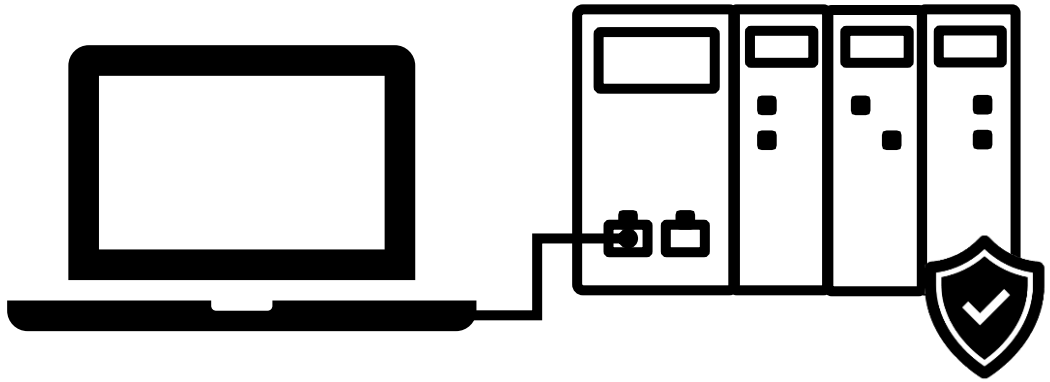
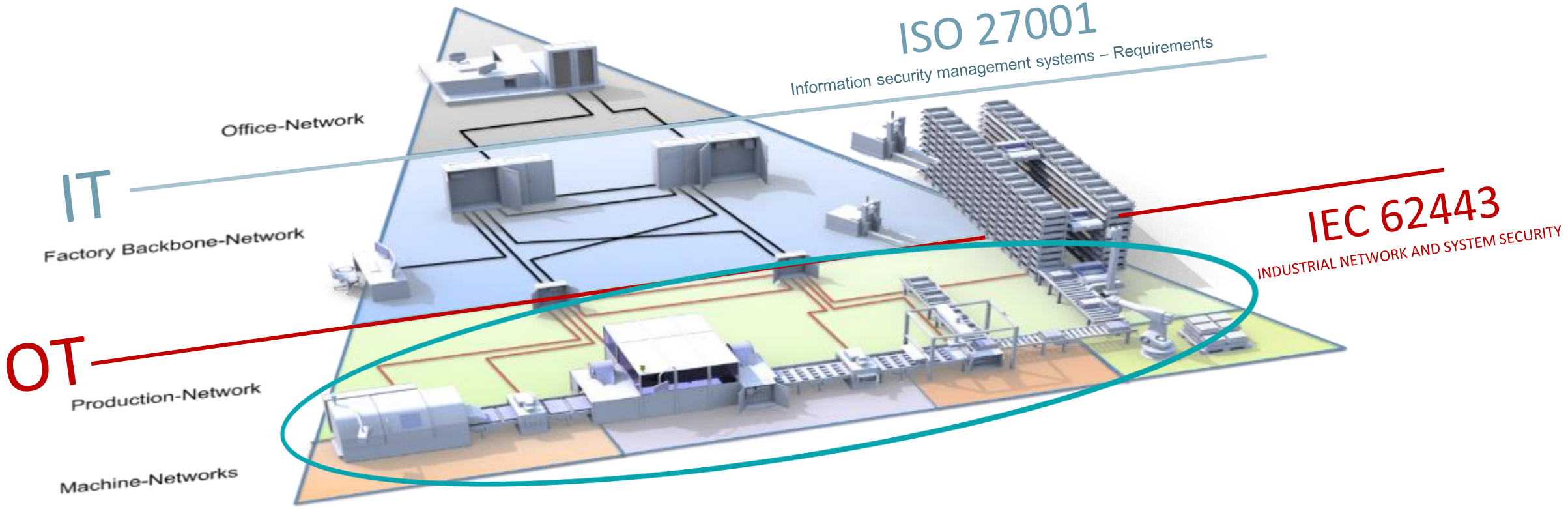
Help! Mijn PLC systeem moet voldoen aan IEC 62443-4-2!



