security health mobility public IoT

PKI for Industrial Communication Networks and Devices

Dr.-Ing. Michael Jahnich, Business Development

achelos

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Secur|Ty made in EU

Trust Seal www.teletrust.de/itsmie

Security for connected solutions in industry and traffic

achelos

Public key infrastructures forms the basis of interconnected devices, machines and systems, whether in **manufacturing** to improve digitalization of processes (industry 4.0) or in the development of future **connected transport and traffic solutions**.

Agenda

a. Industrial Control Systems and Communication Networks

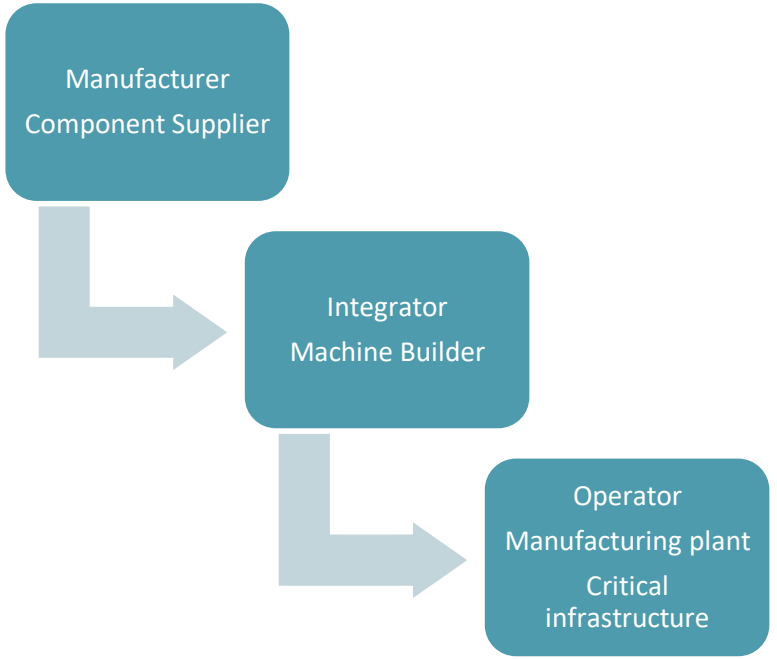
b. ICS Use Cases

c. ICS standards and PKI

d. Best practices for industrial PKI

ICS - Definitions

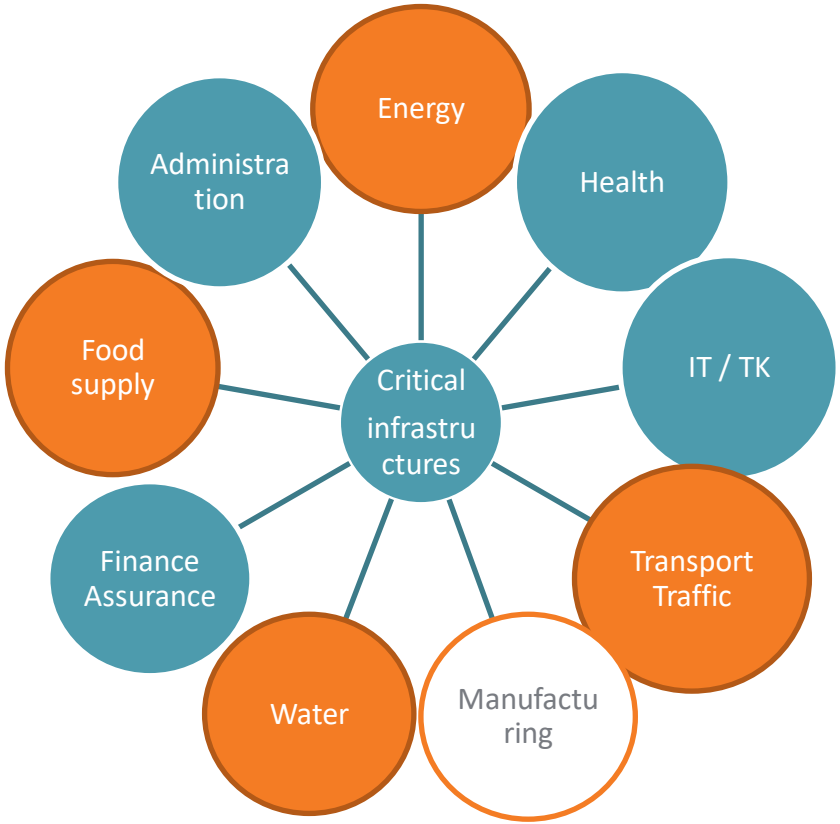
- Industrial Control Systems (ICS, also IACS)
  - Collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process (IEC 62443)
- Interconnected systems and applications
- Equipment used in
  - manufacturing and processing plants
  - Distributed operations such as utilities
  - transportation networks, automated or remotely controlled
  - building environmental control
- Includes Supervisory Control and Data Acquisition systems (SCADA)



