Dynamic Trust Evaluation of Evolving Cyber Physical Systems

IARIA CYBER 2022

Dr. Rainer Falk, Steffen Fries
Siemens AG, Technology

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, functional 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

Cyber security 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

1999
The globe is connected by the internet

1991
The World Wide Web becomes publicly accessible

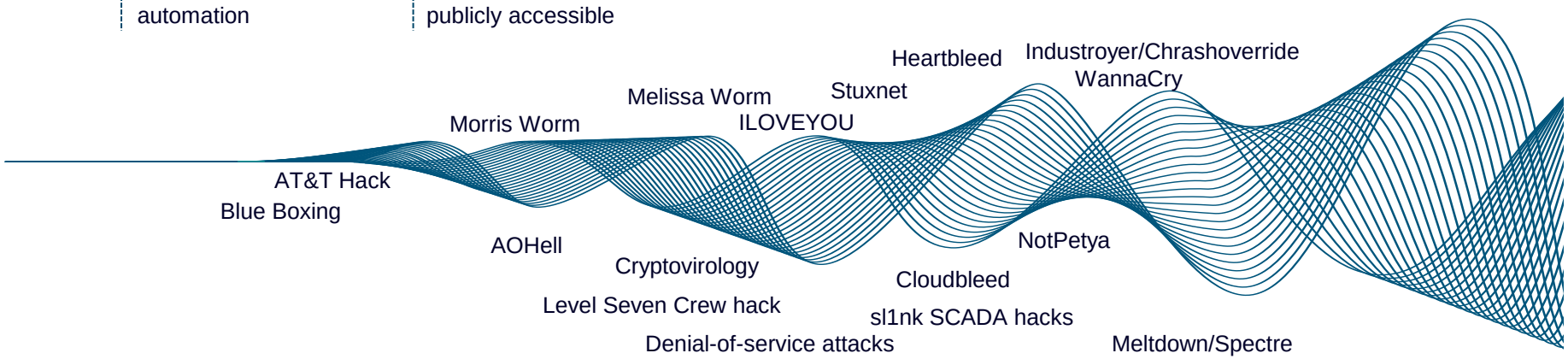
2000s
Mobile flexibility

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

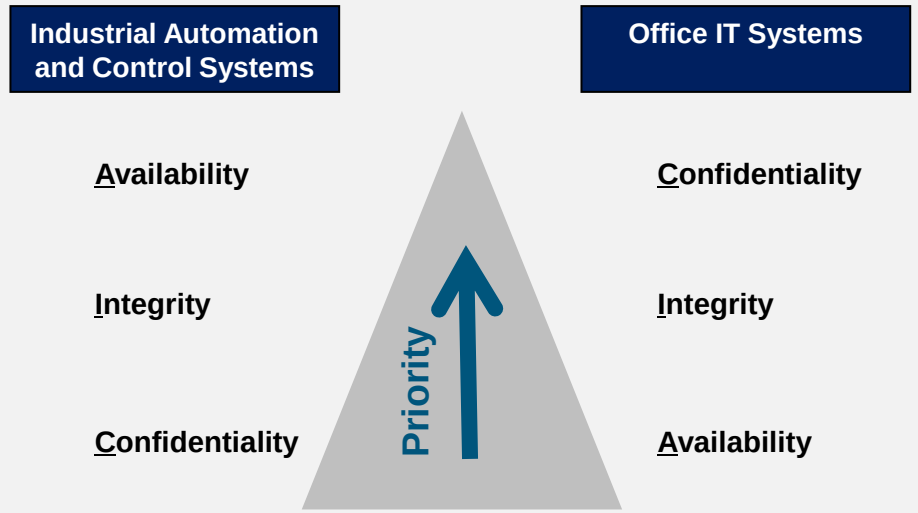


SIEMENS

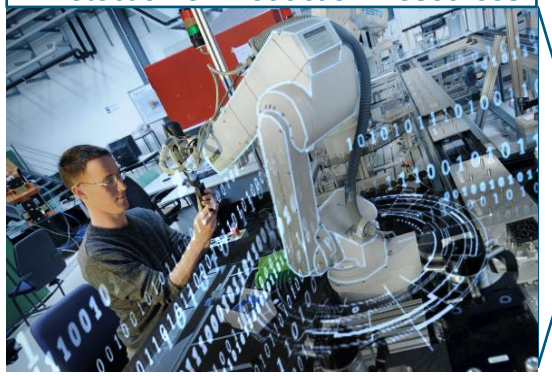
Industrial systems require a specific approach to cybersecurity

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 Systems :
Protection of Production Resources



