

Graceful degradation under attack:

Adapting control device operation
depending on the current threat exposure

Dr. Rainer Falk, Christian Feist, Steffen Fries
Siemens AG, Technology

Authors' background: Applied industrial research at Siemens Technology

Cyber Security 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 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

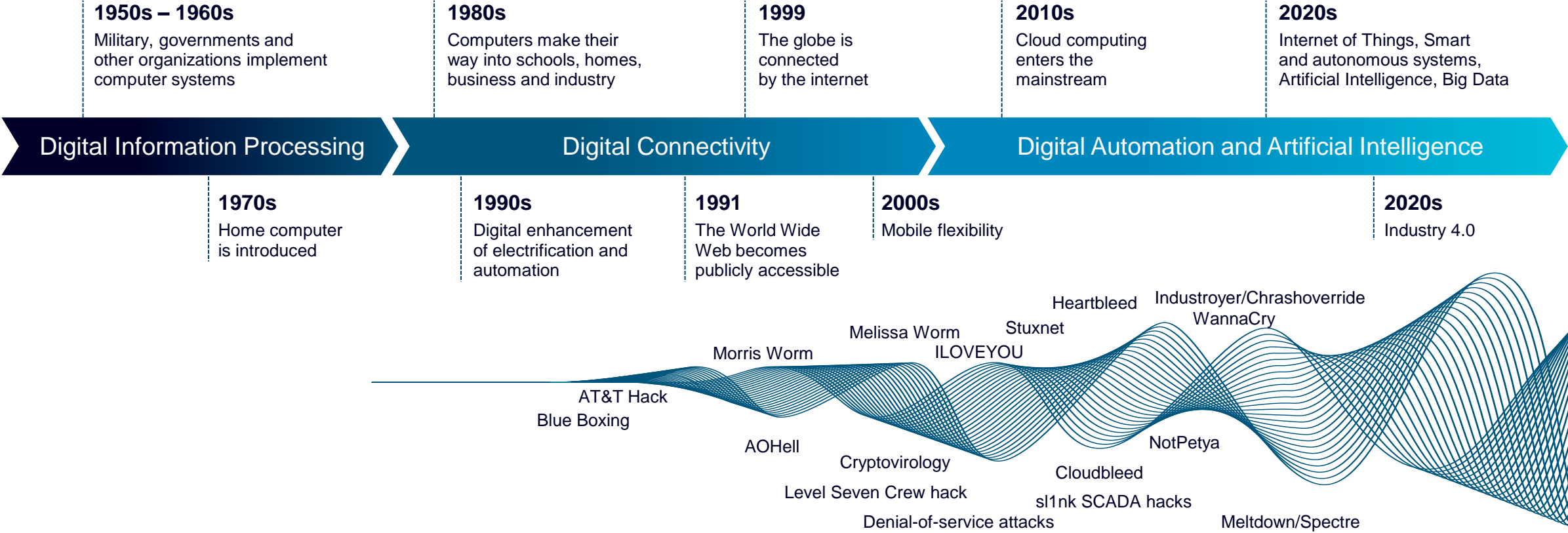


Christian Feist
Senior Key Expert
Siemens Technology



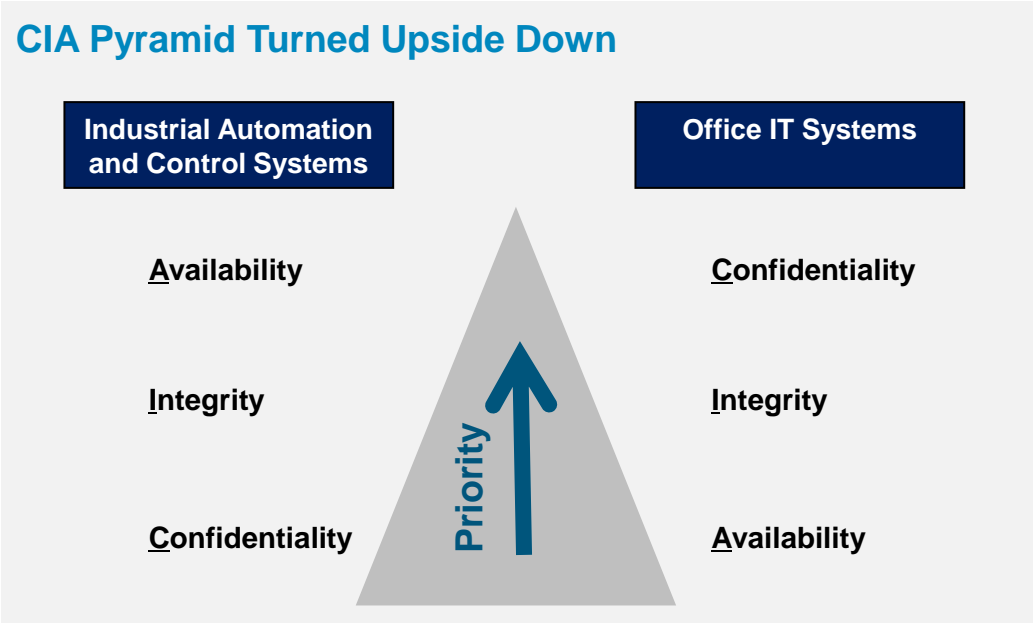
Steffen Fries
Principal Key Expert
Siemens Technology