Sensors, actuators, routers, machines, industrial robots …

Threats associated with ICS

- Denial of service
- Breach of trade secrets
- Shortage of supply
- Environmental damage
- Damage/loss of life
- Loss of production
- Regulatory violations
- Image damage



ICS Trends

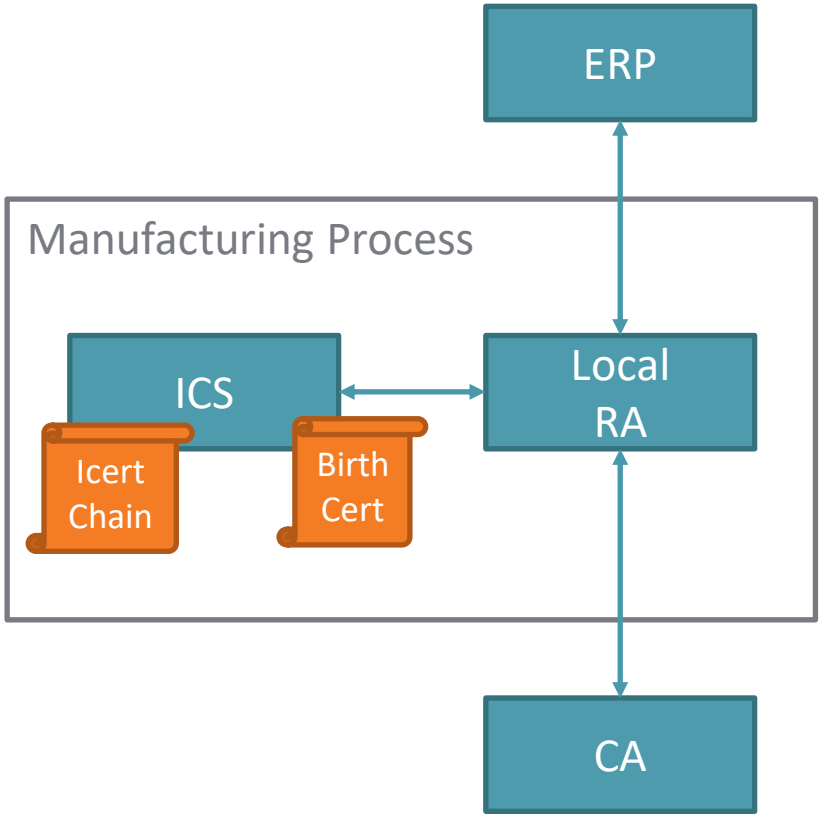
achelos

Today -> Future

- Fully interconnected systems across locations and companies
- Public/private cloud services for ICS
- Operator models/Admin Asset Shells
- Remote OTA Software-Update
- Remote Device Management
- Less non-critical infrastructure
- Crypto agility and PQC

