Enhancing Attack Resilience in the Presence of Manipulated IoT Devices within a Cyber Physical System

IARIA CYBER 2021

Dr. Rainer Falk, Steffen Fries

SIEMENS

Authors' background: Applied industrial research at Siemens Technology

Cyber Security for Industrial Systems

- Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, safety, usability).
- The industrial security standard IEC62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.

Dr. Rainer Falk
Principal Key Expert
Siemens Technology

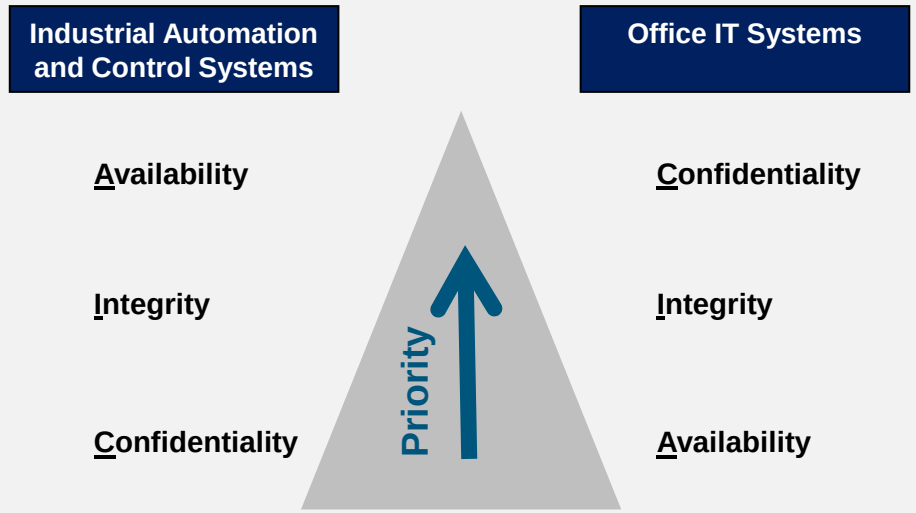
Steffen Fries
Principal Key Expert
Siemens Technology

SIEMENS

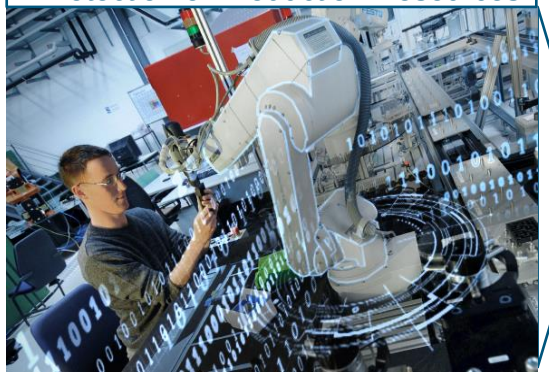
Industrial systems and rail systems require a specific approach to cybersecurity.

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 Systems :
Protection of Production Resources



