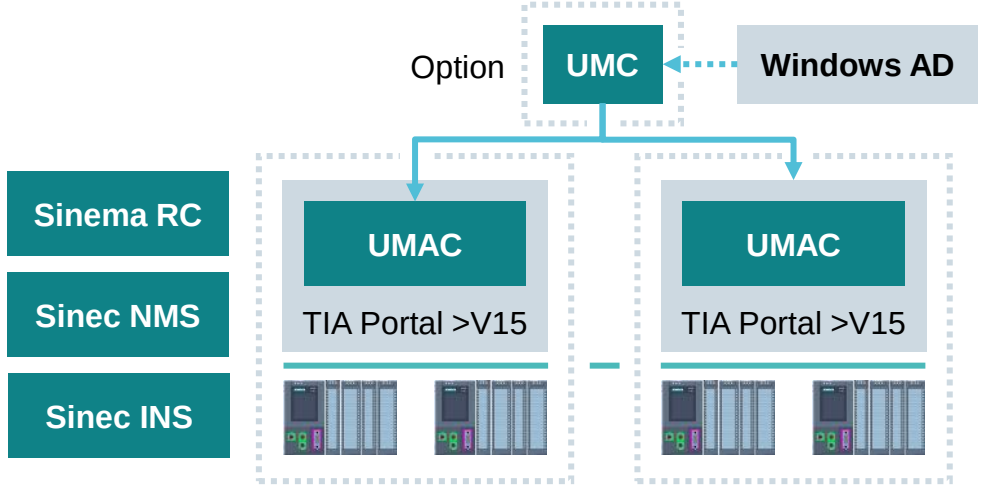
UMAC: User Management and Access Control

- 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



SIEMENS

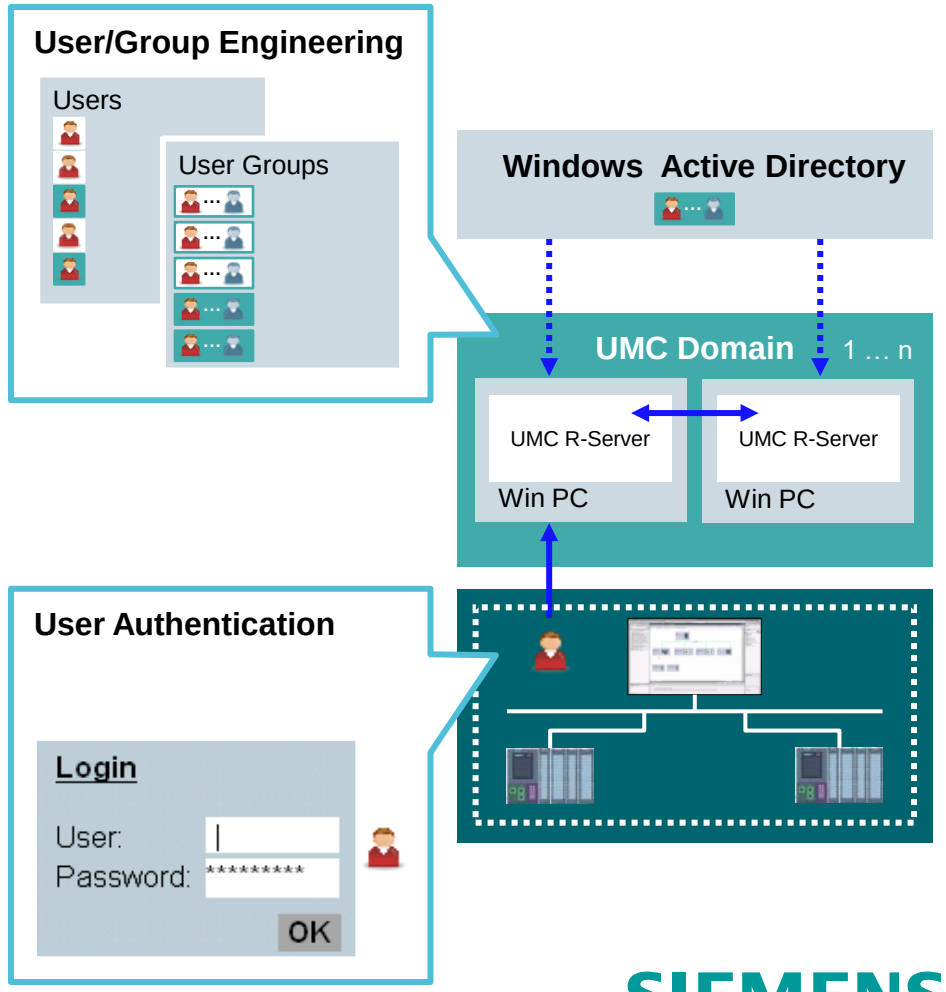
TIA Portal Options –
System-wide user management UMC

