IARIA CYBER 2025, Sep. 28 – Oct. 02, 2025 – Lisbon, Portugal

Attesting the Trustworthiness of a Credential Issuer: never trust – always verify

Dr. Rainer Falk, Steffen Fries
Siemens AG, Technology

SIEMENS

Authors’ background: Applied industrial research at Siemens Foundational Technologies

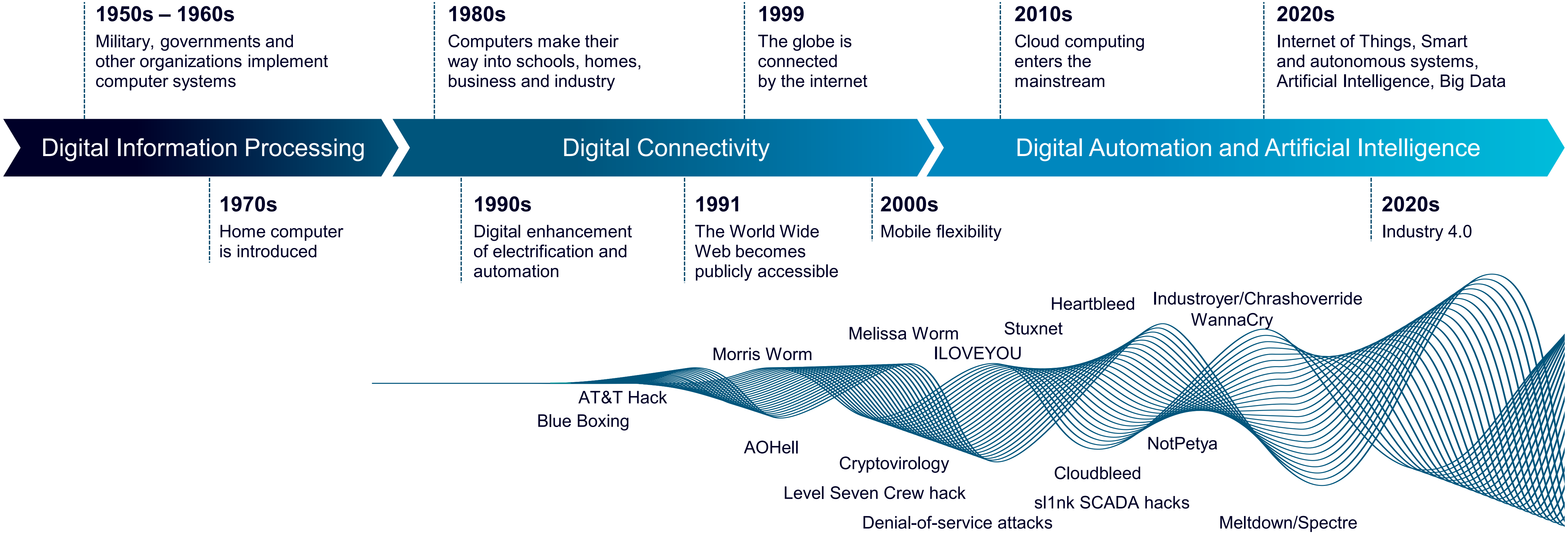
Cybersecurity for industrial systems

- Industrial systems need a security design that addresses the relevant security objectives and respects side conditions for the specific environment (e.g., lifetime, real-time, functional safety, usability).
- The industrial security standard IEC 62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.
- Regulations defining mandatory cyber-security requirements become increasingly relevant

Dr. Rainer Falk
Principal Key Expert
Siemens Technology

Steffen Fries
Principal Key Expert
Siemens Technology

Cybersecurity must be continuously evolved to address the changing threat and vulnerability landscape as well as changing system architectures



1950s – 1960s
Military, governments and other organizations implement computer systems

