Industrial Security

Driving Digitalisation for Industry

IChemE Oct 2021
Applying IEC 62443

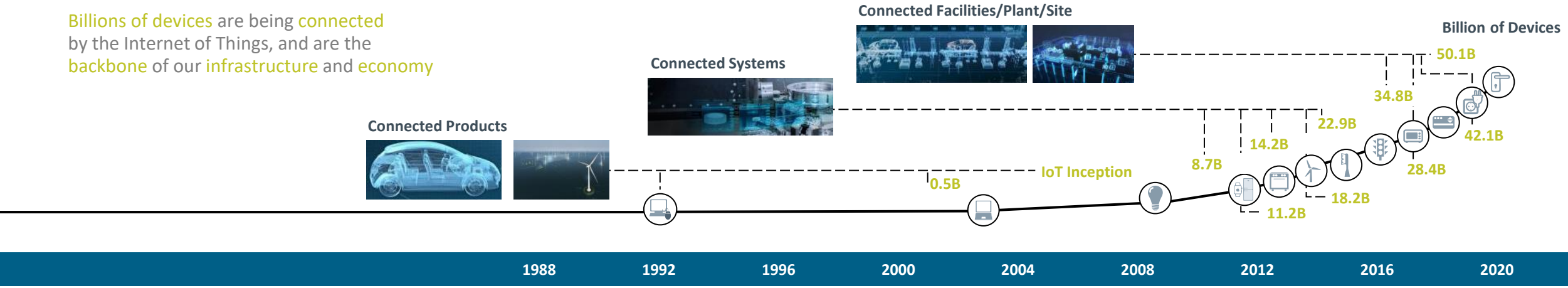
SIEMENS

Digitalization creates …

SIEMENS
Ingenuity for life

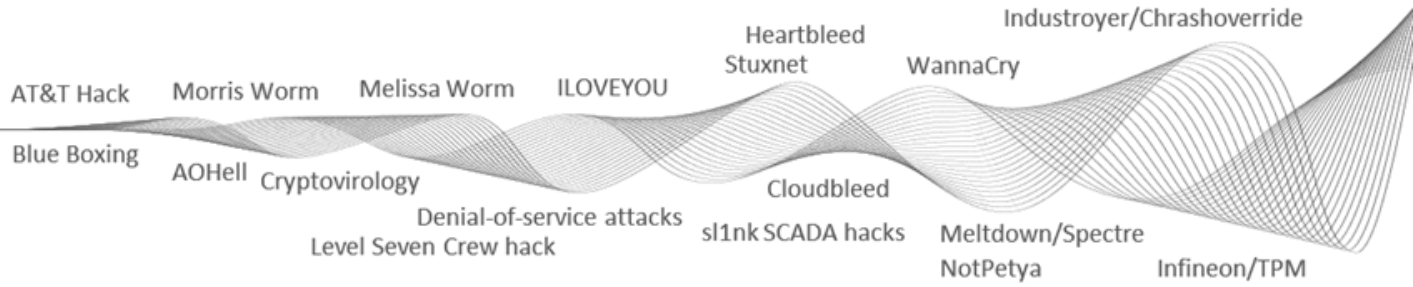
Opportunities

Billions of devices are being connected by the Internet of Things, and are the backbone of our infrastructure and economy