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



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.



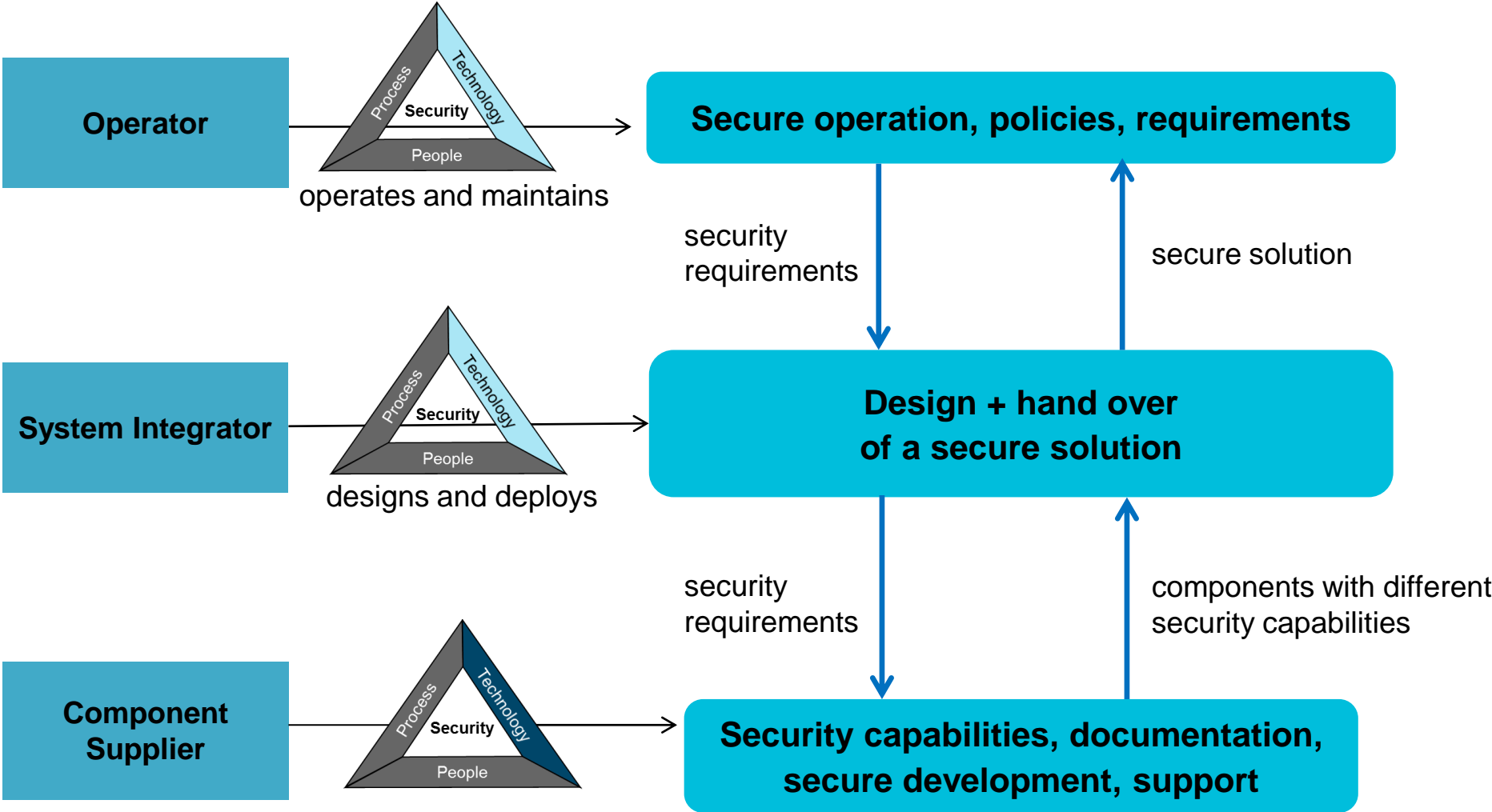
Industrial Systems:
Protection of Production Resources