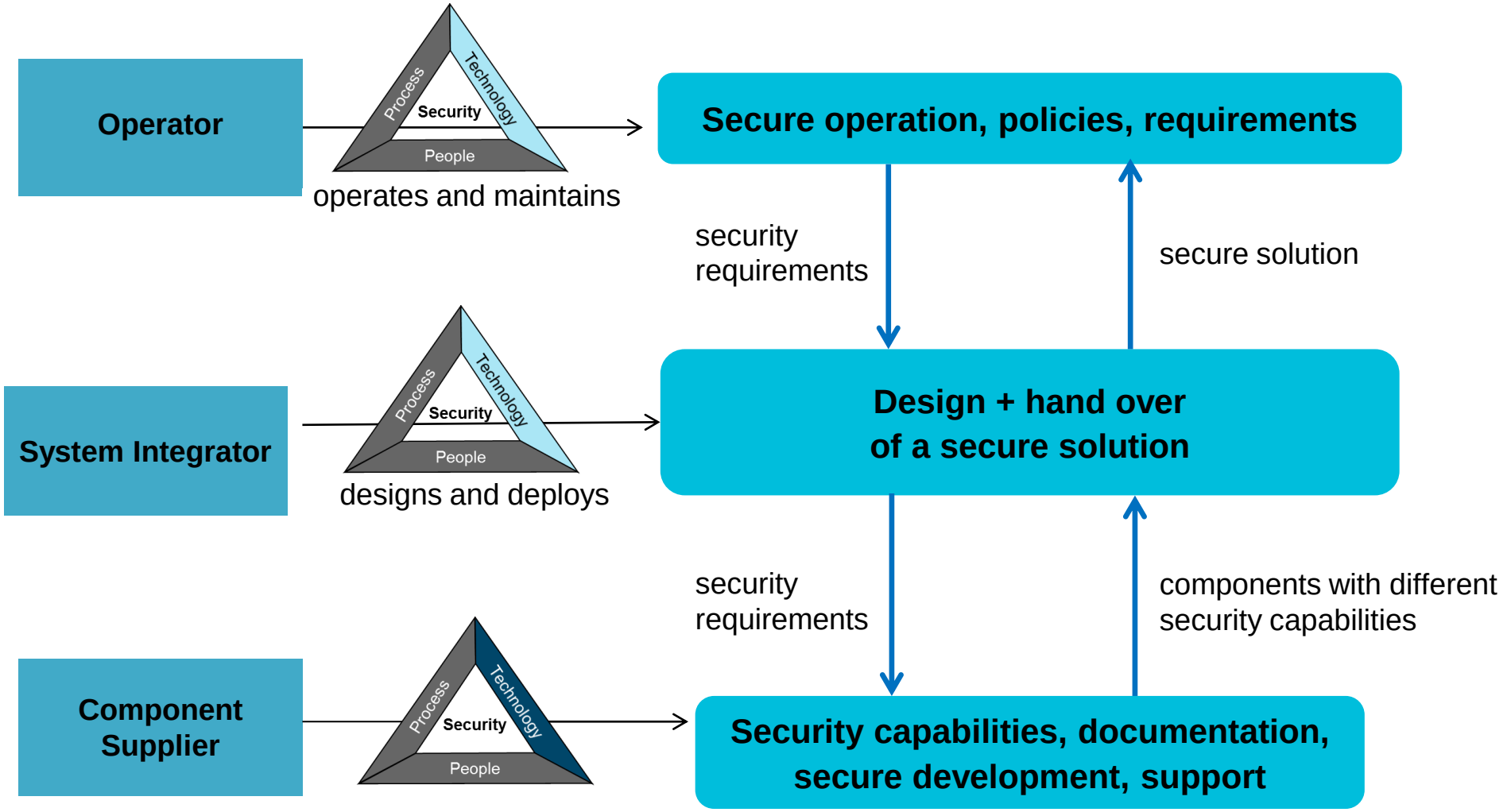
Lifetime up to 20 years and more

Office IT :
Protection of IT-Infrastructure

Lifetime 3-5 years

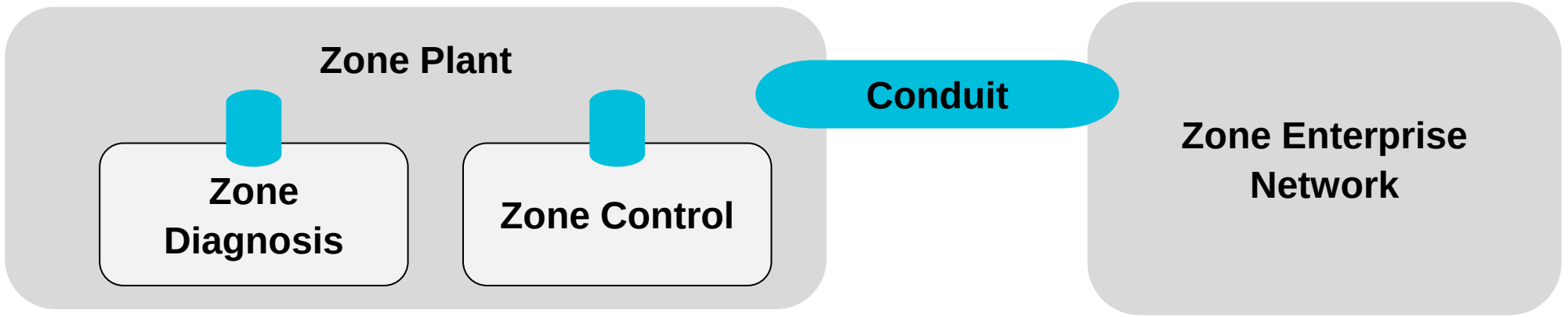
SIEMENS