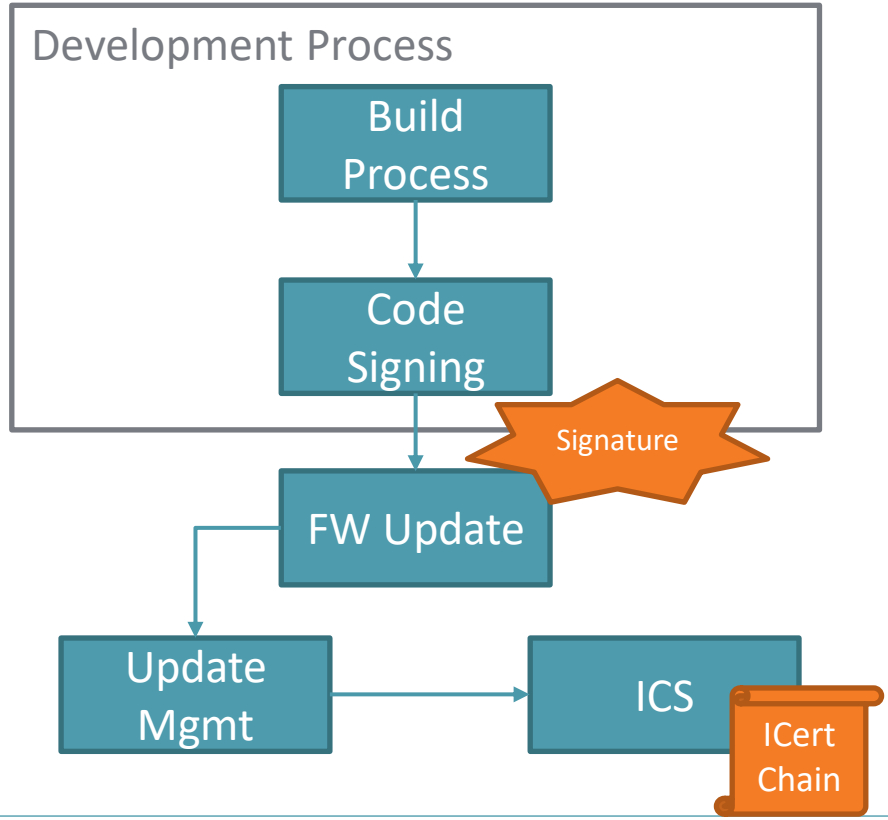
Secure Device Identity

- Device life cycle = cert life-cycle
- Certificate-based authentication, identification
- Automated key- and certificate generation
- IEEE 802.1AR: Initial Device ID in the manufacturer‘s production area
- Lightweight CMP profile for IoT



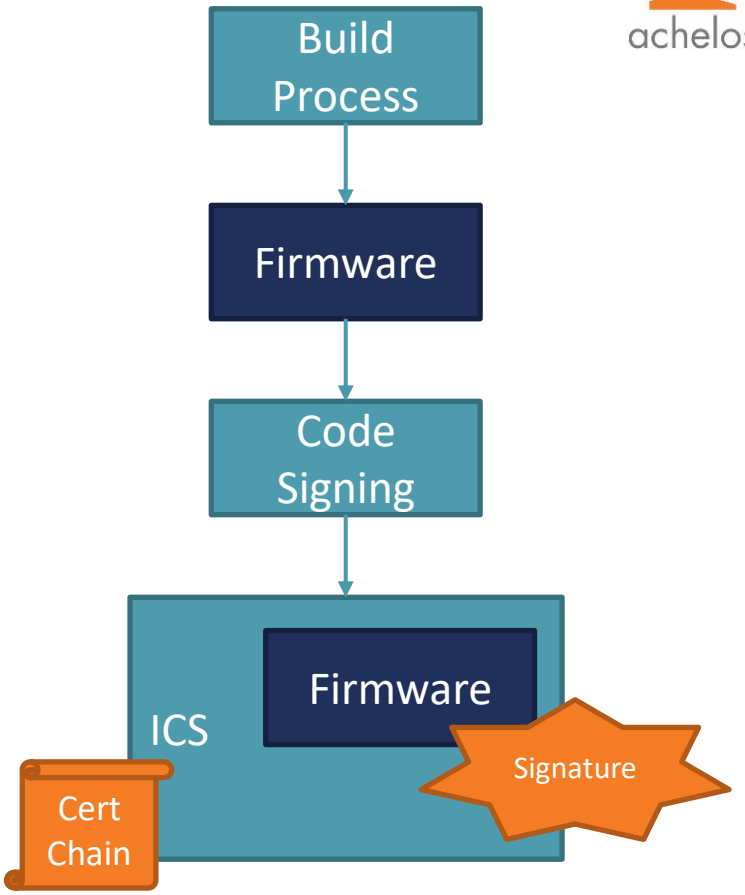
Secure Update Management

- Signed firmware-updates
- Protection against malware and software modifications
- Verification of the software‘s authenticity before performing the update
- Authorization
  - Activation of functionality/features
  - Acceptance of 3rd party software