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

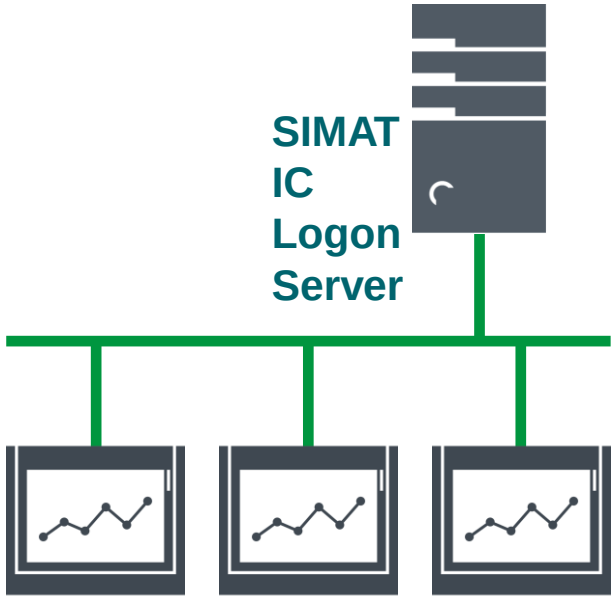


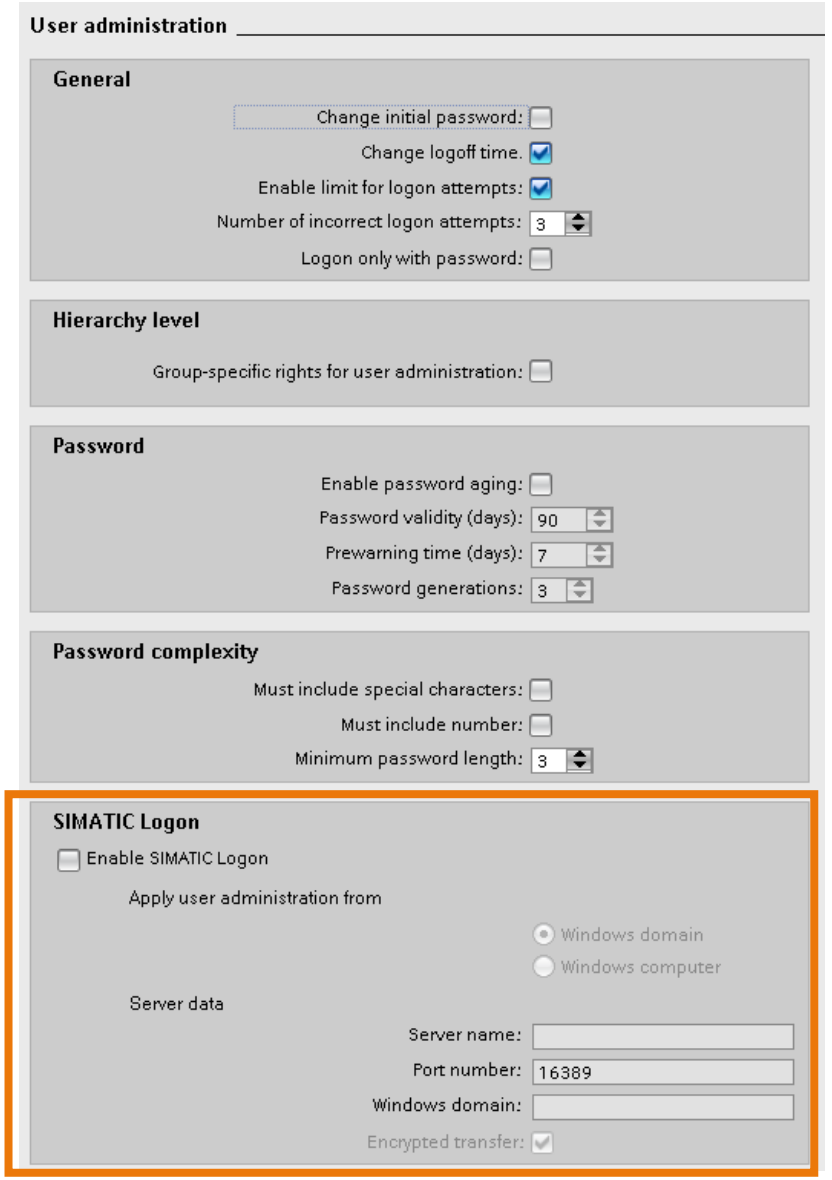
SIEMENS

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



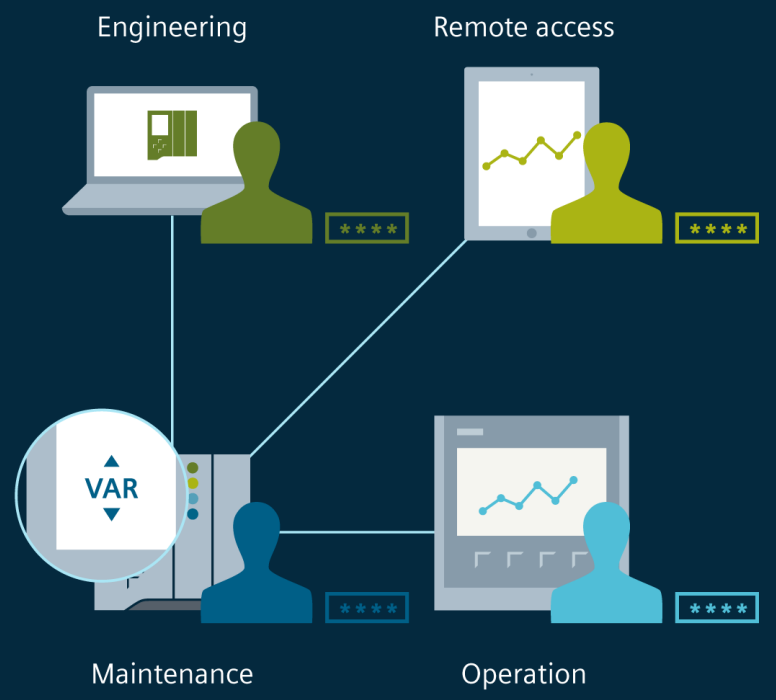


SIEMENS

System Integrity Access Protection and authentication

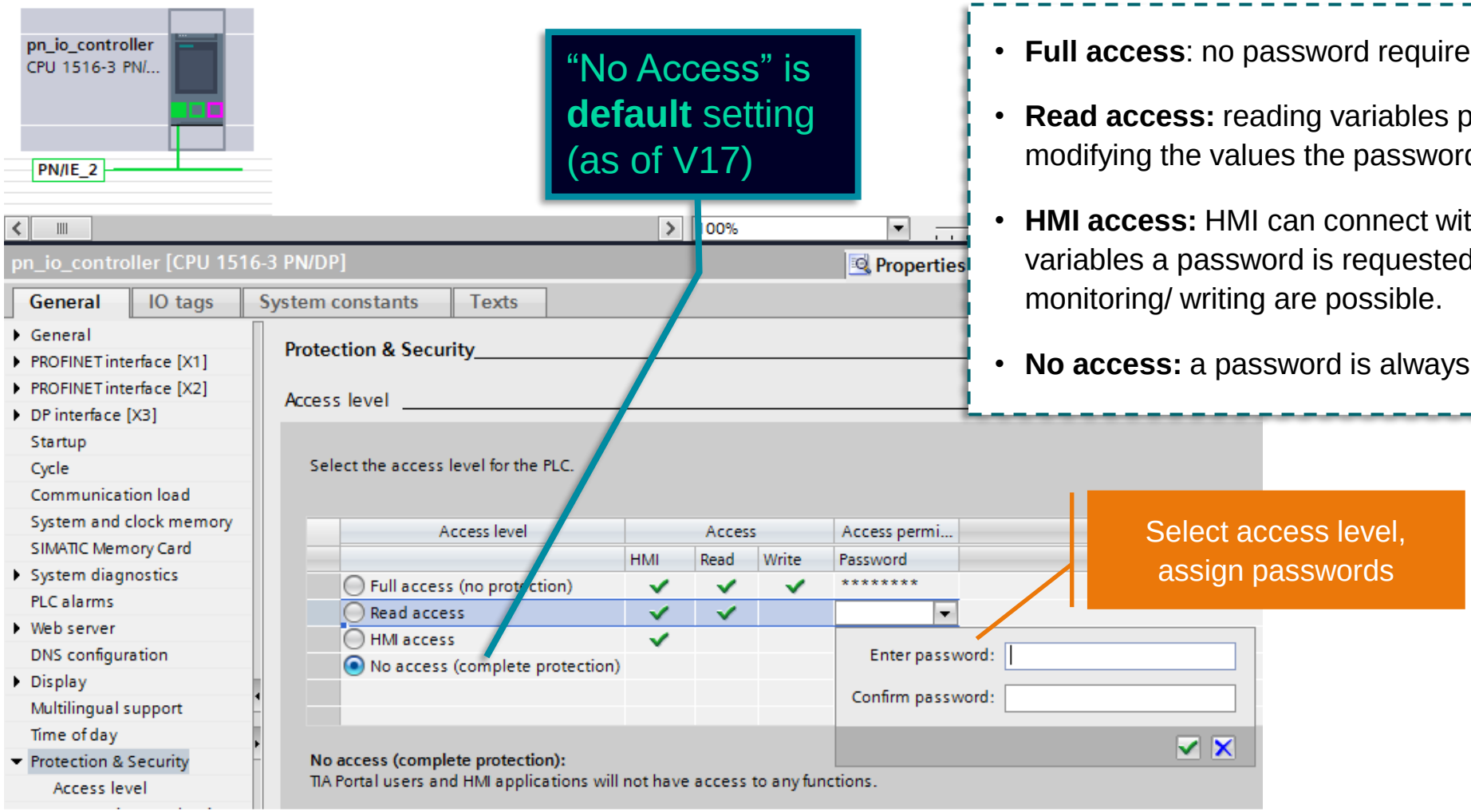
IEC 62443-3-3 – SR 2.1 SL2
The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.

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.