The industrial security standard IEC62443 addresses different roles



SIEMENS

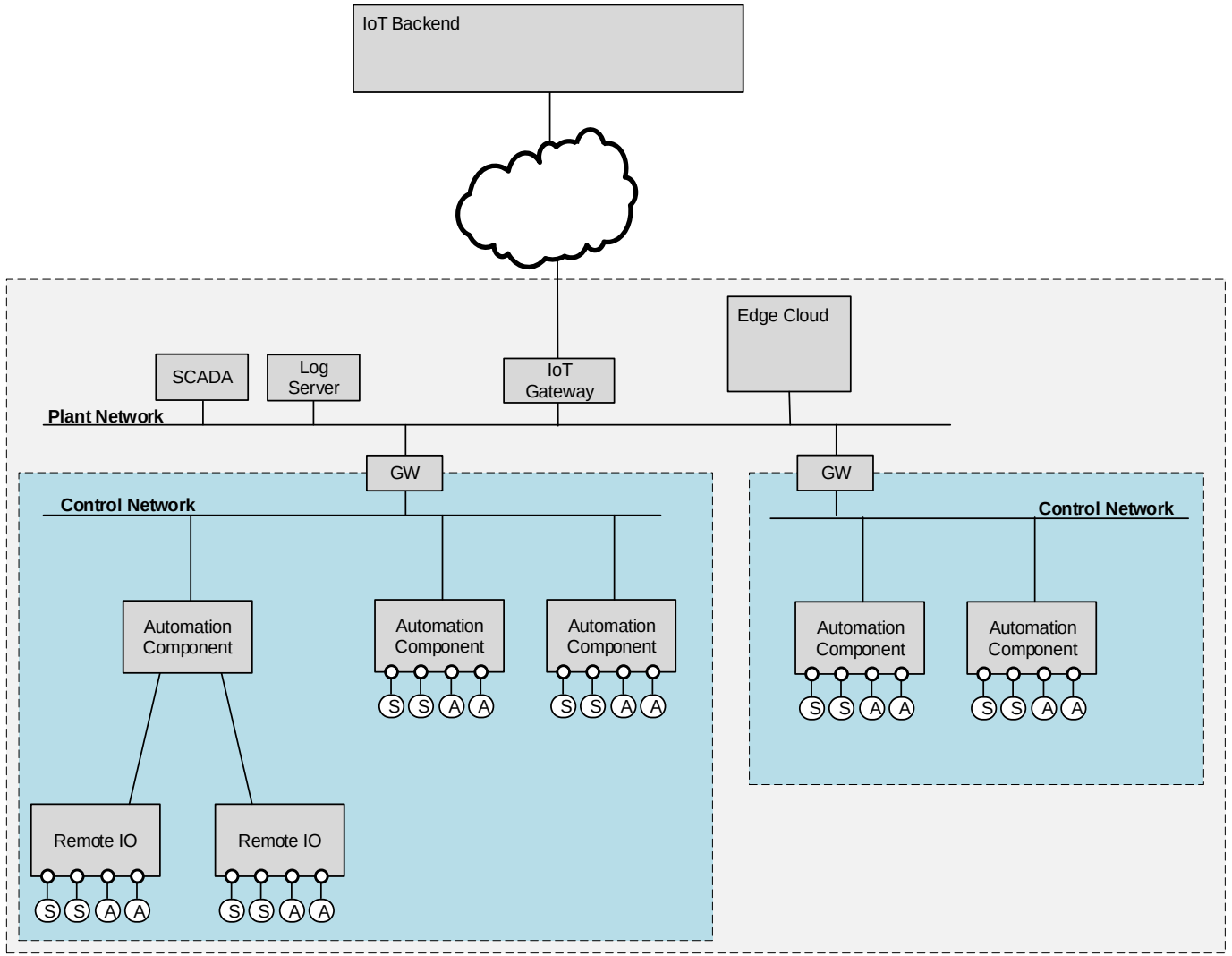
The security levels defined by IEC62443 provide for protection against different attack levels