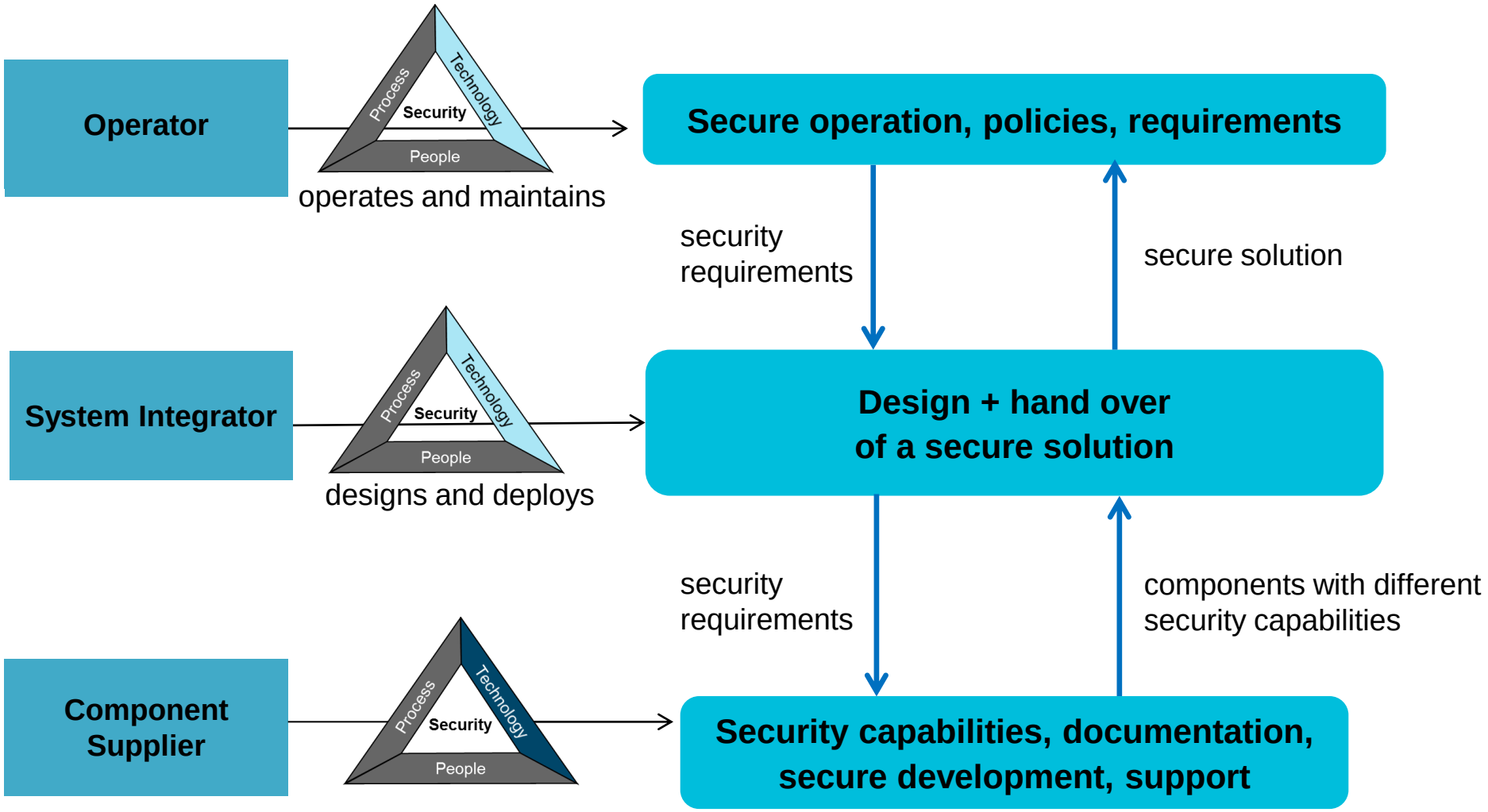
Lifetime up to 20 years and more

Office IT :
Protection of IT-Infrastructure

Lifetime 3-5 years

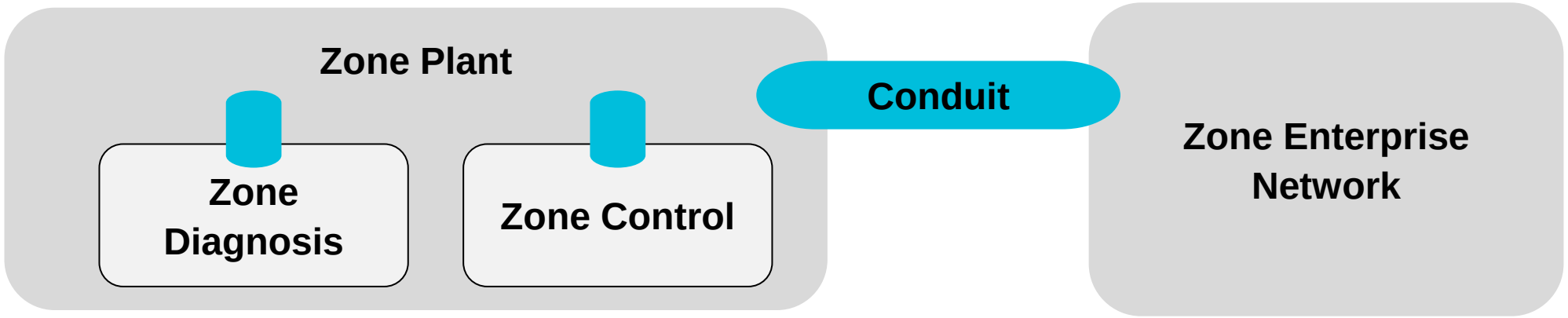
SIEMENS