Lifetime up to 20 years and more

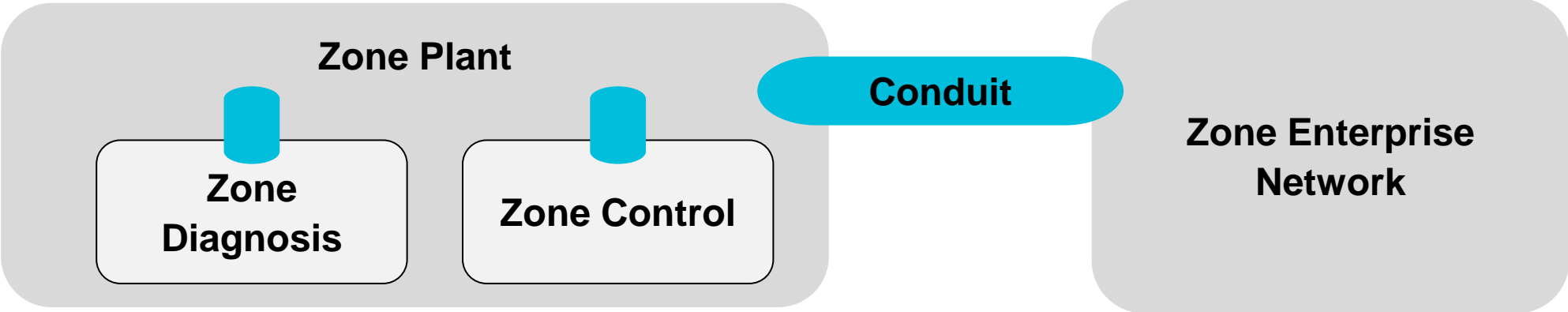
Office IT:
Protection of IT-Infrastructure

Lifetime 3-5 years

The industrial security standard IEC62443 addresses different roles



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









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

IEC 62443 – Security for Industrial Automation and Control Systems

Addresses the complete value chain from product manufacturing to operation

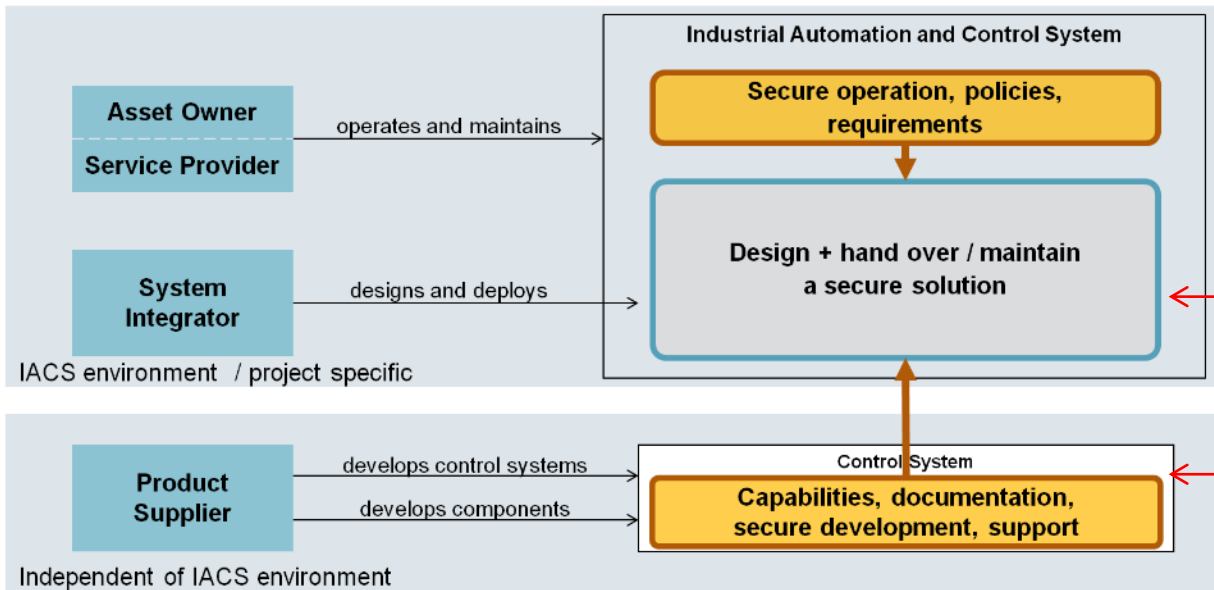
Targets operator, integrator, and product supplier in terms of processes and security capabilities and allows for certification