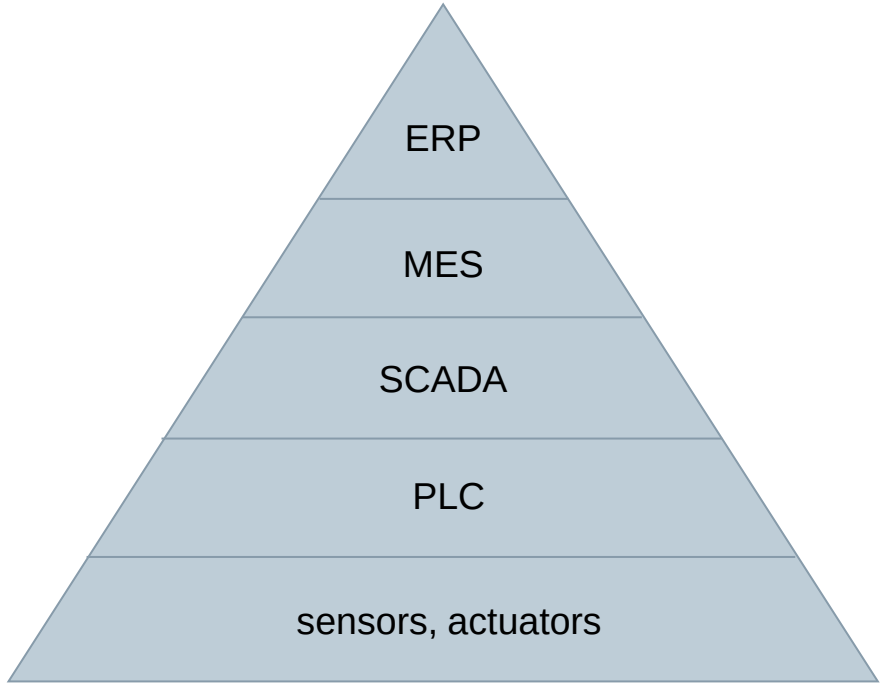


SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation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