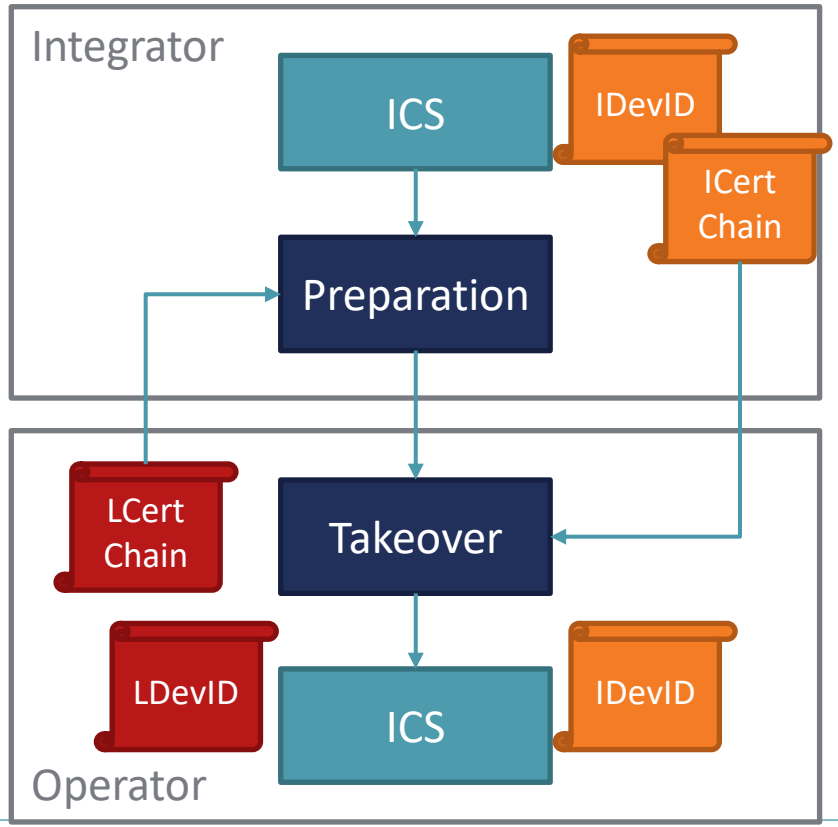
Secure Device Booting

- Verification of firmware's authenticity before system startup
- Integrity of code in ICS components used in critical infrastructures
- Secure key and certificate management



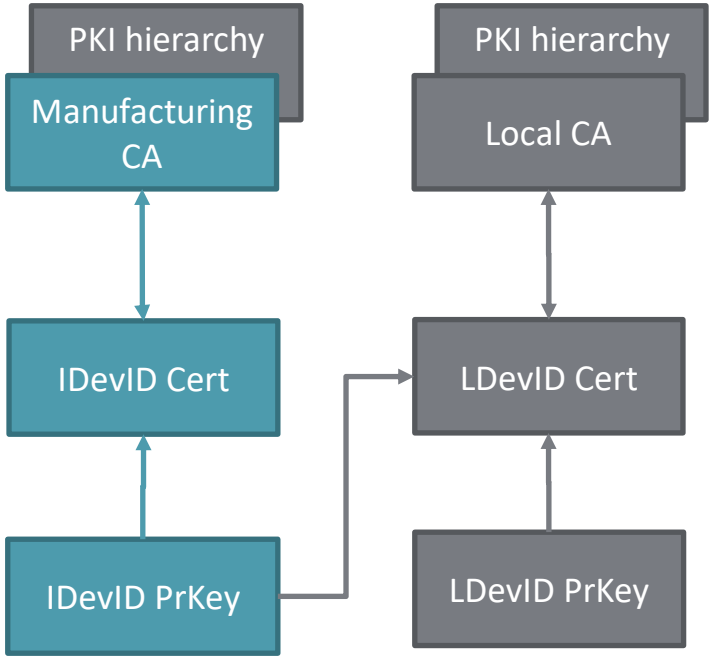
Secure Device Commissioning

- Secured change of ownership and responsibility
- Operator creates locally significiant Device ID after authentication (mutual)
- IEEE 802.1AR: Locally significant Device ID for authentication in the operative environment
- No common root of trust
- Zero touch -> BRSKI



ICS Standards and PKI: IEEE 802.1AR

- Based on asymmetric cryptography
  - RSA-2048/SHA-256
  - ECDSA P-256/SHA-256
  - ECDSA P-384/SHA-384
- Defines DevID Trust Model
- Manufacturer shall publish CP / CPS and trust anchor for each IDevID
- No requirement for a “global trust anchor”
- No requirements on PKI operations



grey is optional

ICS Standards and PKI: CMP

- Lightweight CMP profile (draft)
- Recommends proper processes for issuance, management, verification, revocation, and audit for authorized devices, users and processes.
- Recommends PKI operation according to commonly accepted best practices is also required in IEC 62443-3-3 for security level 2 up to security level 4

IEC 62443

- THE cybersecurity standard for ICS systems
- Risk-based approach to manage security risks
- ICS operators: Cyber Security Management System
- ICS integrators: Security requirements and techniques for systems
- ICS manufacturers: SDL and security requirements for products

- IEC provides conformity assessment and certification of ICS

Security Levels – SL(capability)

- Associated with each security requirement for systems/products
- Requirement enhancements for higher SL