Industrial Cyber Security

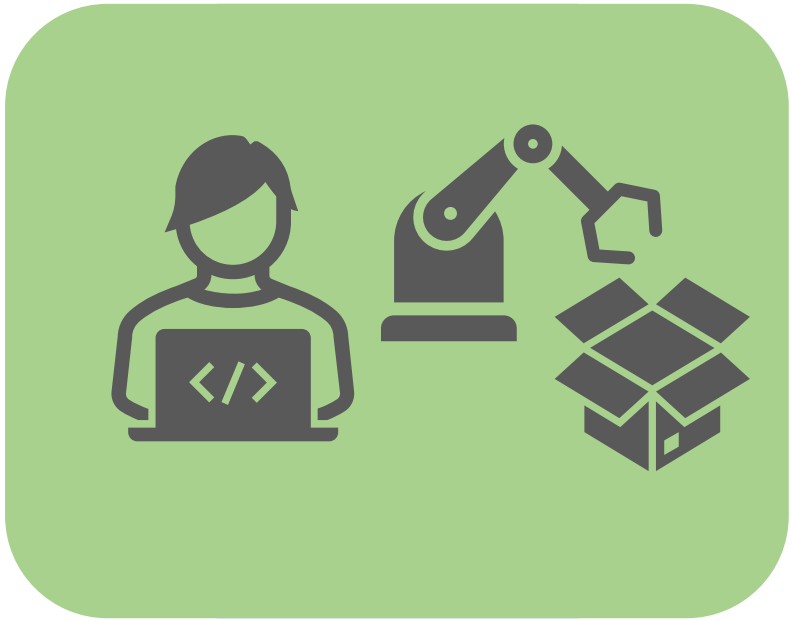
10 oktober 2023 | Congrescentrum 1931, den Bosch



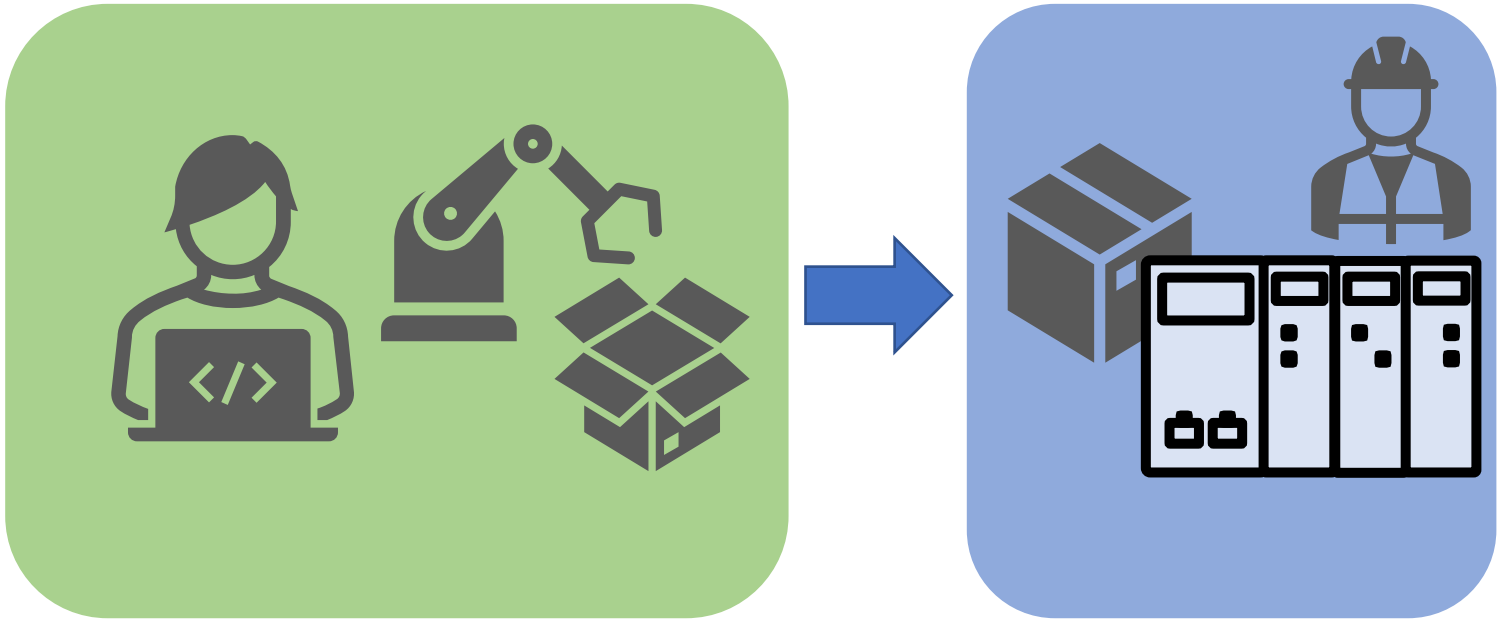
Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