SIEMENS

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



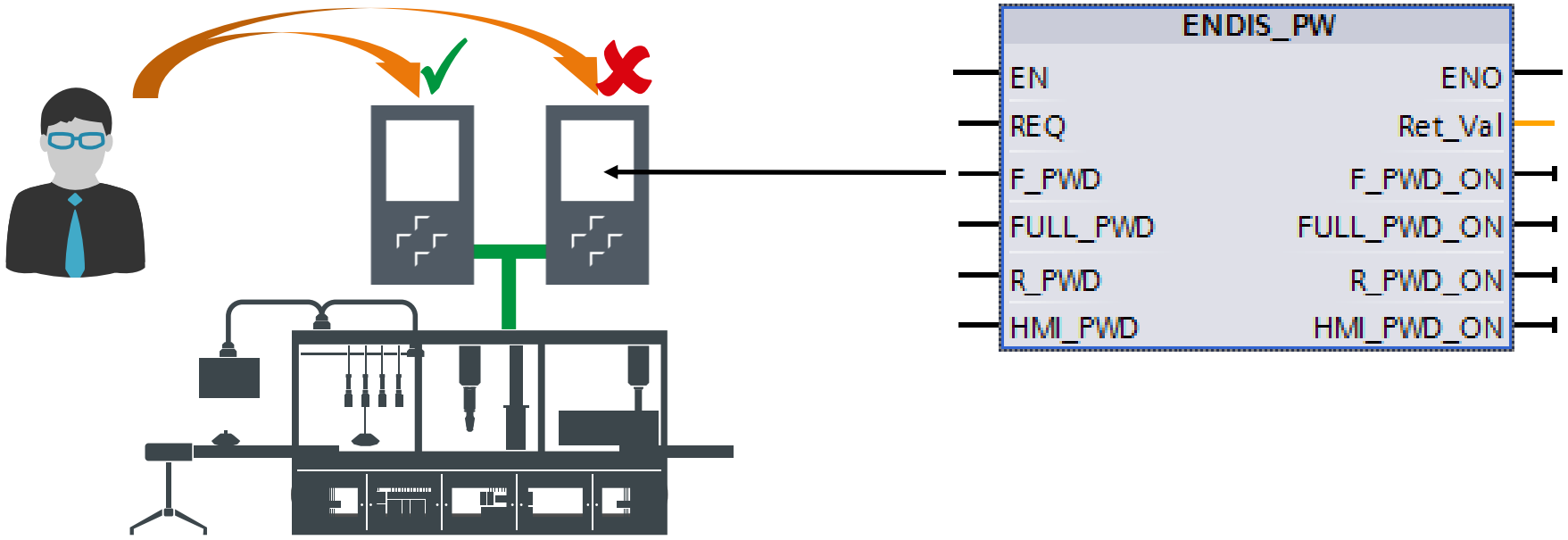
- **Full access**: no password required for access to PLC.
- **Read access:** reading variables possible without password. For modifying the values the password will be requested.
- **HMI access:** HMI can connect without a password. To monitor variables a password is requested. Separate passwords for monitoring/ writing are possible.
- **No access:** a password is always needed, also in the HMI device.