1970s
Home computer is introduced

1980s
Computers make their way into schools, homes, business and industry

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

1999
The globe is connected by the internet

2000s
Mobile flexibility

2010s
Cloud computing enters the mainstream

2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

2020s
Industry 4.0

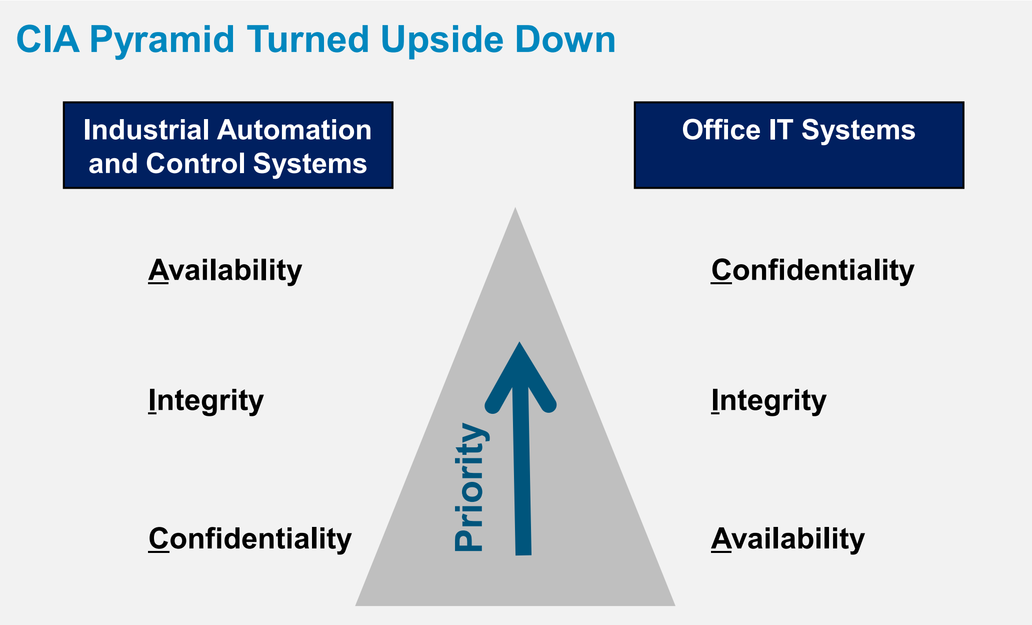
Digital Information Processing

Digital Connectivity

Digital Automation and Artificial Intelligence

Industrial systems require a specific approach to cybersecurity

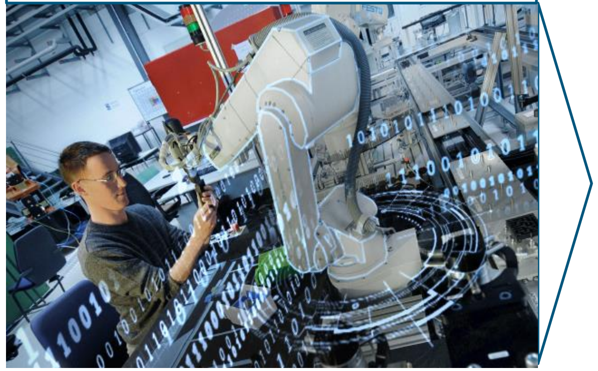
Applying security guidelines (and defined requirements, specific measures) suitable for enterprise IT does not work for industrial systems. A security design has to address the relevant security objectives and respect side conditions.



CIA Pyramid Turned Upside Down

Industrial Automation and Control Systems	Office IT Systems
Availability	Confidentiality
Integrity	Integrity
Confidentiality	Availability