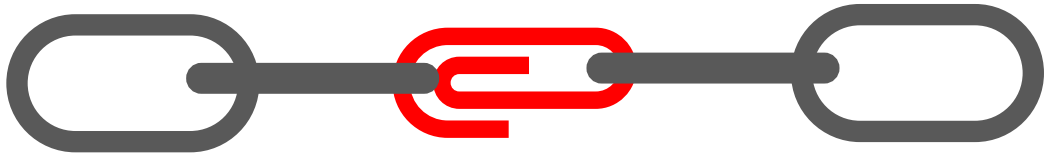
Fabrikant?

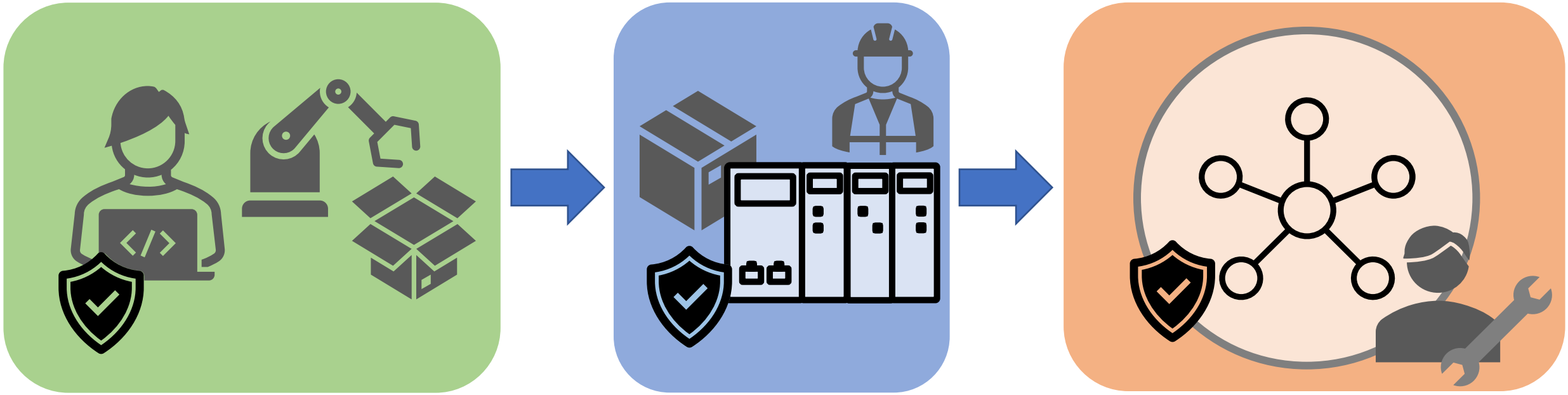


Fabrikant of systeemintegrator?



Fabrikant, systeemintegrator of eindgebruiker?





Daarom IEC 62443!

IEC 62443 structuur en systematiek

General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use-cases	
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

Rol:
Systeem eigenaar

Rol:
Systeemintegrator

Rol:
Fabrikant

Process requirements

Functional requirements

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Daarom IEC 62443!

IEC 62443 structuur en systematiek

General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use-cases
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

Process requirements

Functional requirements

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Daarom IEC 62443!

IEC 62443 structuur en systematiek

General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use-cases
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

Process requirements

Functional requirements

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Secure Development Lifecycle (SDL) volgens IEC 62443-4-1

IEC 62443 4-1 definieert 8 practices & 47 requirements

1. **SM** Security Management
2. **SR** Security Requirements
3. **SD** Secure by Design
4. **SI** Secure Implementation
5. **SVV** Security Verification and Validation testing
6. **DM** Security Defect Management
7. **SUM** Security Update Management
8. **SG** Security Guidelines

Secure Development Lifecycle (SDL) volgens IEC 62443-4-1

Waarvoor zoveel moeite?