SIEMENS

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,…

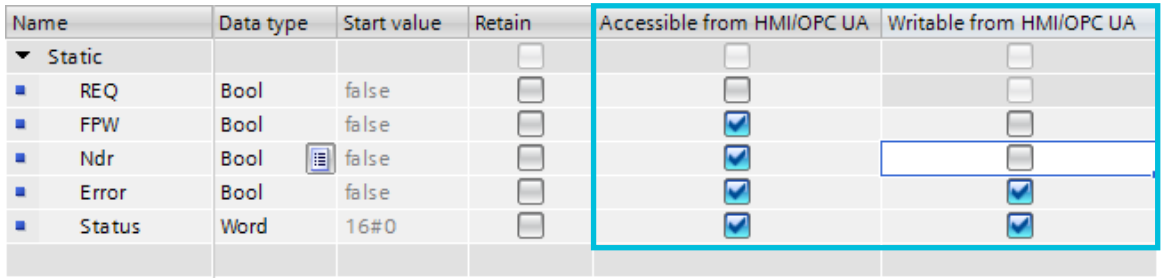


SIEMENS

SIMATIC S7 CPU: HMI communication
Secure data access

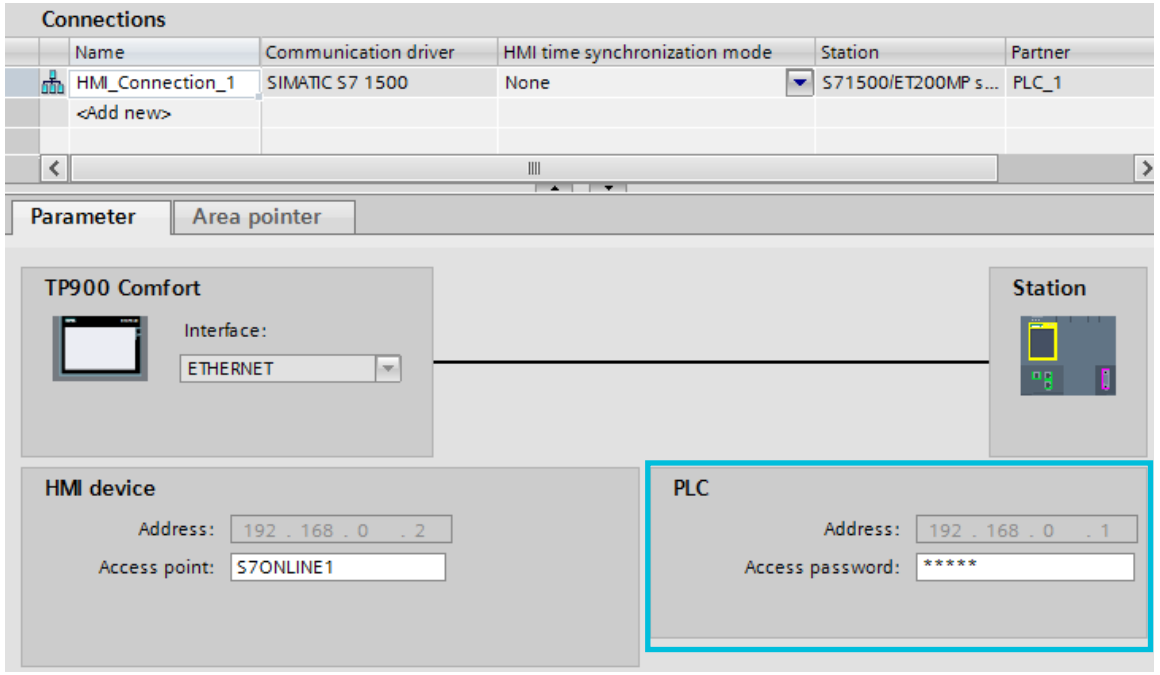
Restrict accessibility of data

- 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

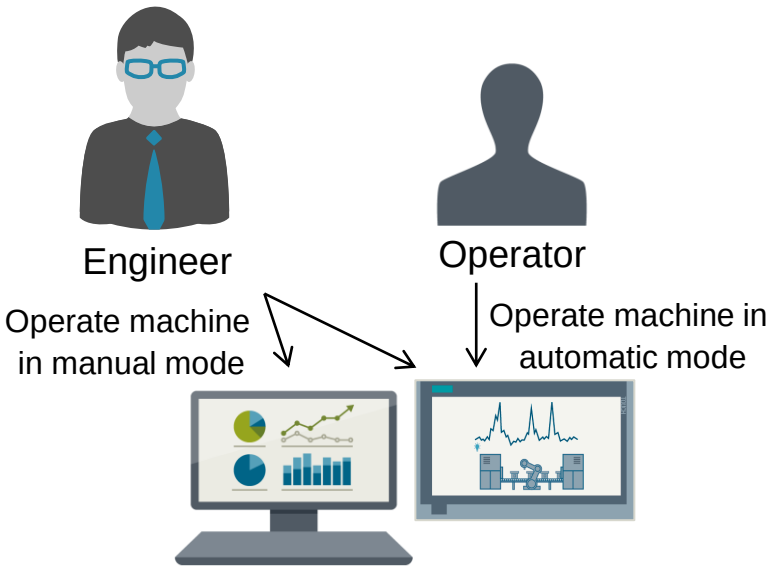


SIEMENS

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

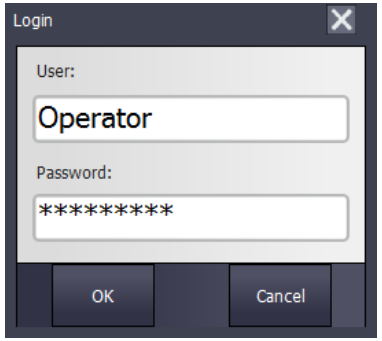
Challenge

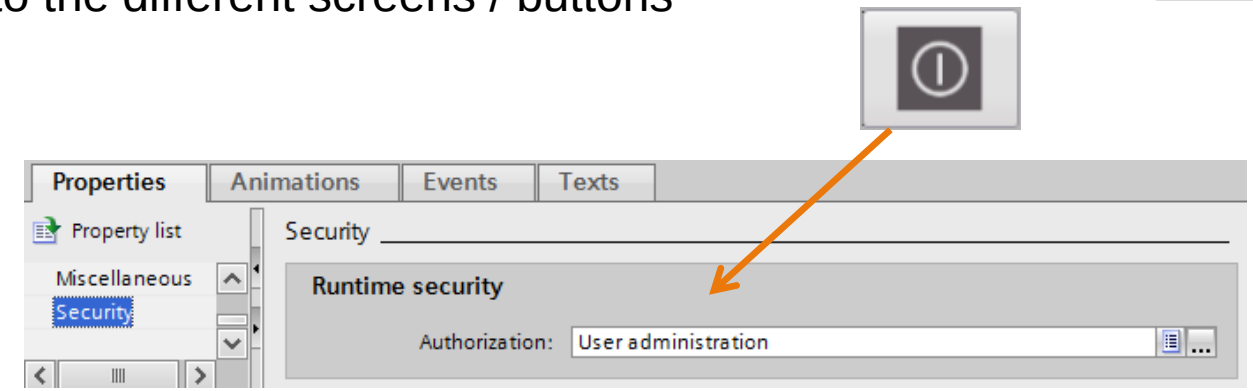
- HMI has different screens to operate machine in automatic or manual mode
- Machine might get damaged if operated in manual mode
- Some employees have insufficient training

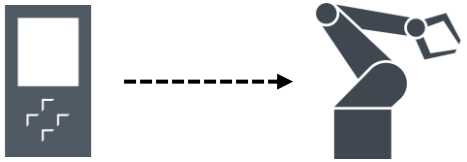


Solution

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







SIEMENS

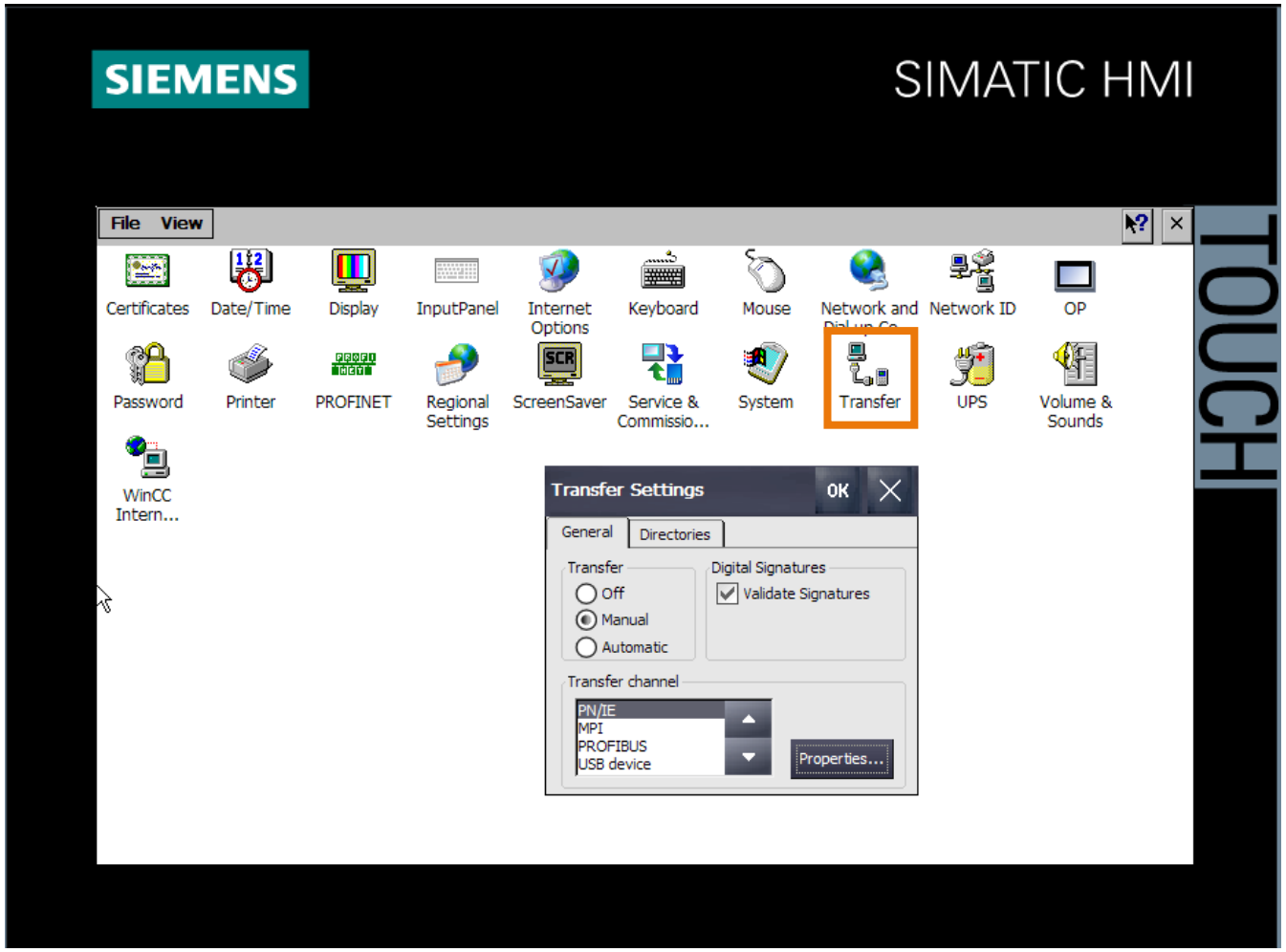
HMI & WinCC: Secure Access
Protect against unauthorized download