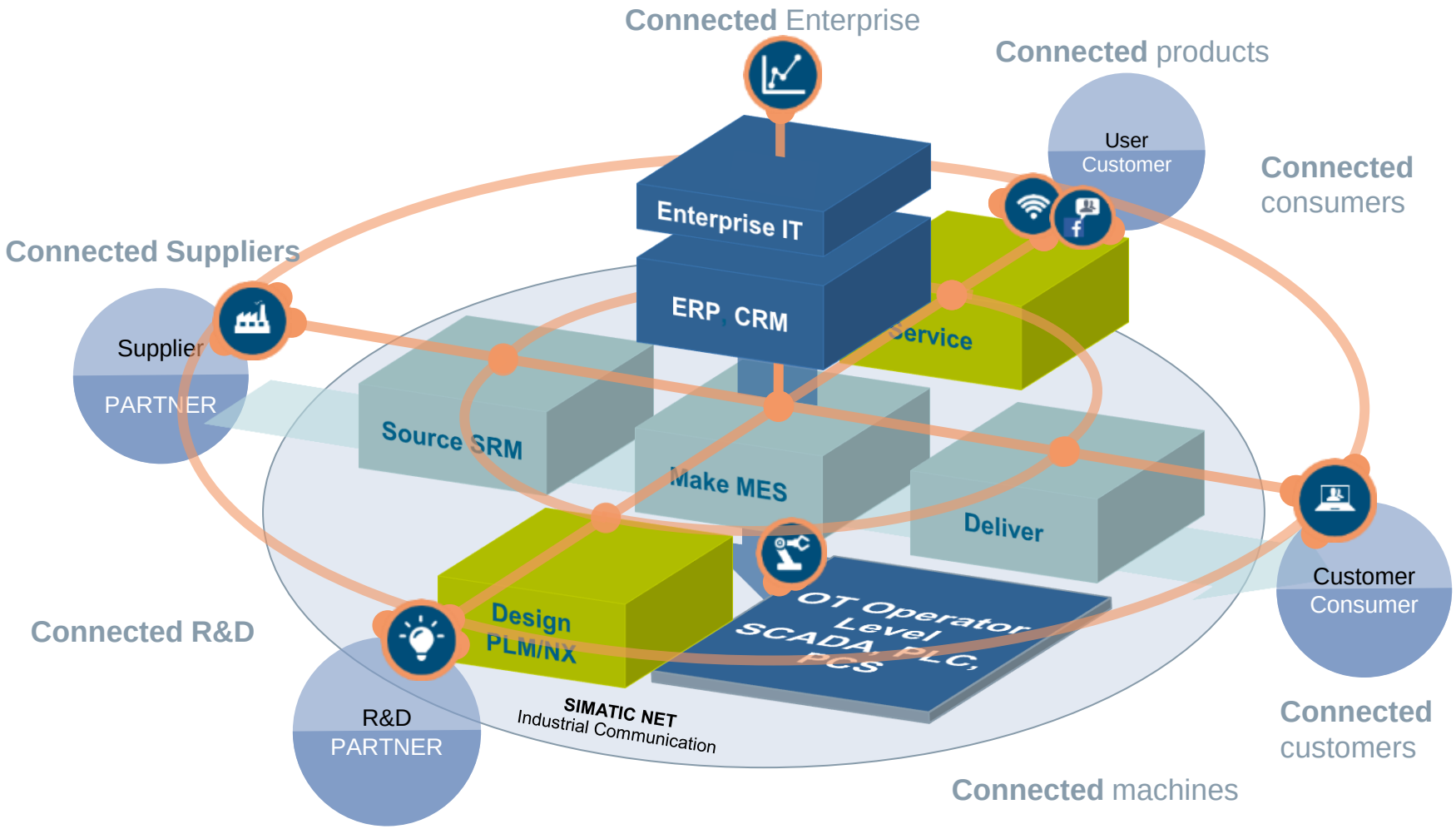
… and risks

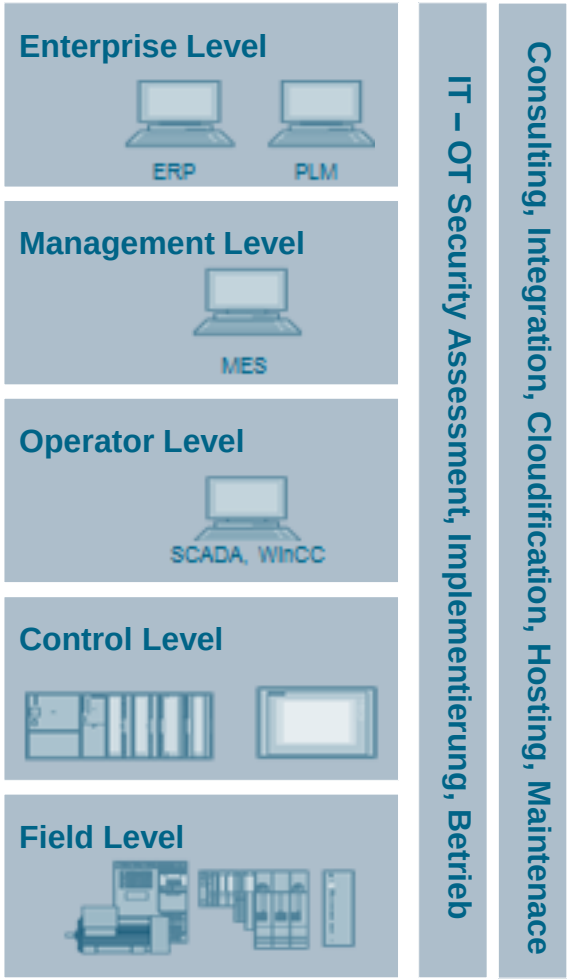
Exposure to malicious cyber attacks is also growing dramatically, putting our lives and the stability of our society at risk