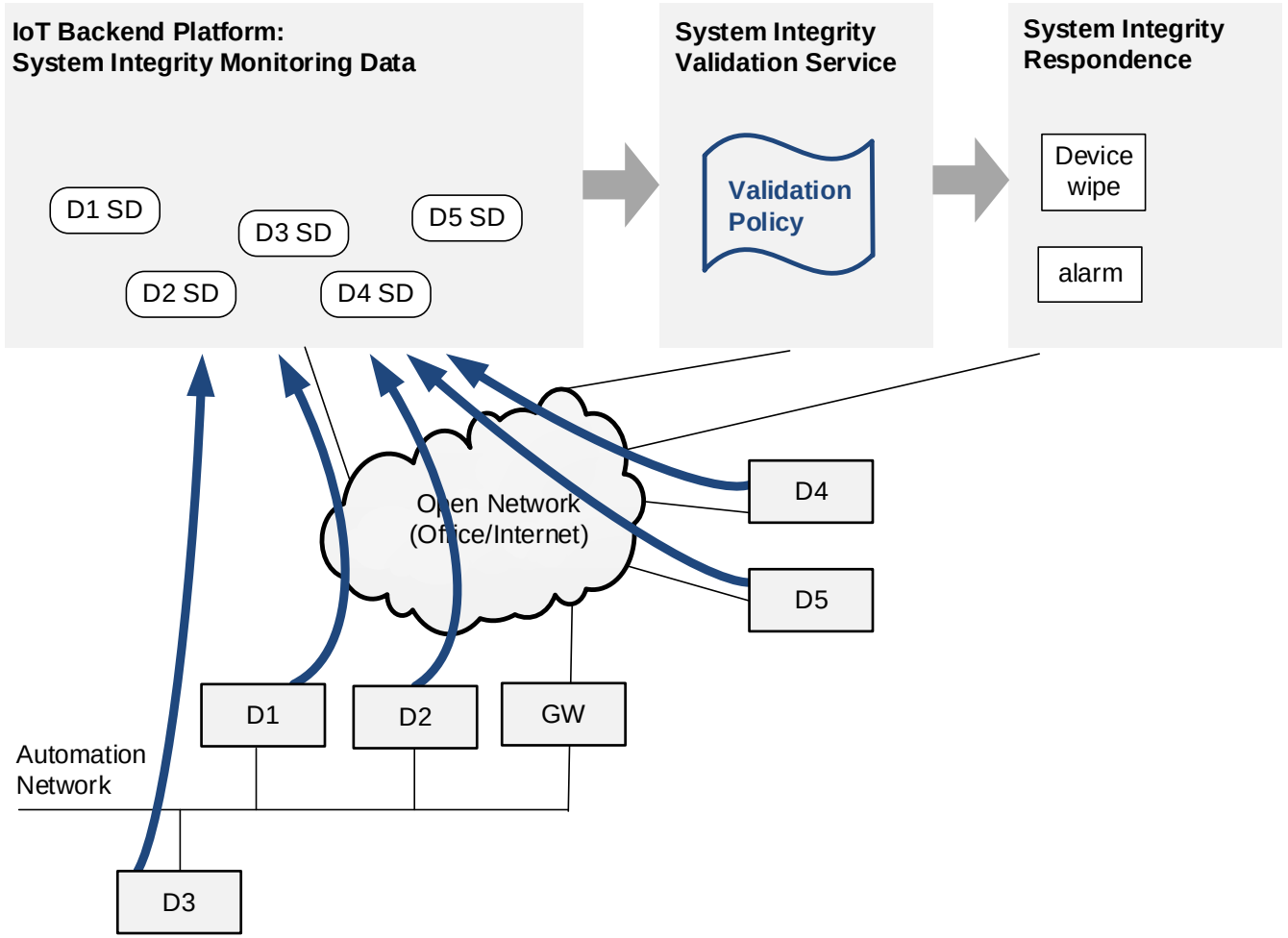




Automation Pyramid

SIEMENS

Besides secure system design and development, system integrity monitoring realizes an additional layer of defense during operation