Security levels	Means	Resources	Motivation	Skills
SL-1	eavesdropping or exposure, casual or accidental			
SL-2	simple	limited	low	generic
SL-3	sophisticated	moderate	moderate	ICS specific
SL-4	sophisticated	extensive	high	ICS specific

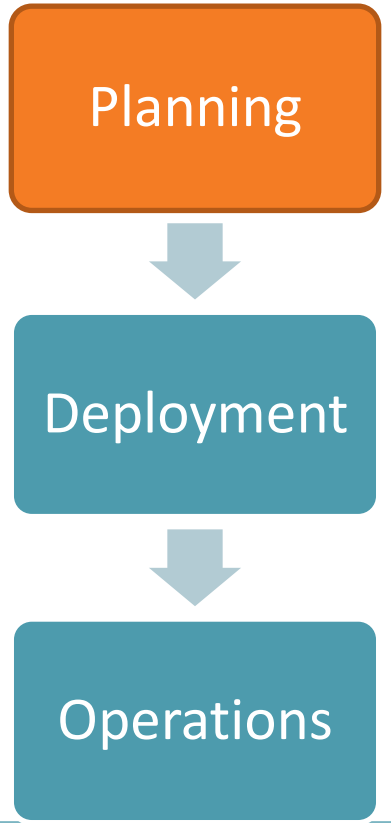
ICS Standards and PKI: IEC 62443-4-2

- SR 1.8 – PKI Certificates
  - „Capability to operate a PKI according to commonly accepted best practices or obtain certificates from existing PKI“
  - Certificate Policy based on risk assessment based on RFC 3647
  - Security Level 2 to 4
- SR 1.9 – Strength of public-key authentication
- SR 1.9 RE – Hardware security for public key authentication
  - Security levels 3 and 4
- SR 4.3 Use of cryptography according to commonly accepted industry practices and recommendations

What are PKI best practices in the Industrial Sector?

Industrial PKI best practices – planning 1

- Objective: lay foundation of secure industrial PKI operations
- PKI solution architecture
  - Use cases – current and future
  - IT infrastructure
  - System interfaces
  - Operational, adminstrative, physical measures and processes
  - Implementation and operational costs



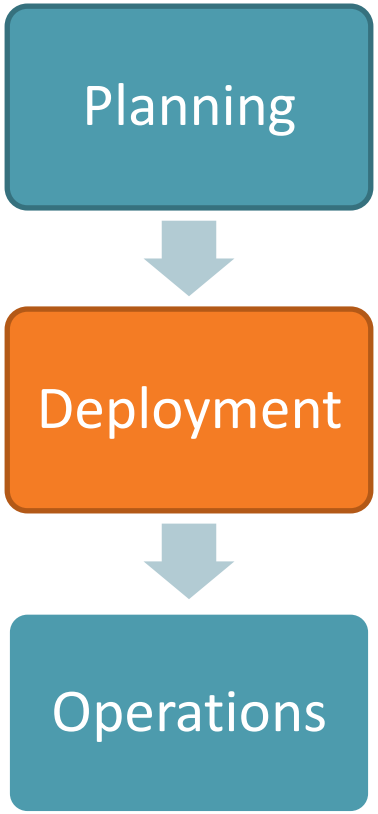
Industrial PKI best practices – planning 2

- Risk Assessment for each use case
- Certificate Policy
- Certification Practice Statement

- Implementation options
  - Public or private PKI
  - On-premise or cloud services
  - Managed services

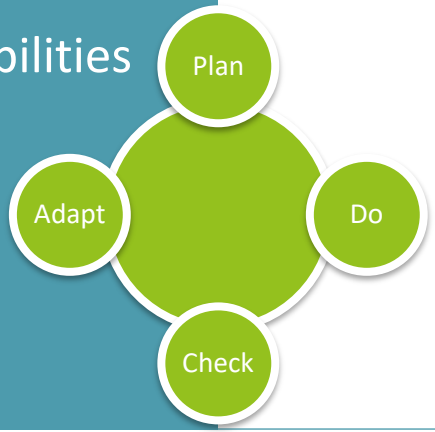
Industrial PKI best practices – deployment

- Integration into existing IT
  - Build process
  - Manufacturing process
- Integration and acceptance testing
- Integration into ISMS / CSMS
- Internal/external audit/evaluation
- Enable people to operate PKI
- Document operational processes



Industrial PKI best practices – operations

- Objective: maintain security
- Regular audits
- Maintain and improve the quality of your documentation
- Maintain roles and responsibilities and abilities to operate PKI
- Train stuff



Vielen Dank! | Thank you!

achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com