IT/OT convergence supporting New Business and Collaboration Models

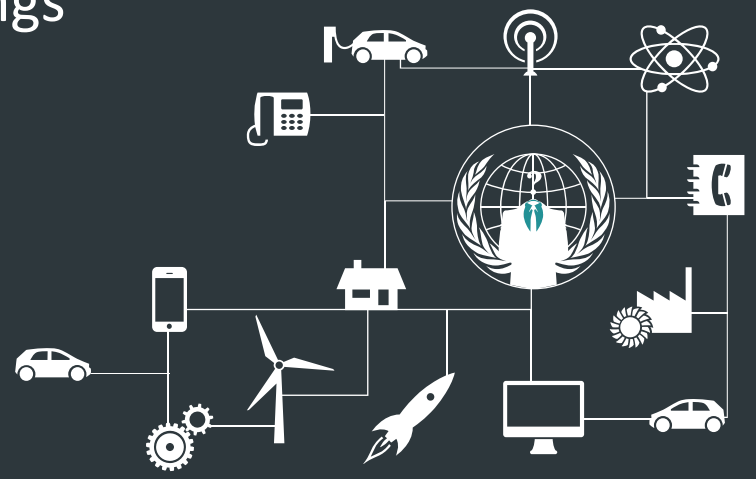
SIEMENS
Ingenuity for life





Why is Industrial Security so important?