Industrial Systems:
Protection of Production Resources

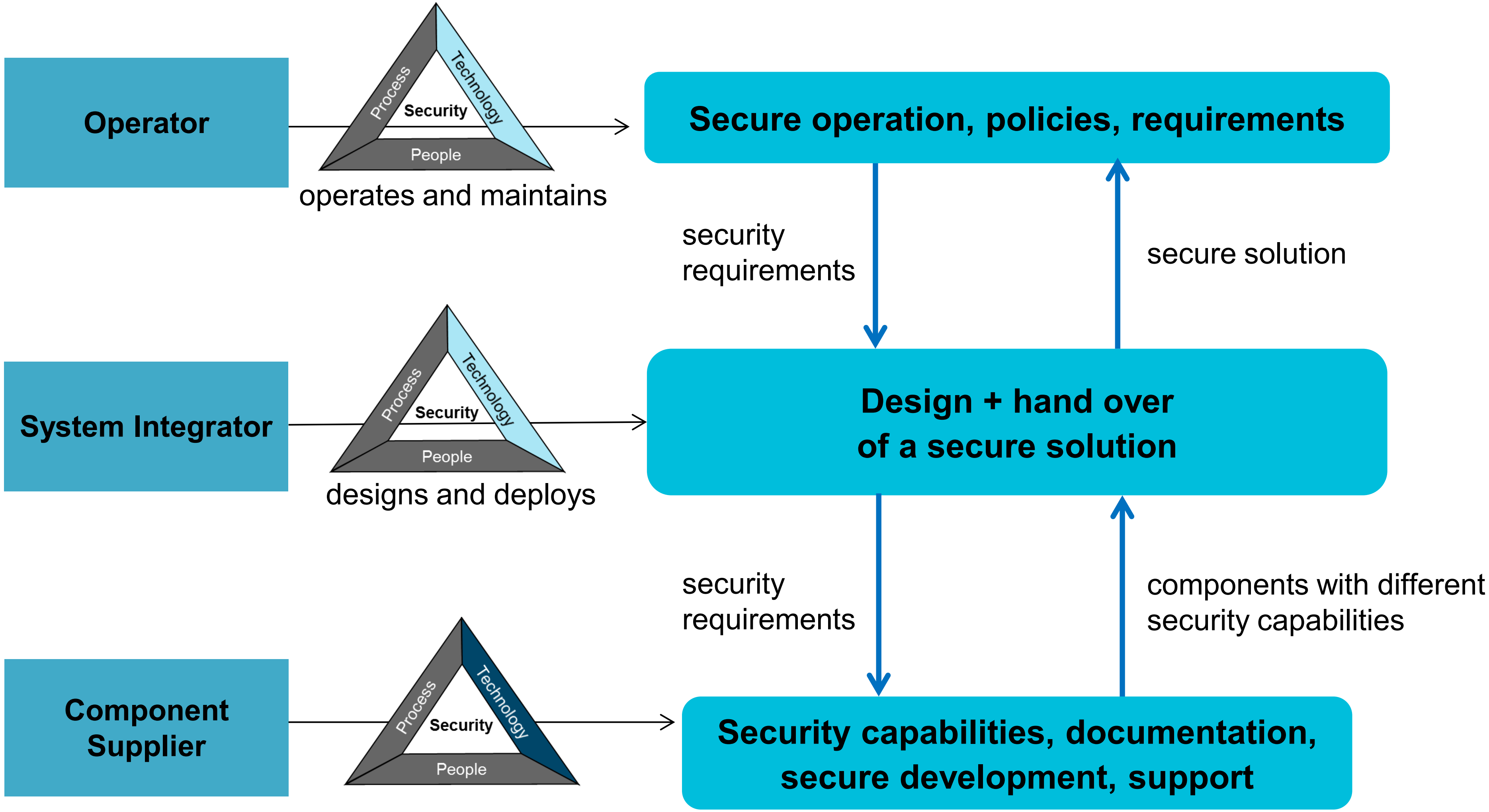


Lifetime up to 20 years and more

Office IT:
Protection of IT-Infrastructure

Lifetime 3-5 years

The industrial security standard IEC62443 addresses different roles



Operator

operates and maintains

Secure operation, policies, requirements

security requirements

secure solution

System Integrator

designs and deploys

Design + hand over of a secure solution

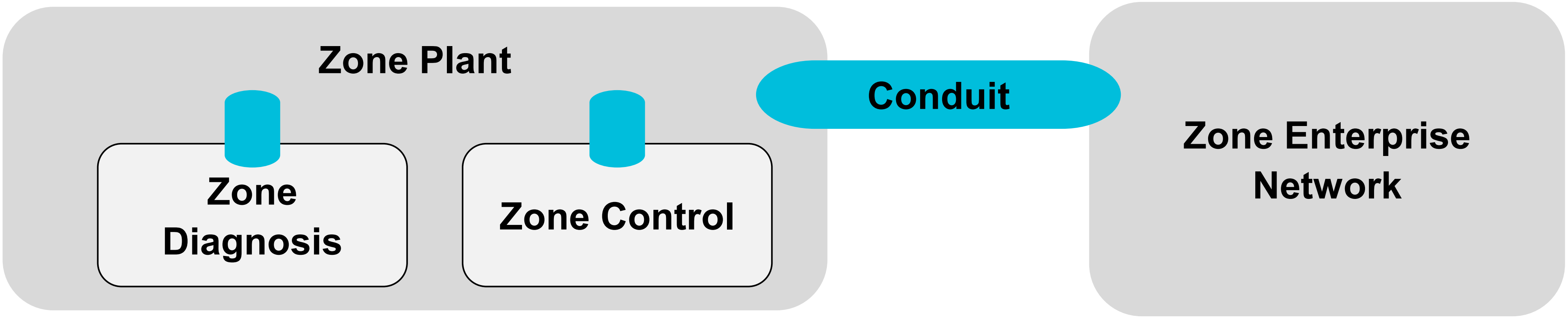
security requirements

components with different security capabilities

Component Supplier

Security capabilities, documentation, secure development, support

The security levels defined by IEC62443 provide for protection against different attack levels



SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

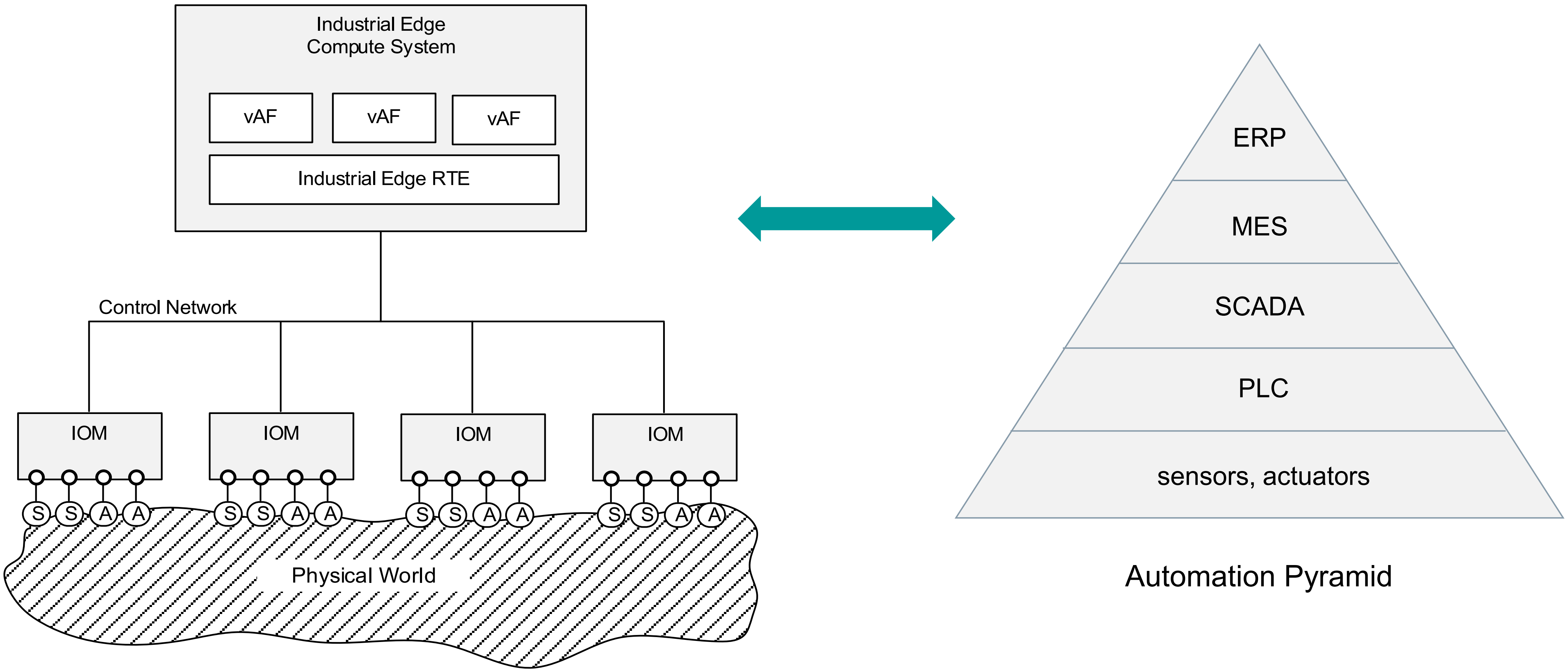
IEC 62443 – Security for Industrial Automation and Control Systems
Addresses the complete value chain from product manufacturing to operation

Targets operator, integrator, and product supplier in terms of processes and security capabilities and allows for certification