Security Management **SM**

Development Process & Environment | Roles & Responsibilities | Expertise | Handling of External Components | Continuous Improvement

Training	Requirements	Design	Implementation	Verification & Validation	Release	Response
	SR	SD	SI	SVV	DM SG	DM SUM

IEC 62443-4-2 definieert ca. 70 Security-functies voor SL3 :

- Vooral de embedded device requirements (EDR) vereisen een robuuste implementatie van de cryptografie in het device en een beveiligingsinfrastructuur.
  (Secure Device Identity IEEE 802.1AR)

- De certificering van de SDL volgens IEC 62443-4-1 stelt de fabrikant van het apparaat in staat om de processen vast te stellen en, in het geval van een productcertificering volgens IEC 62443-4-2, om de producteigenschappen te bewijzen.

EDR 3.10 Support for updates
EDR 3.10 RE1 Update authenticity and integrity
EDR 3.11 Physical tamper resistance and detection
EDR 3.11 RE1 Notification of a tampering attempt
EDR 3.12 Provisioning product supplier roots of trust
EDR 3.13 Provisioning asset owner roots of trust
EDR 3.14 Integrity of the boot process
EDR 3.14 RE1 Authenticity of the boot process

Secure Development Lifecycle (SDL) volgens IEC 62443-4-1

Geen security zonder proceskwaliteit!

IEC 62443-4-2 definieert ca. 70 Security-functies voor SL3 :

- Vooral de embedded device requirements (EDR) vereisen een robuuste implementatie van de cryptografie in het device en een beveiligingsinfrastructuur.
  (Secure Device Identity IEEE 802.1AR)

- De certificering van de SDL volgens IEC 62443-4-1 stelt de fabrikant van het apparaat in staat om de processen vast te stellen en, in het geval van een productcertificering volgens IEC 62443-4-2, om de producteigenschappen te bewijzen.

EDR 3.10 Support for updates
EDR 3.10 RE1 Update authenticity and integrity
EDR 3.11 Physical tamper resistance and detection
EDR 3.11 RE1 Notification of a tampering attempt
EDR 3.12 Provisioning product supplier roots of trust
EDR 3.13 Provisioning asset owner roots of trust
EDR 3.14 Integrity of the boot process
EDR 3.14 RE1 Authenticity of the boot process

Security Profile

Hardware voorwaarden

- TPM met apparaat certificaat
- Integrity check tijdens boot fase
- Gebruik van gesegmenteerde netwerkverbindingen
- Bij gebruik van SD kaart: encrypted partitie, wachtwoord beveiligd

Firmware voorwaarden

- Security release van Linux modulen;
  geautomatiseerde scans naar nieuwe zwakheden
- Beveiligde communicatie TLS 1.2, HTTPS, OPC UA, SFTP, SSH, VPN
- User Manager welke rollen ondersteund, toelatingen, credentials en LDAP verbinding
- Certificate store voor fabrikant, systeemintegrators en eindgebruikers
- Firewall met management voor verschillende niveaus
- SYSLOG voor security berichtgeving en centrale opslag daarvan

Daarom IEC 62443!

IEC 62443 structuur en systematiek

General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use-cases	
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

Rol:
Systeem eigenaar

Rol:
Systeemintegrator

Rol:
Fabrikant

Process requirements

Functional requirements

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Daarom IEC 62443!

IEC 62443 structuur en systematiek

General

IEC-62443-1-1	IEC-62443-1-2	IEC-62443-1-3	IEC-62443-1-4
Concepts and models	Master glossary of terms and abbreviations	System security conformance metrics	IACS security life-cycle and use-cases

Policies and procedures

IEC-62443-2-1	IEC-62443-2-2	IEC-62443-2-3	IEC-62443-2-4	IEC-62443-2-5
Security program requirements for IACS asset owners	IACS protection levels	Patch management in the IACS environment	Security program requirements for IACS service providers	Implementation guidance for IACS asset owners

System

IEC-62443-3-1	IEC-62443-3-2	IEC-62443-3-3
Security technologies for IACS	Security risk assessment and system design	System security requirements and security levels

Component

IEC-62443-4-1	IEC-62443-4-2
Product security development life-cycle requirements	Technical security requirements for IACS components