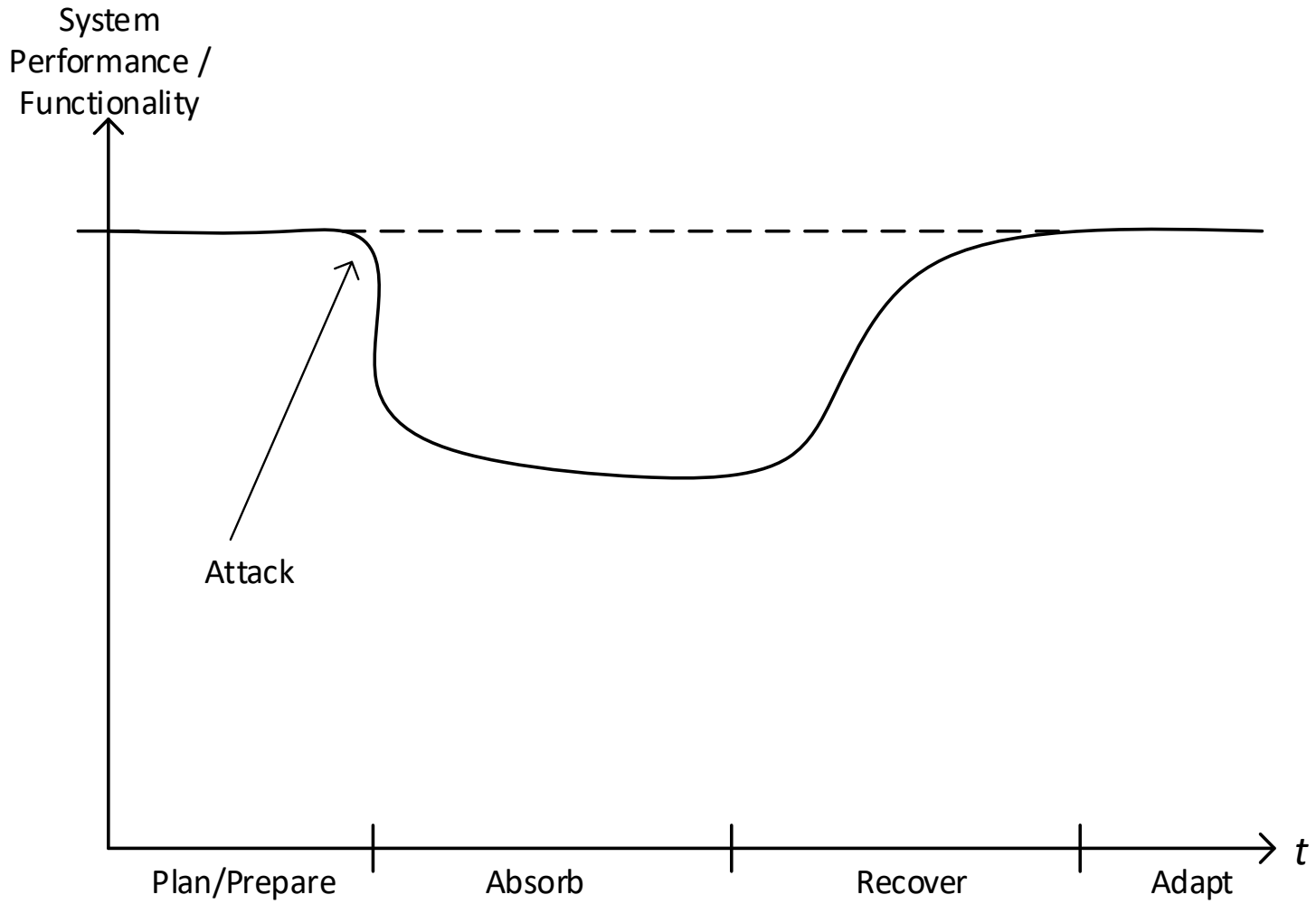


Integrated integrity monitoring of control systems and technical process:

- Device inventory
- Runtime device integrity measurements
- Network monitoring
- Physical automation process monitoring