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

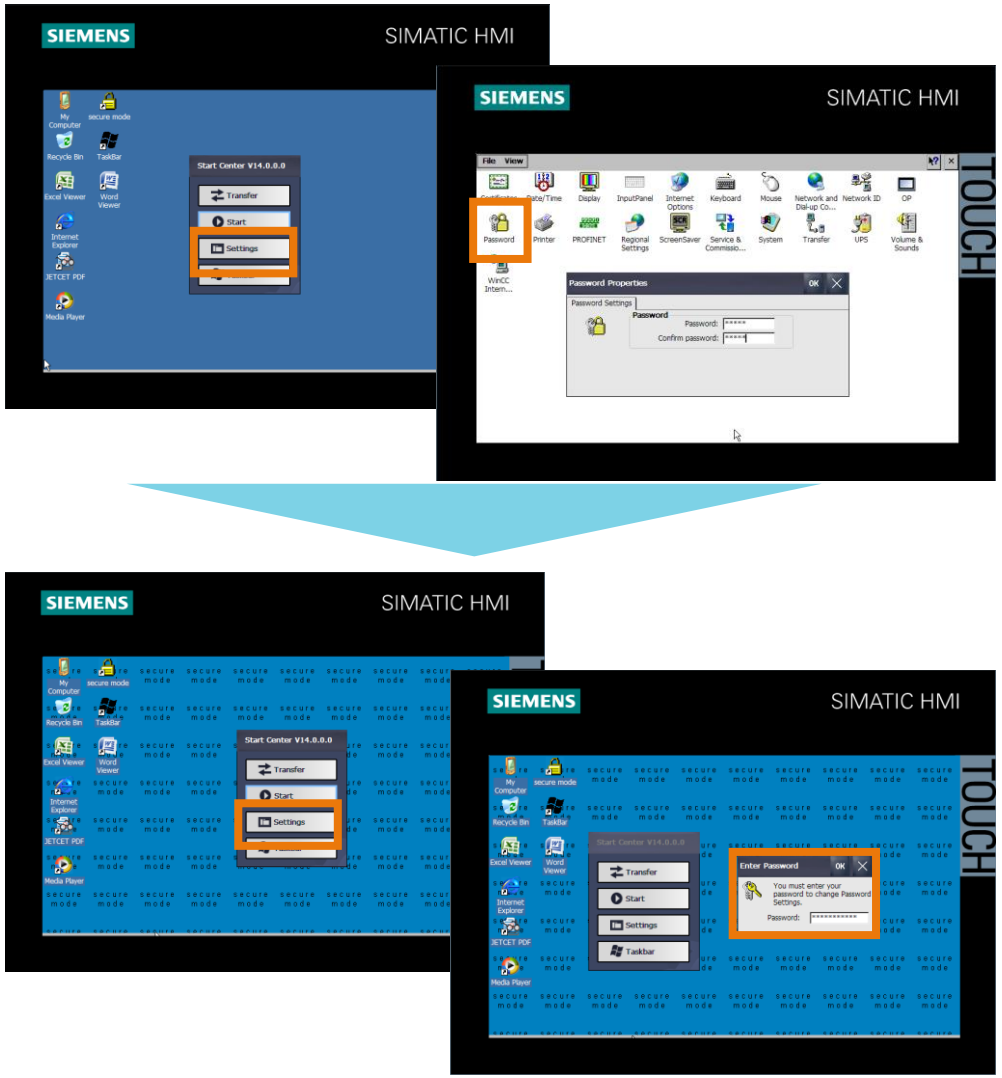


SIEMENS

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

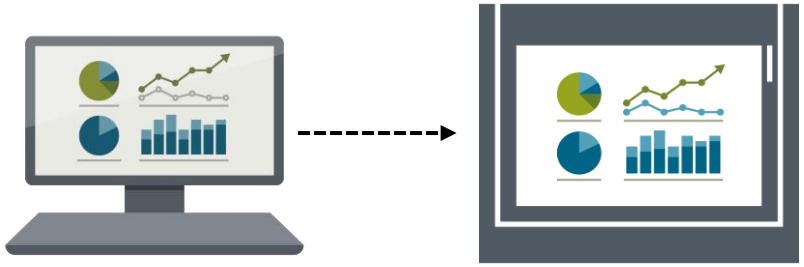


SIEMENS

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

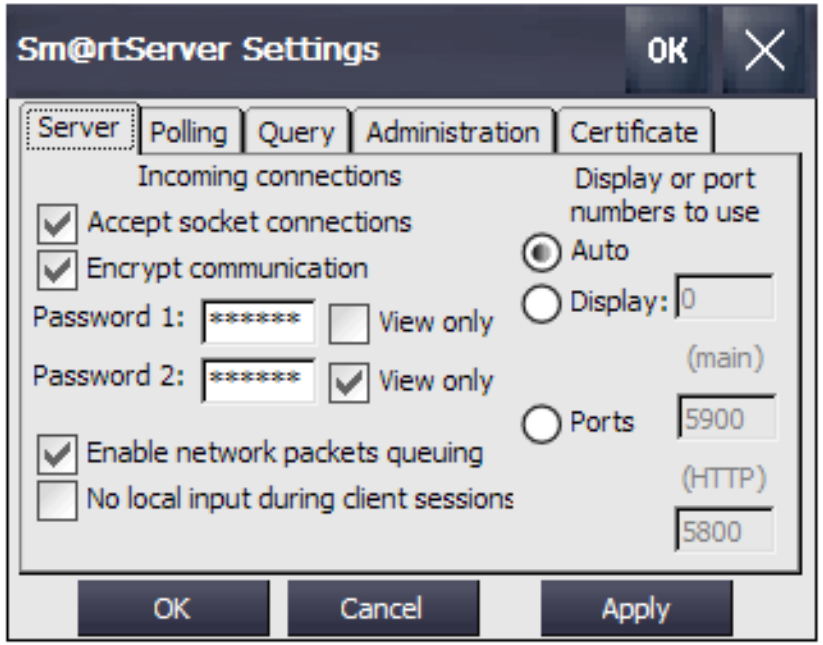
Challenge

- 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

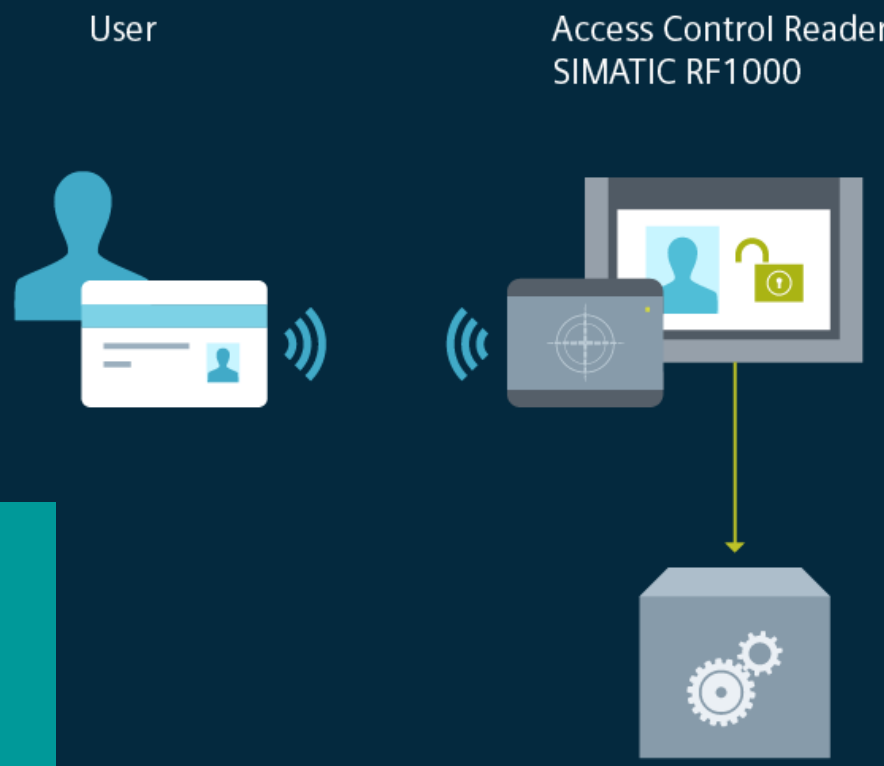


SIEMENS

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.