Rol:
Systeem eigenaar

Rol:
Systeemintegrator

Rol:
Fabrikant

Process requirements

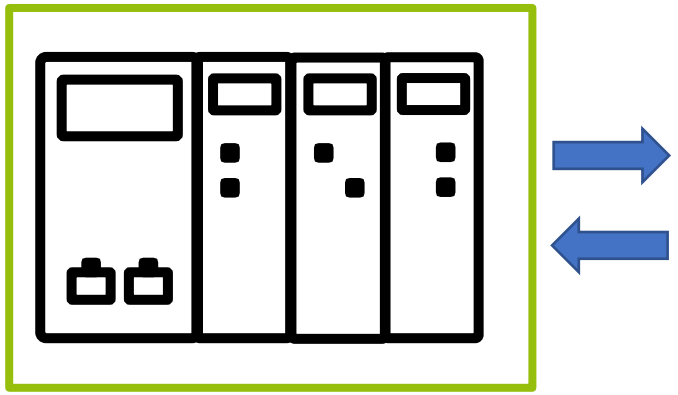
Functional requirements

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

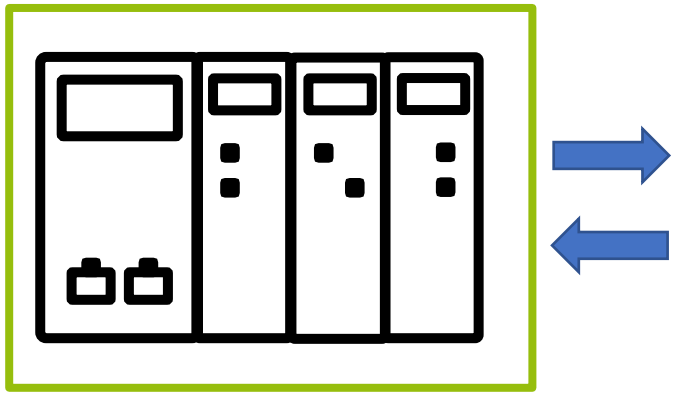
PLC security profiel (1/2)

- Clean device (Reset 1) en Boot met integrity check
- Least functionality
  - Gelimiteerde PLC openheid
  - Alleen noodzakelijke PLC modules worden geladen
  - Geen root access, geen SSH access, Admin uitgeschakeld
- Autorisatie
  - Wachtwoord complexiteit regels, lifetime restricties en timeouts (brute force protectie)
  - Nieuwe rollen “SecurityAdmin” and “SecurityAuditor” voor apparaat configuratie en security monitoring
  - Centraal User Management system met support via LDAP
- Zone en Denial of Service (DoS) protectie
  - Firewall enkel te activeren met WBM en Engineer software (secure)
  - Netload limiter voorgeconfigureerd

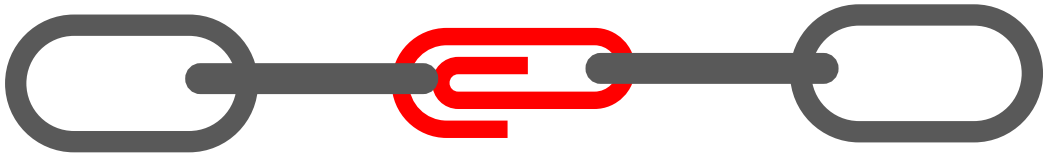


PLC security profiel (2/2)

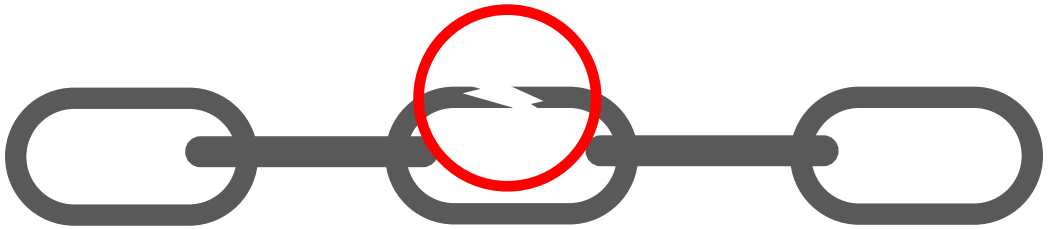
- Certificate Authority managed apparaat identiteit en vertrouwde partners
- Integriteit en Authenticiteit van data in rust en doorvoer
  - SD kaart met encrypted partitie
  - Enkel beveiligde communicatie; TLS 1.2 en OPC UA (signed & encrypted)
- Security logging
  - Beveiligde security logging
  - Connectie naar centrale server
- Expliciete her-activatie van PLC features via WBM
  - OPC UA, HMI
- Lokale I/Os worden ondersteund
- Profinet kan geactiveerd worden nadat er een Threat Analysis en beschermende maatregelen vanuit de security context worden genomen
- Schakelkast moet op slot; applicatie moet de toegang tot de kast monitoren



Fabrikant, systeemintegrator of eindgebruiker?