- Power monitoring, …
- Physical world integrity (trusted sensors)

SIEMENS

Cyber resilience allows a system to stay operational even when being attacked



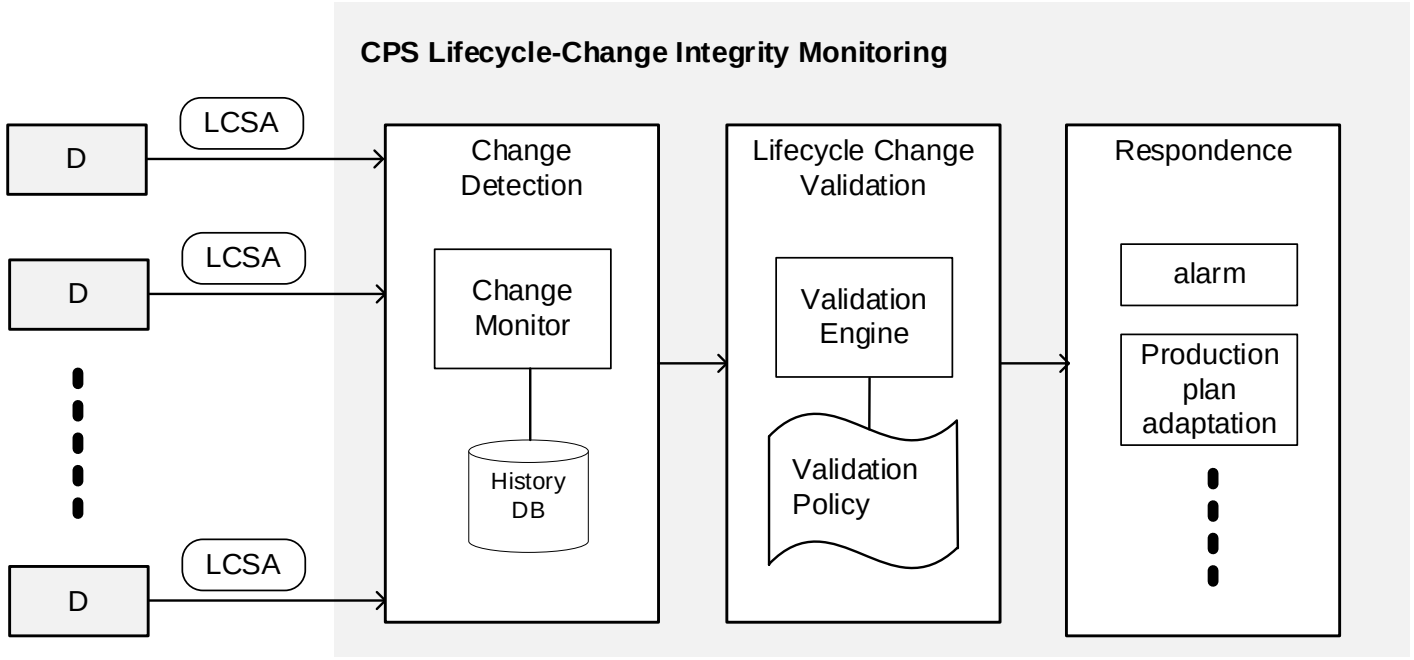
Resilience of a system is the capability