SIEMENS

Industrial Security
Access control with SIMATIC RFID Card Reader

SIMATIC RFID Card reader

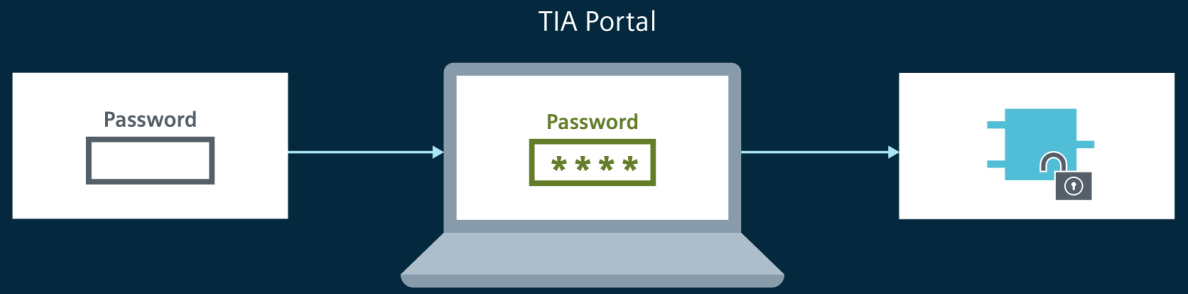
- Protects automation machinery
- Reliably identify operators
- Assign appropriate access rights based on user
- Quick & easy login during operator changeover

RJ45 Locks protect against:

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

SIEMENS

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.

SIEMENS

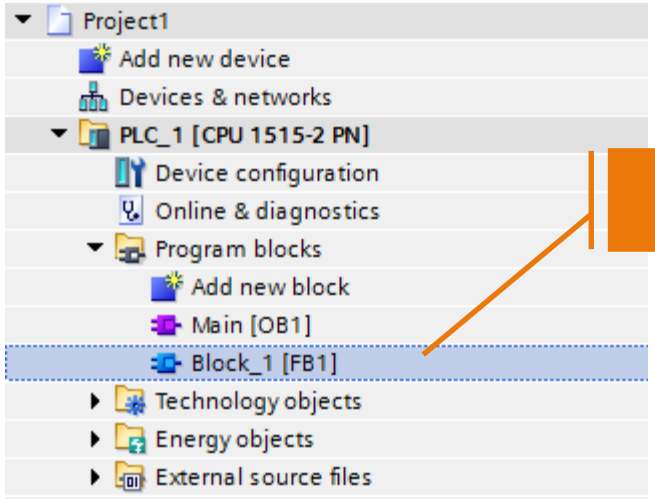
SIMATIC S7 CPU: Know-How Protection
Protect your engineering know-how!

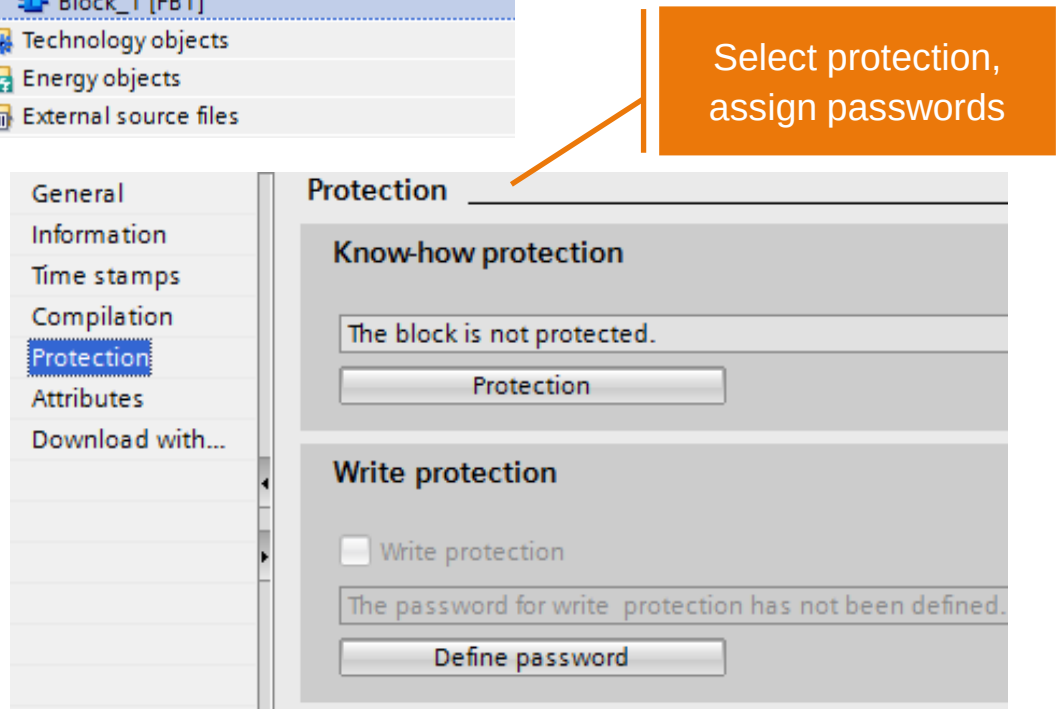
Know-How Protection

- 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.



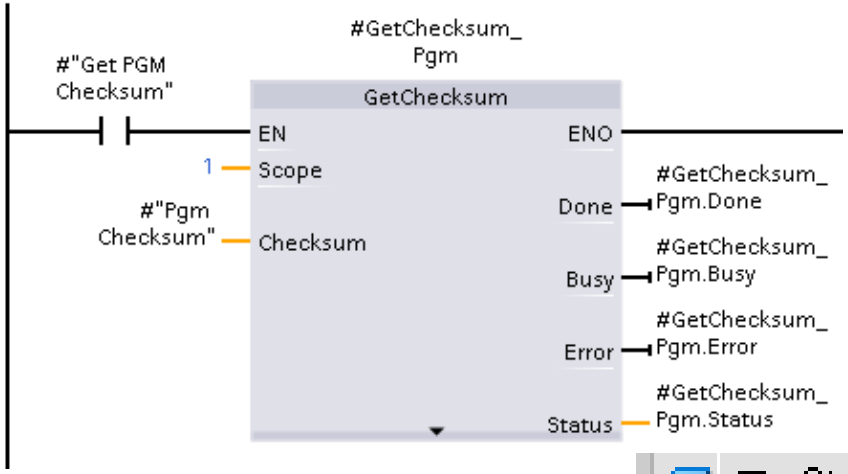


SIEMENS

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

Check integrity during runtime

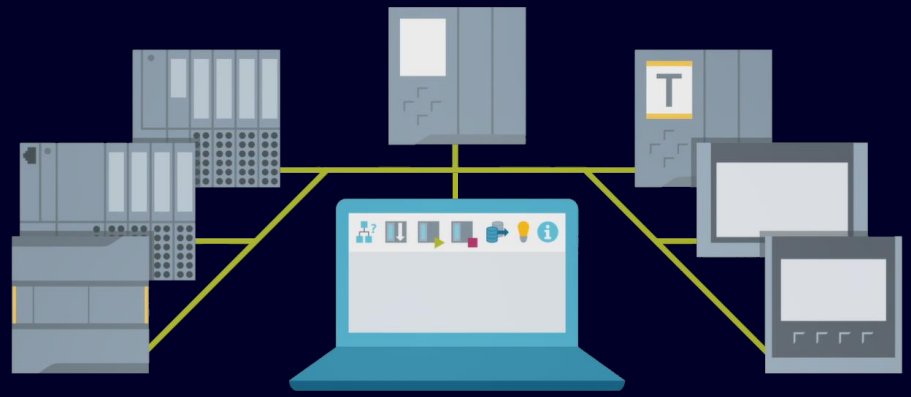
- By use of instruction *GetChecksum* the integrity of the PLC program and data can be checked during runtime
  - ➢ **Detects manipulation/ unauthorized program changes**