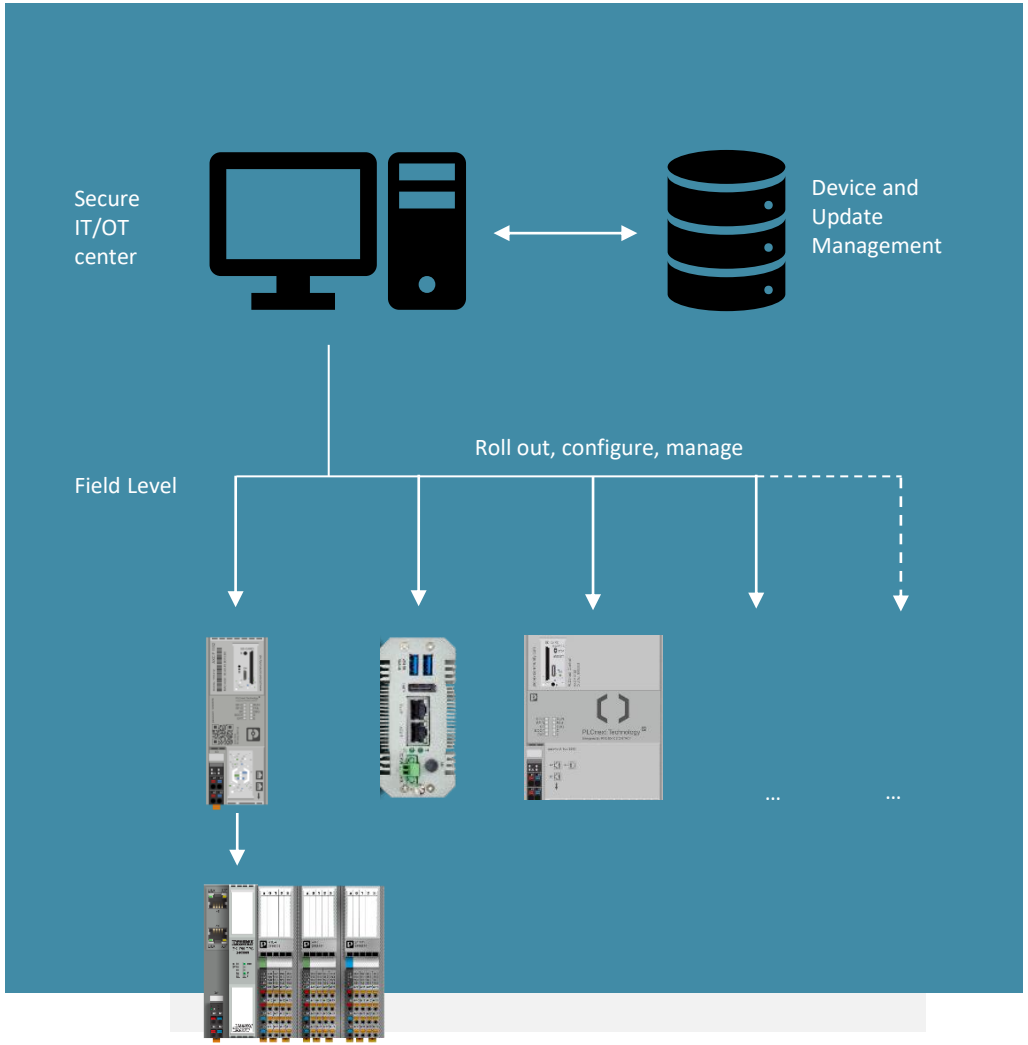
Fabrikant, systeemintegrator of eindgebruiker?