- to be resistant to a range of threats and withstand the effects of a partial loss of capability
- to recover and resume its provision of service with the minimum reasonable loss of performance

It allows the system to stay operational with a degraded performance or functionality even when it has been attacked successfully.

SIEMENS

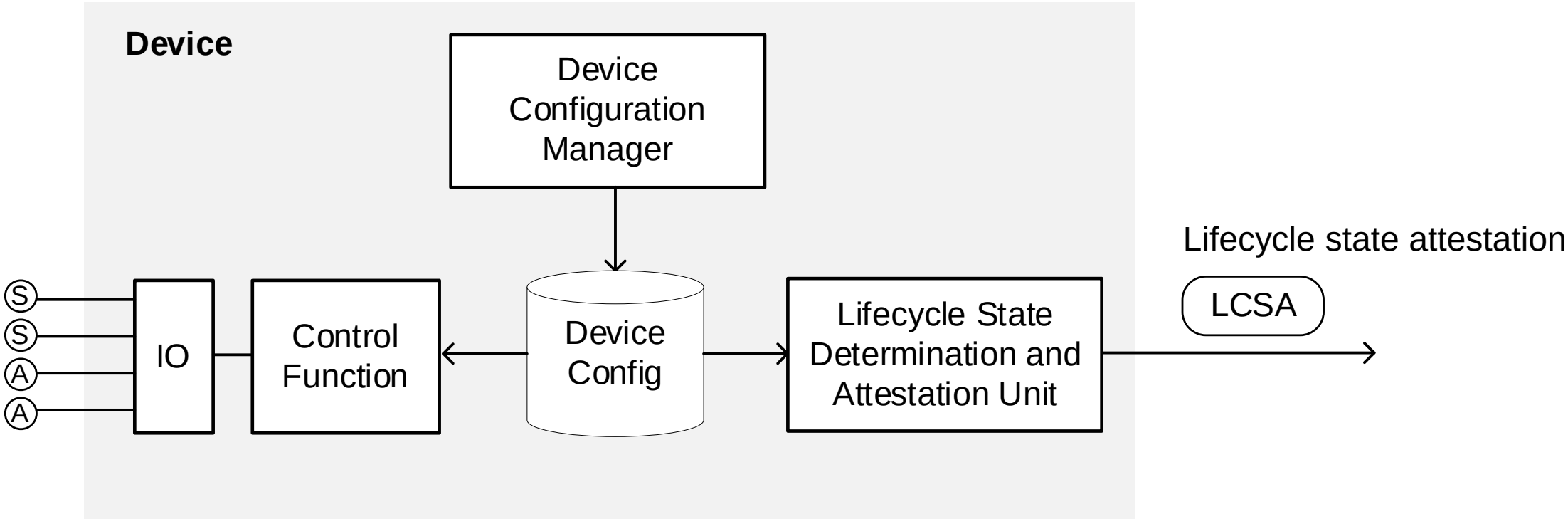
Device lifecycle integrity monitoring validates configuration changes



- Observe changes to device configuration along their lifecycle is validated. The device configuration may change on purpose during the lifecycle, which requires a monitoring regarding a dynamic configuration policy.
- An integrity violation is detected if changes are not in-line with a change authorization policy.

SIEMENS

A device can determine its own lifecycle state and confirm it reliably as lifecycle state attestation



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