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										

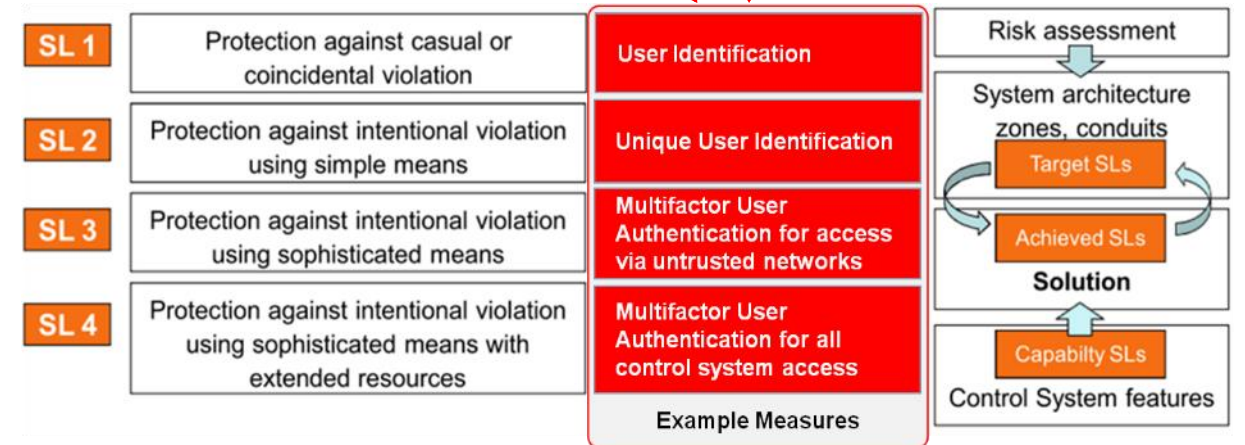
-  Certification relevance
-  Published
-  Functional
-  Under revision
-  Procedural
-  In development / planned