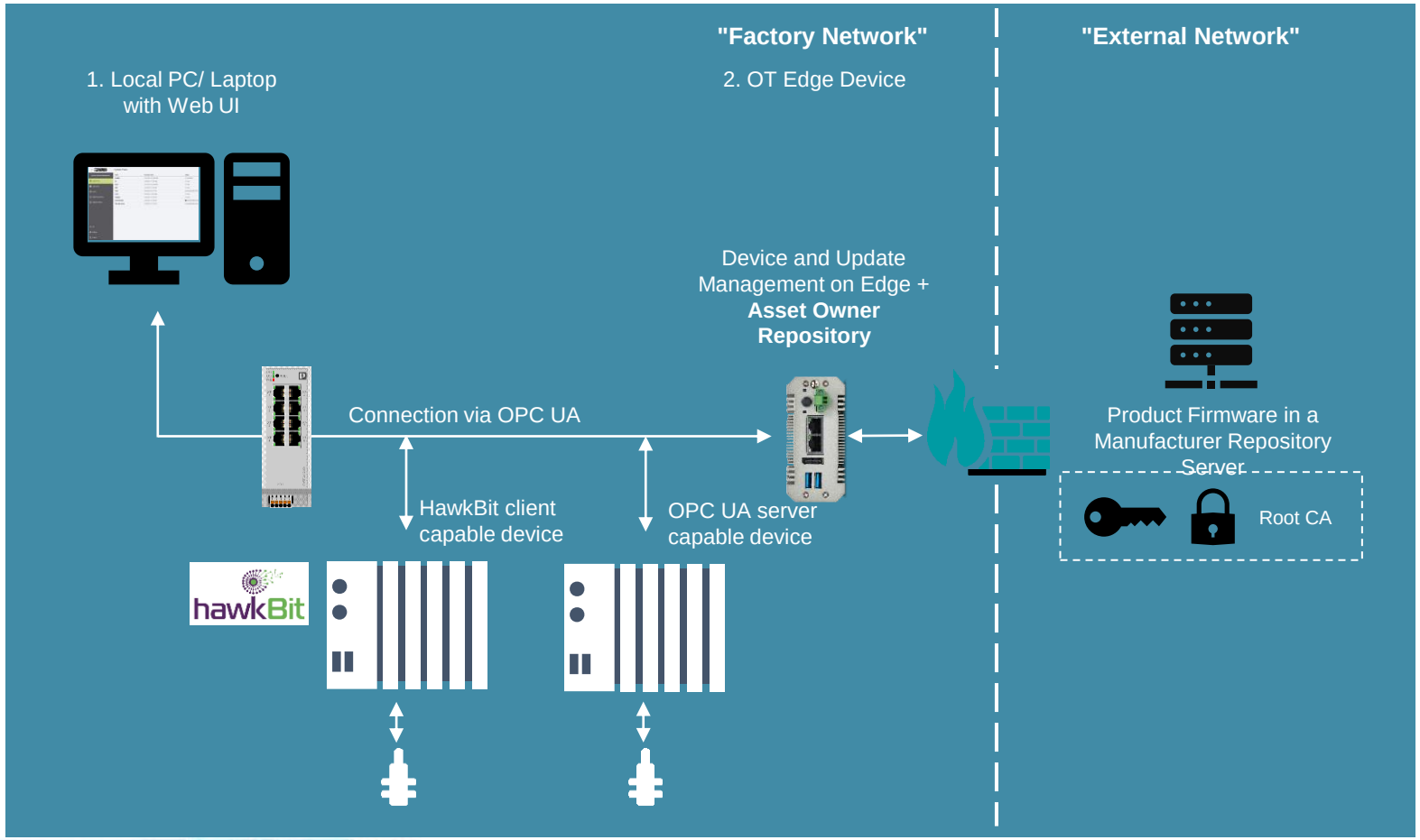
Samen!

Device & Update Management

- Cyber security requirements voor machines en systemen zijn enorm toegenomen de laatste tijd.
- Vandaag de dag worden nieuwe updates beschikbaar gemaakt via de product website. Maar hoe moeten operators hun apparatuur en updates managen zonder gecentraliseerd management systeem?
- We hebben open standaarden nodig om Device & Update Management holistisch te kunnen benaderen!
- OPC UA is zo'n standaard!



Device & Update Management on the edge



Device and Update Management Software on Edge automates the device management:

- Upcoming updates for the devices are available via the manufacturer's repository server.
- Updates can be installed manually or automatically on the connected devices at a specified time.
- A rollout can be managed centrally via the Update Management software.
- Devices that have an OPC UA server or a HawkBit client can be managed with this principle.

Bedankt voor uw aandacht!