The industrial security standards IEC62443 distinguishes different roles



SIEMENS

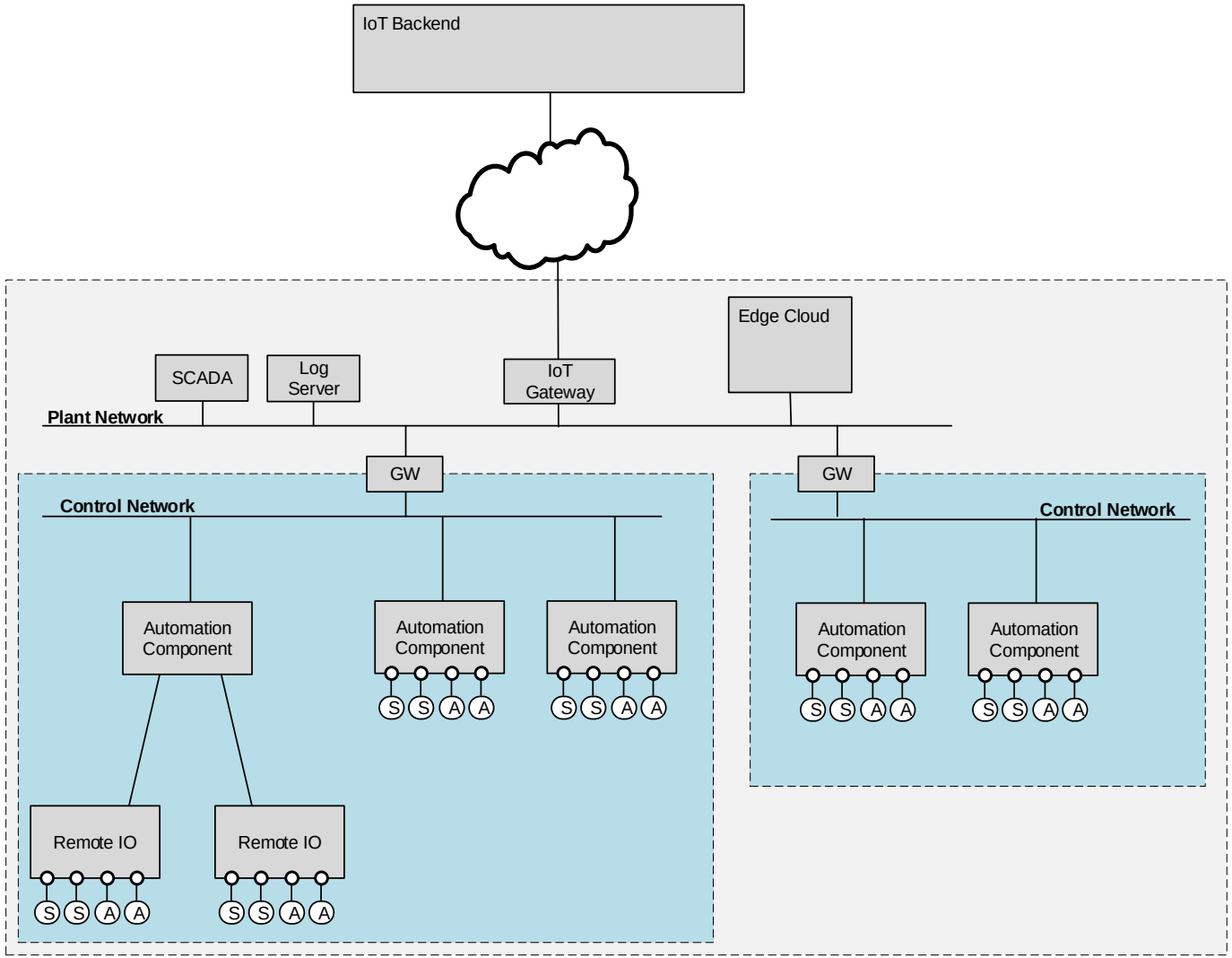
The security levels defined by IEC62443 provide for protection against different attack levels