IEC 62443 – Security for Industrial Automation and Control Systems

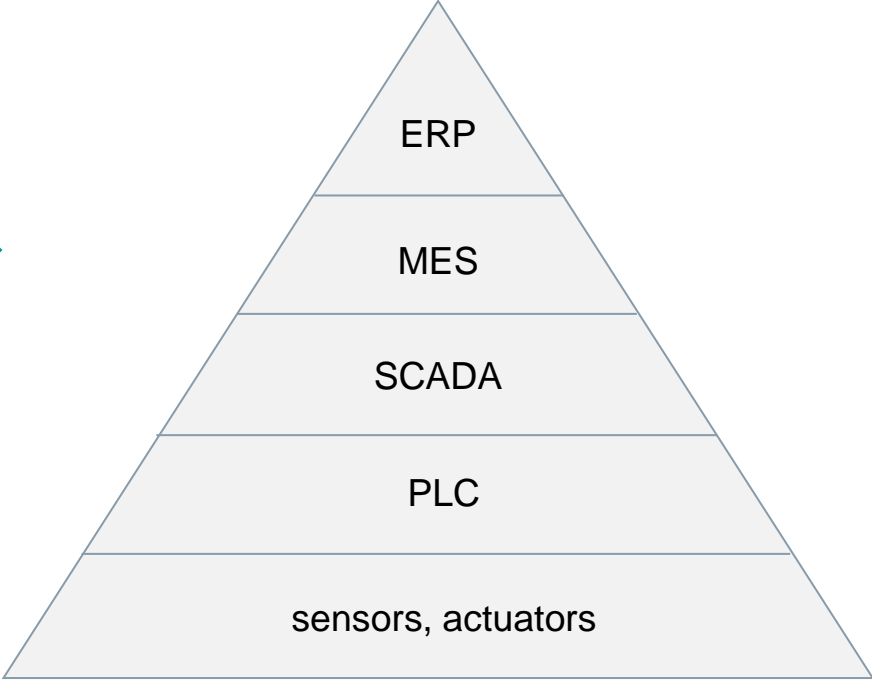
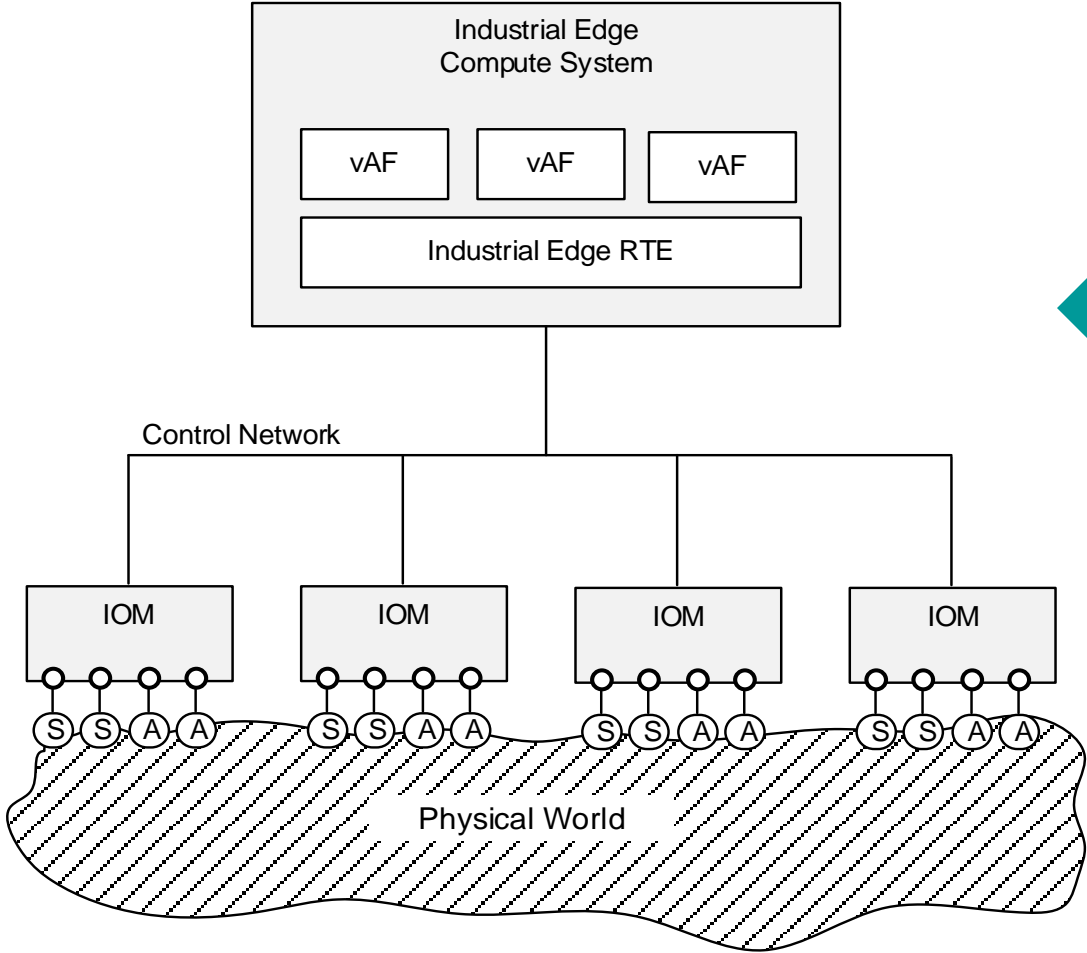
Enables a graded security approach to achieve appropriate protection