	Static	
	Pgm Checksum	Array[0..7] of Byte
	Text Checksum	Array[0..7] of Byte

SIEMENS

System Integrity: Asset Management

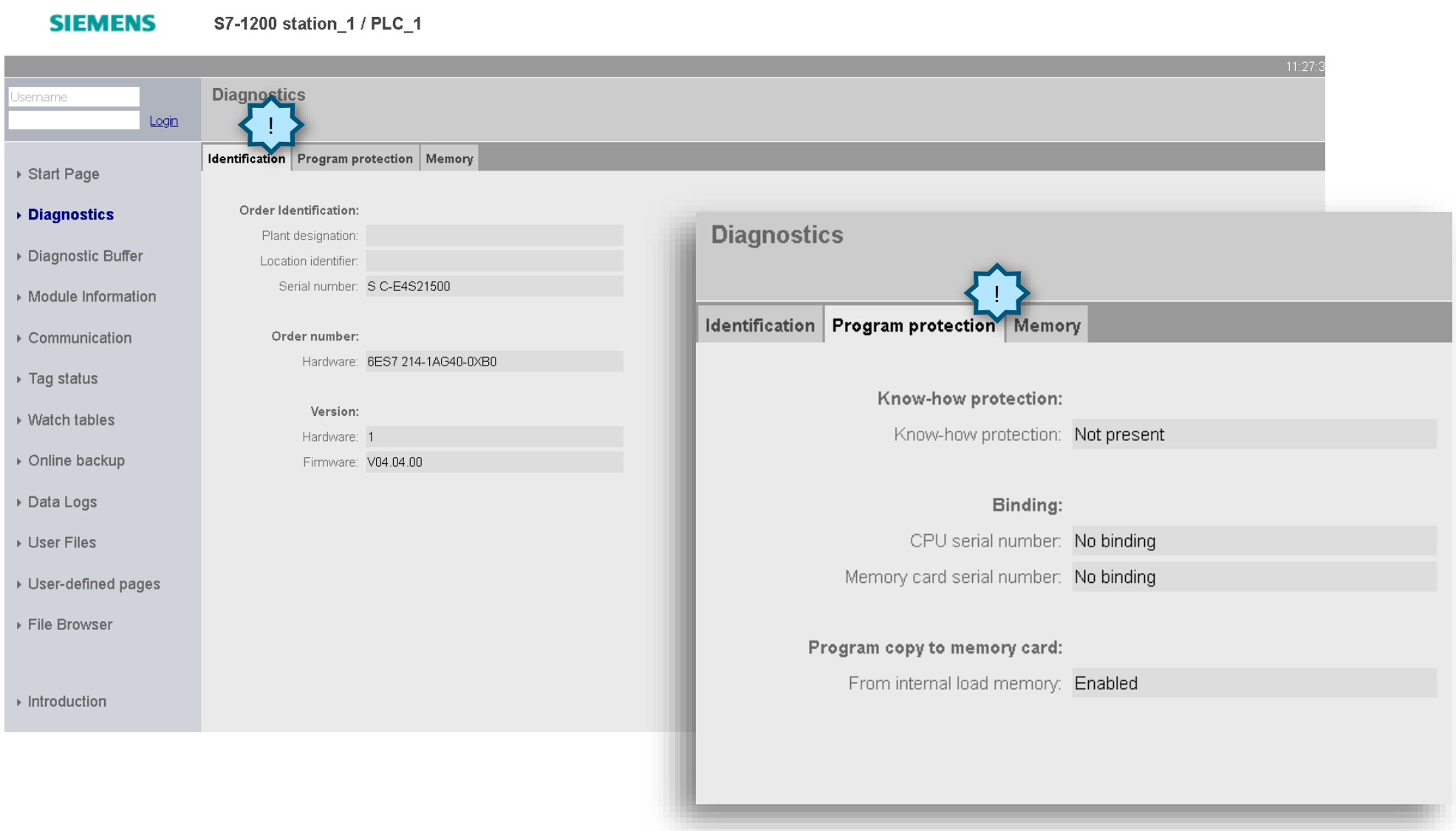


IEC 62443-3-3 – SR 7.3 SL1
The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.

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.

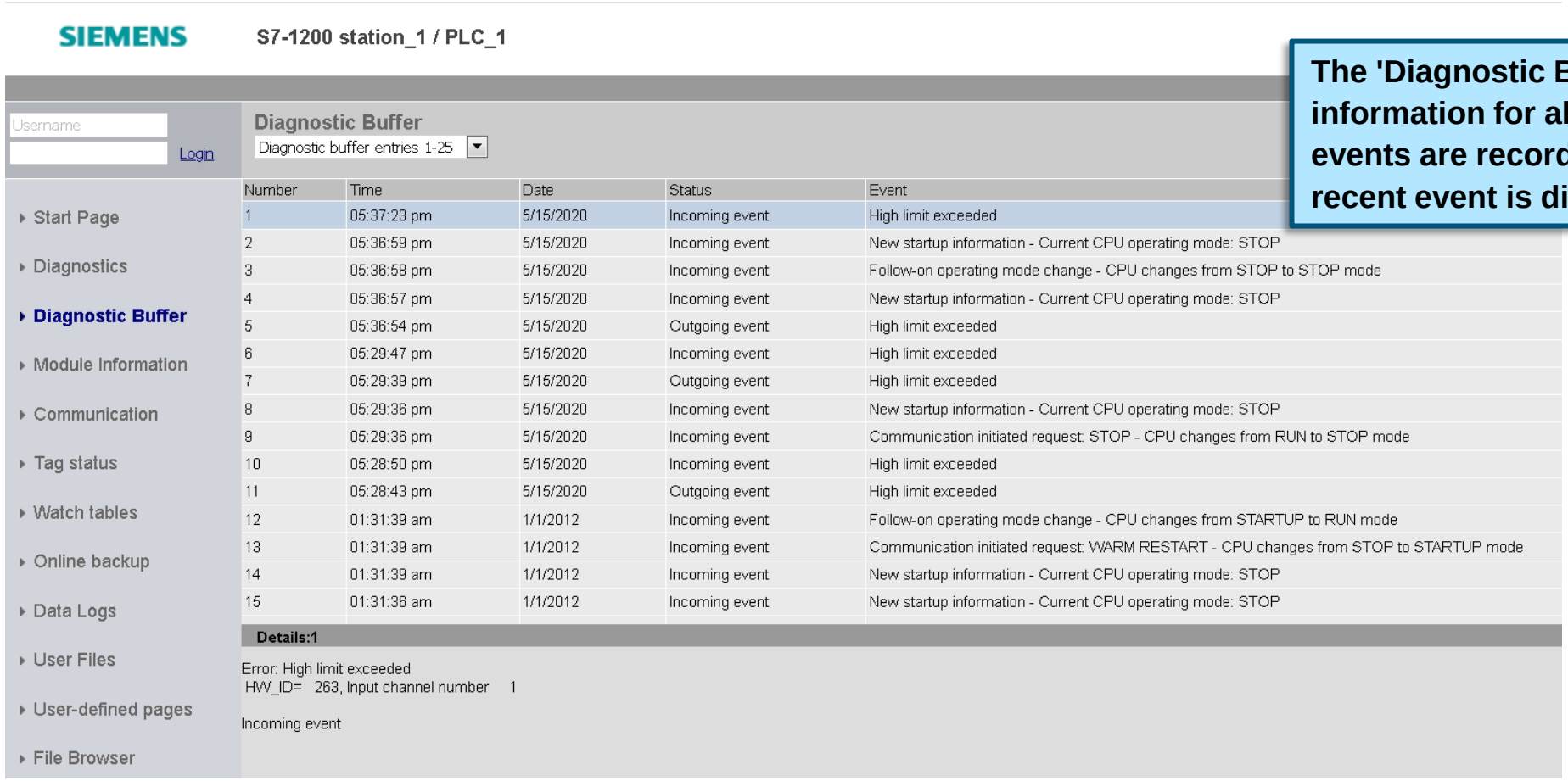
SIEMENS

Online Diagnostic & Maintenance Features
Integrated Web Server - Diagnostics



SIEMENS

Online Diagnostic & Maintenance Features
Integrated Web Server – Diagnostics Buffer



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.