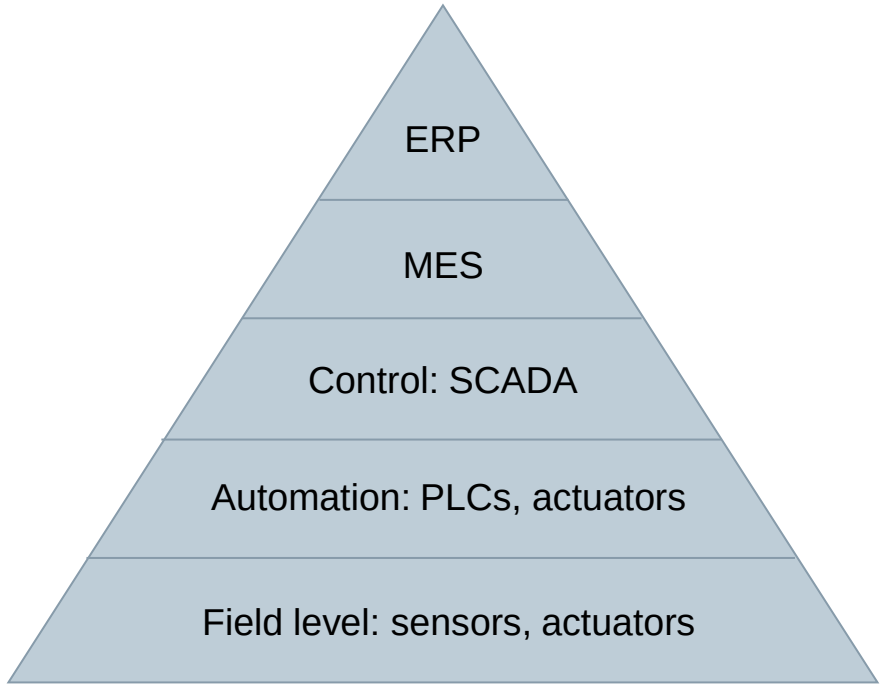


SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation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

SIEMENS

Cyber-Physical Systems: Control and monitoring functions are realized by software-based components