IEC 62443 Security for Industrial Automation and Control Systems					
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 Comp. Security Req.		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 Req.			
1-4 IACS security lifecycle and use-cases	2-4 Req. for IACS Service Provider				
1-5 Scheme for IEC 62443 Cyber Security Profiles	2-5 Implementation guidance for IACS asset owners				

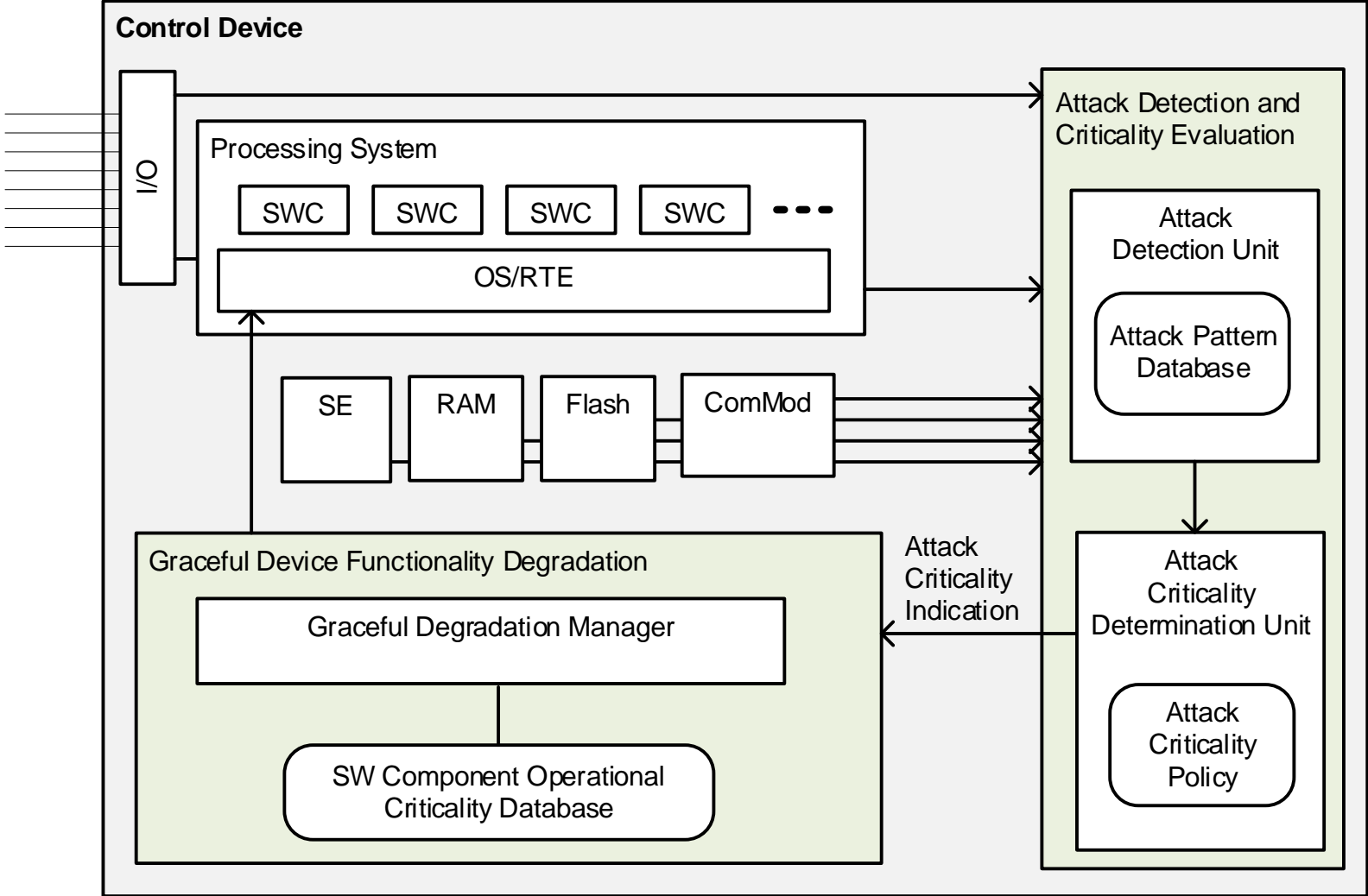


Control and monitoring of automation systems can be realized by virtualized, software-based automation functions