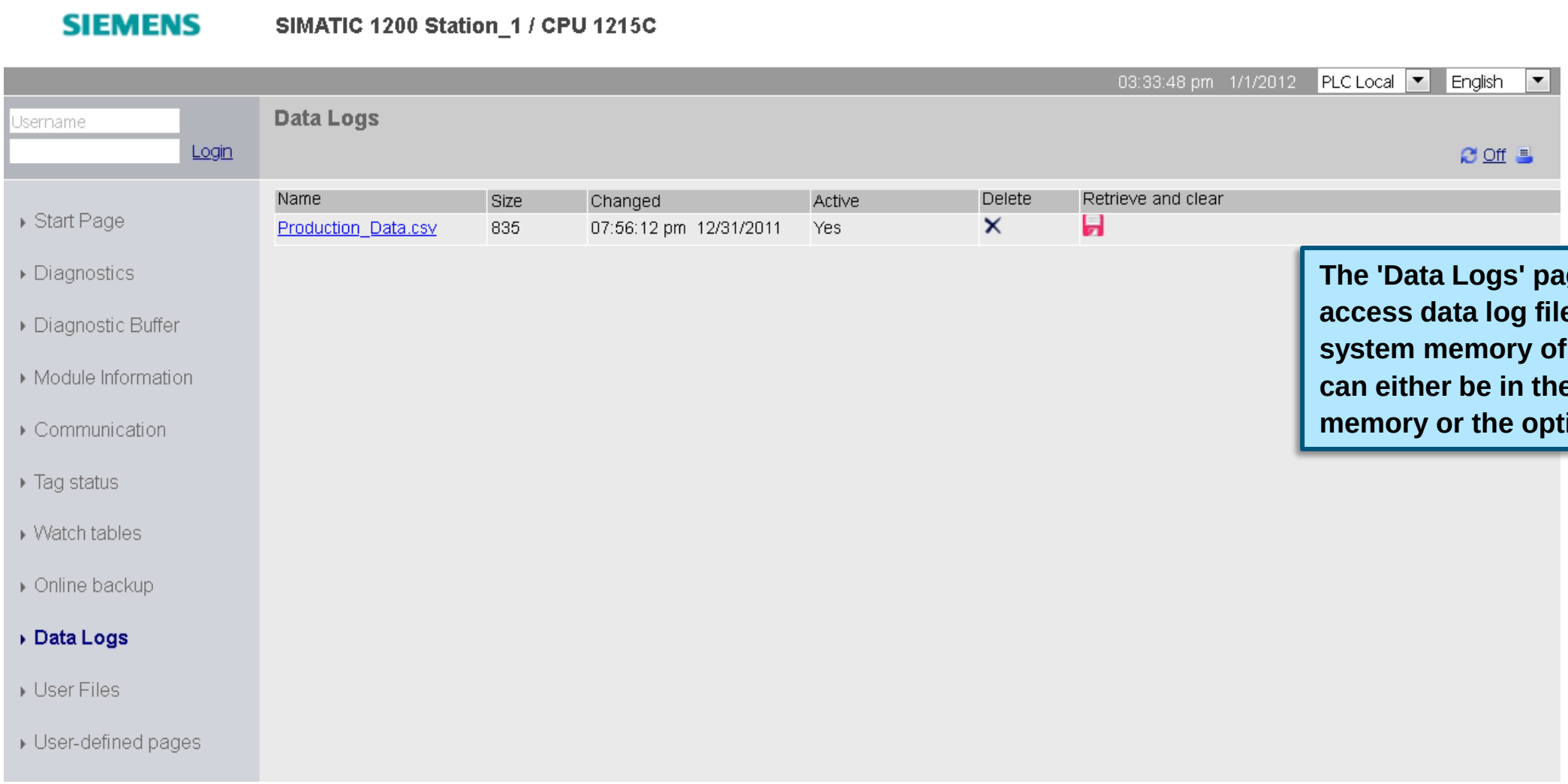
SIEMENS

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

Create a backup of the project in the PLC and/or restore your PLC from a previous backup file.

SIEMENS

Online Diagnostic & Maintenance Features
Integrated Web Server – Data Logs



The 'Data Logs' page allows you to access data log files stored in the system memory of the CPU. This can either be in the integrated CPU memory or the optional SD Card.

SIEMENS

Online Diagnostic & Maintenance Features
Integrated Web Server – File Browser

The "File Browser" page allows you to access system-generated files such as recipes and data logs files.

SIEMENS

SIMATIC Automation Tool

SIMATIC Controller incl. safety	**I/Os**	**SIMATIC HMI**	**Other**

incl. T-CPU and MFP

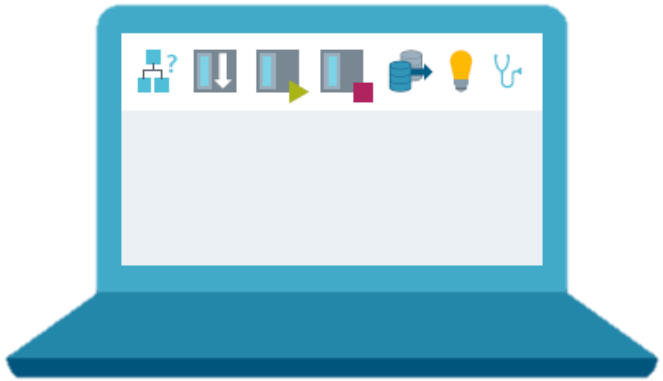
SITOP

SCALANCE X

MOBY / RFID

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

SIEMENS

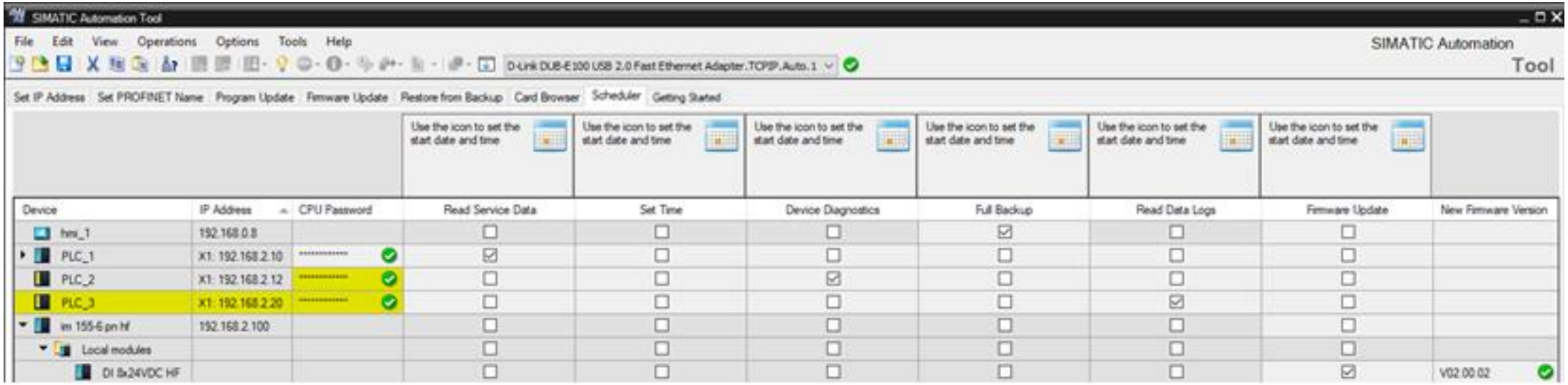
SIMATIC Automation Tool V4.0 Advanced – Scheduler

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



SIEMENS

Kontakt

Morten Kromann
morten.kromann@siemens.com

SIEMENS

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