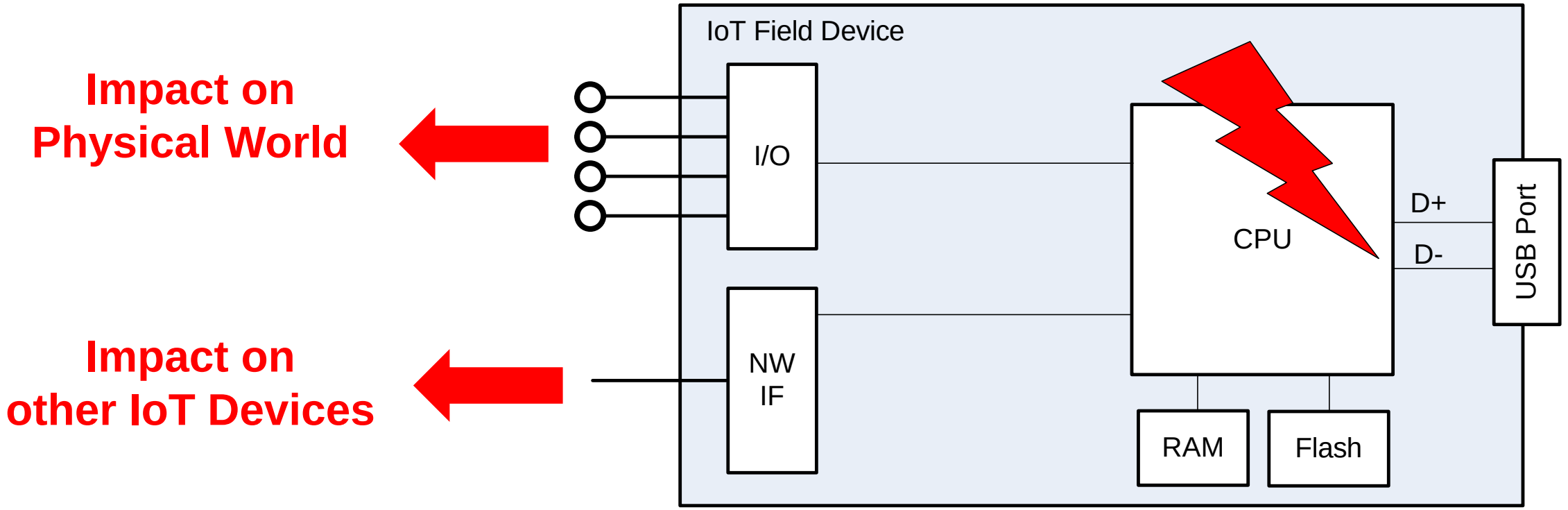




Automation Pyramid

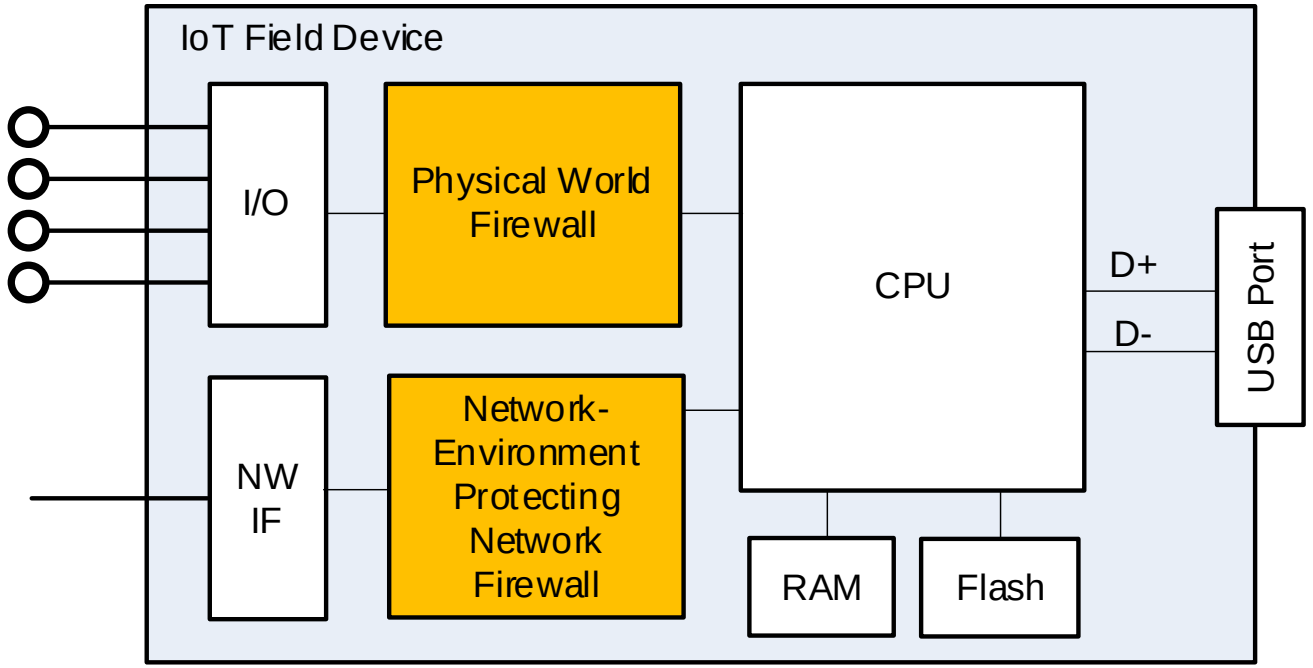
SIEMENS

It has to be considered that attackers could successfully attack and manipulate IoT devices



SIEMENS

The impact of a successful attack on an IoT device can be reduced to enhance “resilience under attack”



- Impact of successful attack on IoT device on both the network environment as well as on physical world is limited.
- Protection against using the manipulated IoT device for launching attacks on other systems

SIEMENS

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

SIEMENS