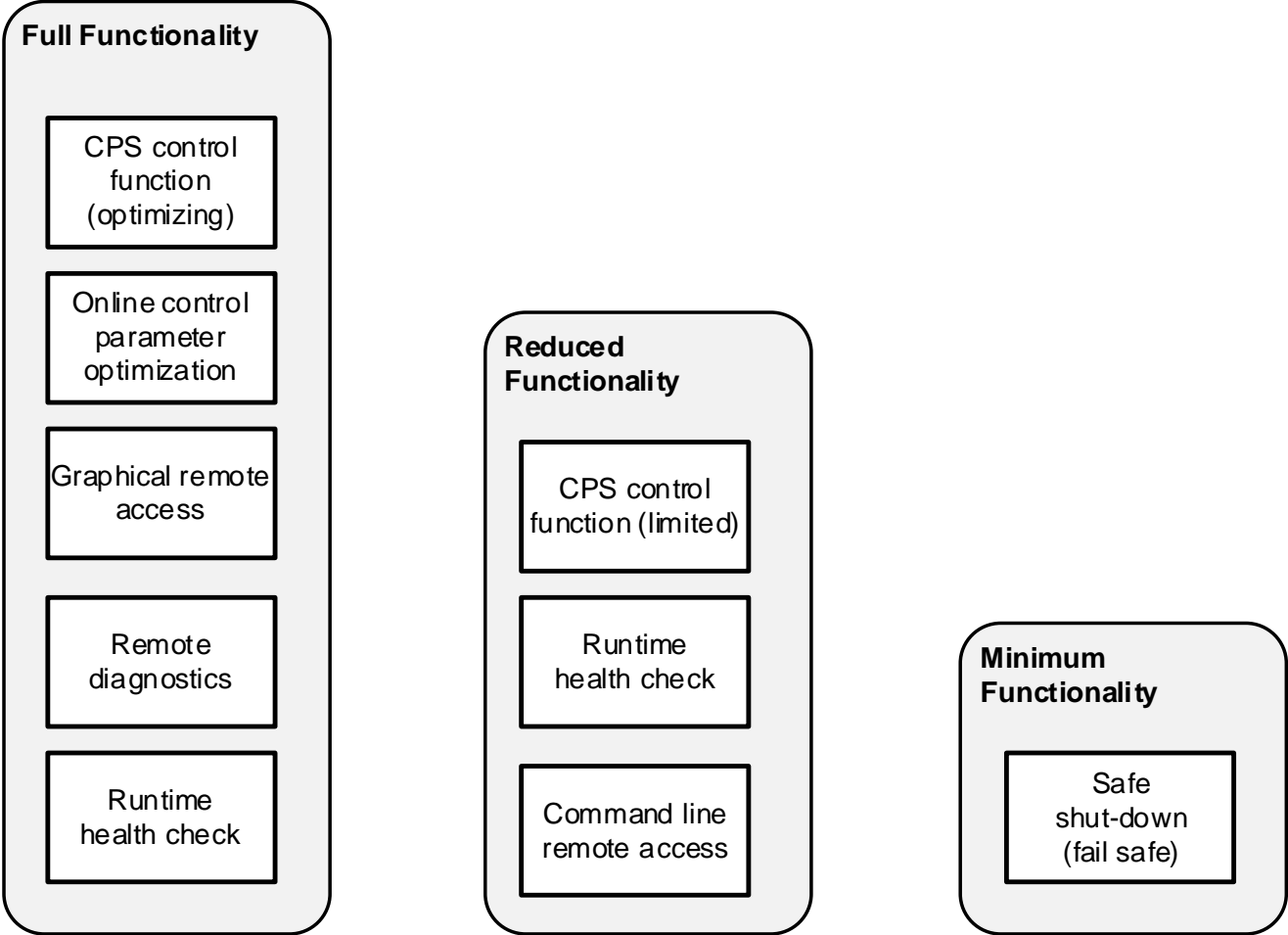
Automation Pyramid

A control device with graceful degradation under attack adapts its control function depending on the criticality of an ongoing attack