General	Policies & Procedures	System	Component / Product	Profiles	Evaluation
1-1 Terminology, concepts and models 🟧	2-1 Security program requirements for IACS asset owners ▦ 🟧	3-1 Security technologies for IACS 🟩	4-1 Secure Product Development Lifecycle Requirements 🏅 ▦ 🟩	5-x Profile x	6-1 Security Evaluation Methodology for IEC 62443-2-4 🟩
1-2 Master glossary of terms and abbreviations 🟥	2-2 IACS Security Protection ▦ 🟥	3-2 Security Risk Assessment for System Design ▨ ▦ 🟧	4-2 Technical security requirements for IACS components 🏅 ▨ 🟩		6-2 Security Evaluation Methodology for IEC 62443-4-2 🟥
1-3 Performance metrics for IACS security 🟥	2-3 Patch management in the IACS environment ▦ 🟧	3-3 System security requirements and security levels 🏅 ▨ 🟩			
1-4 IACS security lifecycle and use-cases 🟥	2-4 Security program requirements for IACS service providers 🏅 ▦ 🟧				
1-5 Scheme for IEC 62443 Cyber Security Profiles 🟩	2-5 Implementation guidance for IACS asset owners 🟥				
1-6 Application of IEC 62443 to the Industrial Internet of Things 🟥					

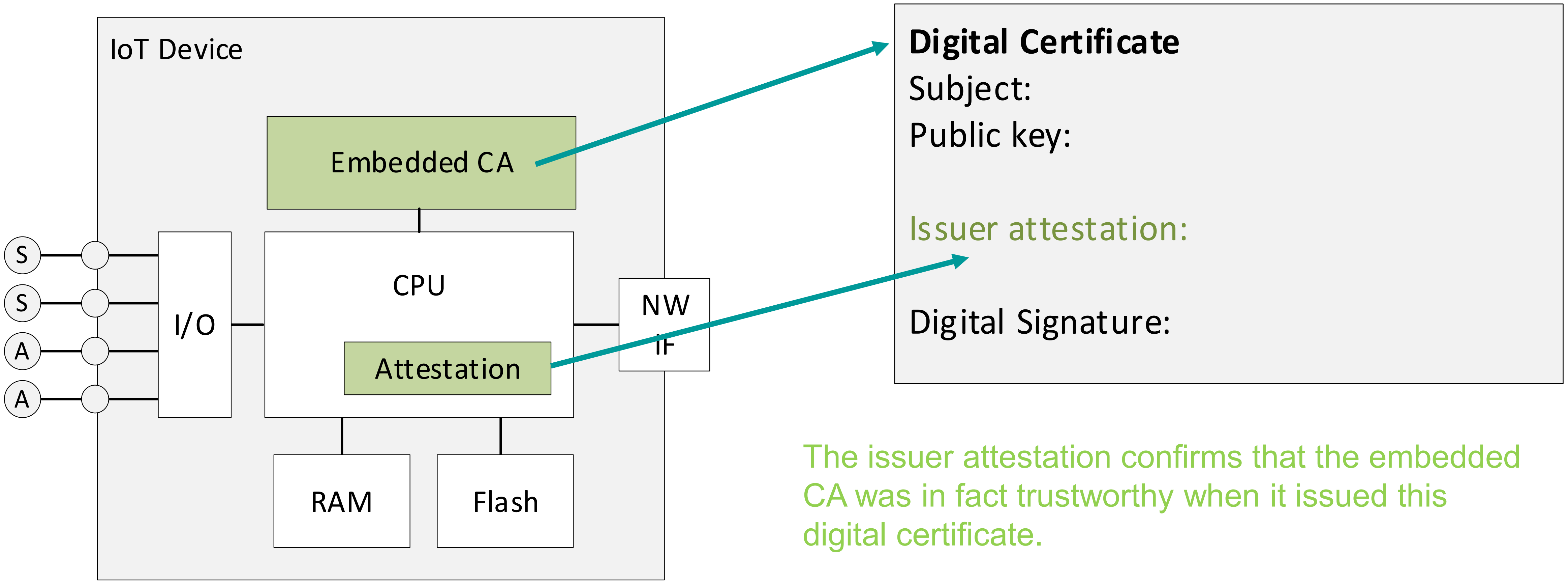
🏅 Certification relevance	🟩 Published
▨ Functional	🟧 Under revision
▦ Procedural	🟥 In development / planned

Control and monitoring of automation systems can be realized by virtualized, software-based automation functions



Automation Pyramid

Digital certificates may be issued by an embedded or local Certification Authority (CA)



Digital Certificate

Subject:

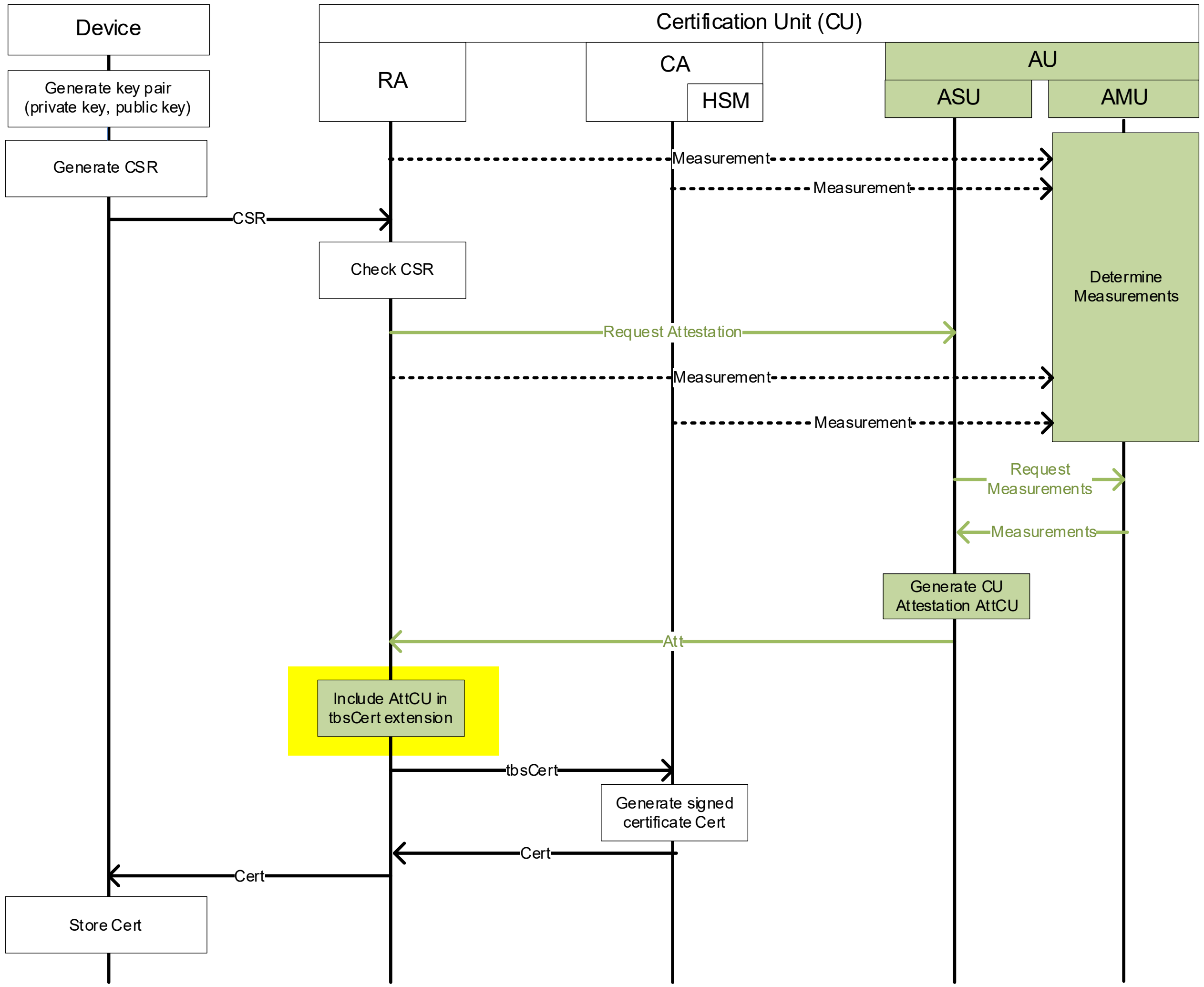
Public key:

Issuer attestation:

Digital Signature:

The issuer attestation confirms that the embedded CA was in fact trustworthy when it issued this digital certificate.

The issuer attestation is added to the digital certificate during certificate issuance



Security has to be suitable for the addressed environment.

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue.

This needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user-friendly interfaces and processes

Summary

- Cybersecurity includes preventing, detecting, and reacting to cyber-security attacks.
- Cyber resilience goes one step further and aims to maintain essential functions even during ongoing attacks, and to recover efficiently after an attack
- The basic idea of zero trust is “never trust – always verify”

- Certificates may be issued by a device not having the same protection as a classical PKI (embedded CA, local CA)
- An attestation included in a credential allows to determine whether the issuer was in fact trustworthy when it issued the credential