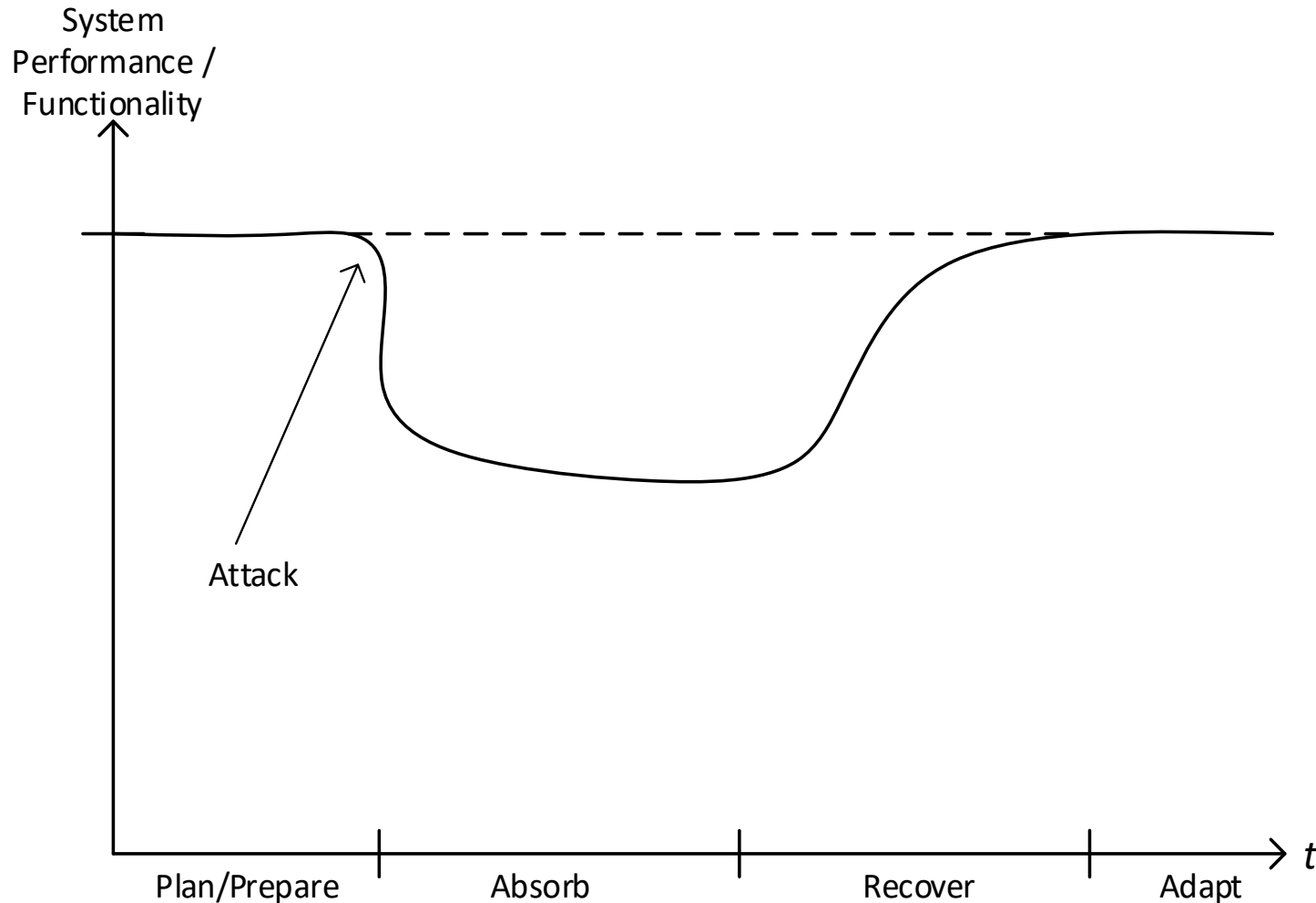


Software components have different operational criticality

The graceful degradation manager activates the software components of the respective functionality group depending on the criticality of the ongoing attack



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.

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
- Control devices of a cyber physical system can adapt to a changing threat landscape by adapting and limiting their functionality. Functionality is increasingly limited towards essential functions, thereby reducing the attack surface in risky situations, while allowing the cyber physical system to stay operational.
- The additional effort needed for implementing cyber resilience for control devices can be justified by the positive impact on CPS operation, allowing to maintain a reliable CPS operation during ongoing attacks.