Internet of Things



Secure

Benefits of Industry 4.0 must be ensured with industrial security

Vulnerabilities

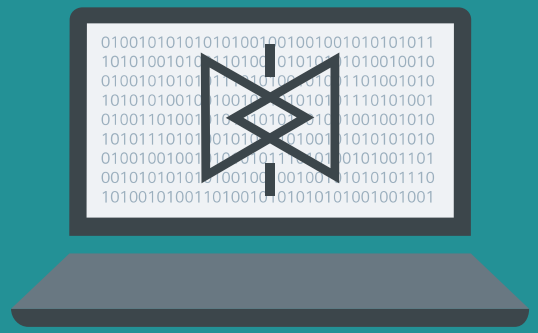
in processes and systems

Reduce

Right security measures avoid unplanned costs

Professional

Attacker



Protect from

Productivity and assets must be protected from external threats

Security integrated in

Regulations

Comply

Industry must comply security norms and regulations

Key Decisions To Be Made……

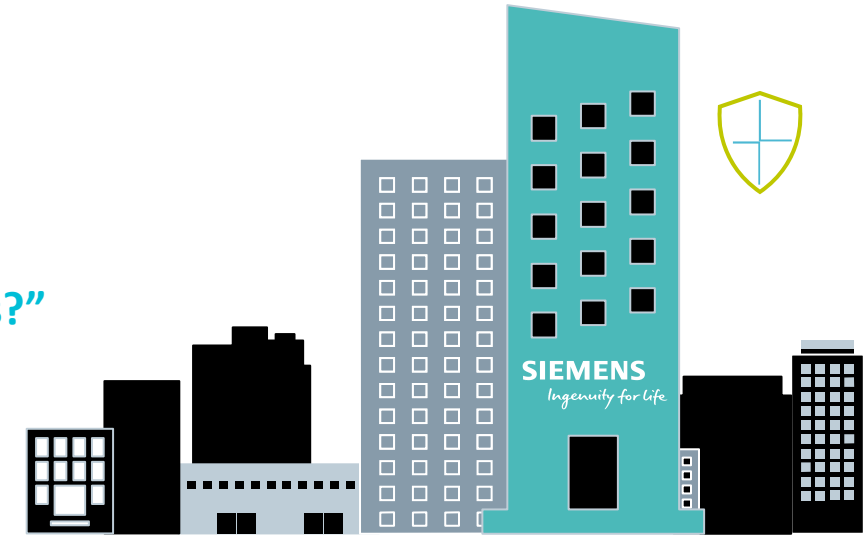
SIEMENS
Ingenuity for life

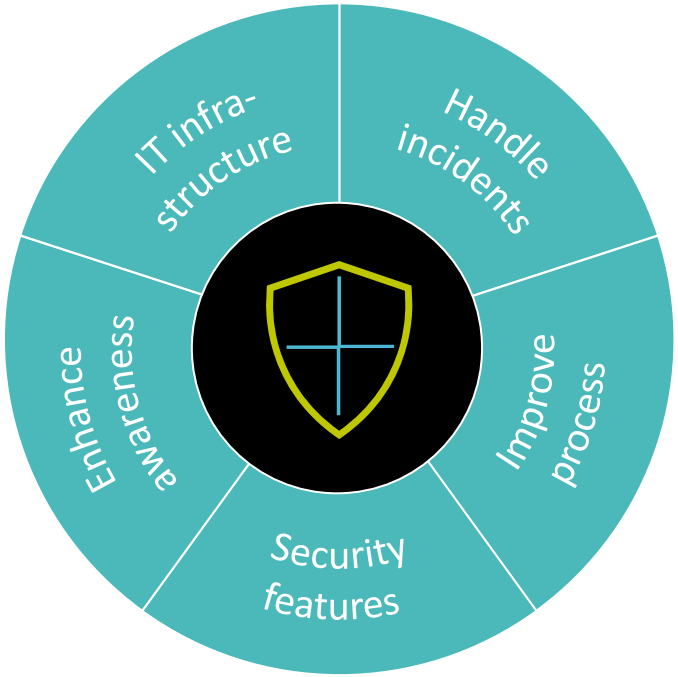
… by answering key questions and addressing five levers for security in business including IT

“What in my business do I need to protect?”

“Which level of security do I need?”

“How do I protect the specific assets?”





Industrial Security – from risk to resilience

Unprotected business

- People and assets exposed to risk
- Business vulnerable to disruptions, sabotage and theft
- Costs and liability
- Reputational damage

Secure business

- Safer and more resilient environments
- More sustainable business, resume operations faster
- Improved plant uptime to maximize profitability
- Trust with customers and shareholders

Industrial Security
protection goals & value added aspects

SIEMENS
Ingenuity for life

1 Availability

Increased plant availability through reduced interference from attacks or malware.

2 Integrity

Increased protection of system and data integrity to avoid malfunctions and production errors

3 Confidentiality

Protection of confidential data and information as well as intellectual property

Protecting productivity through risk minimization

Secure Availability, Integrity and Confidentiality at reasonable risk

Challenges are similar but reality is very different in IT and Industrial (OT) Security

SIEMENS
Ingenuity for life

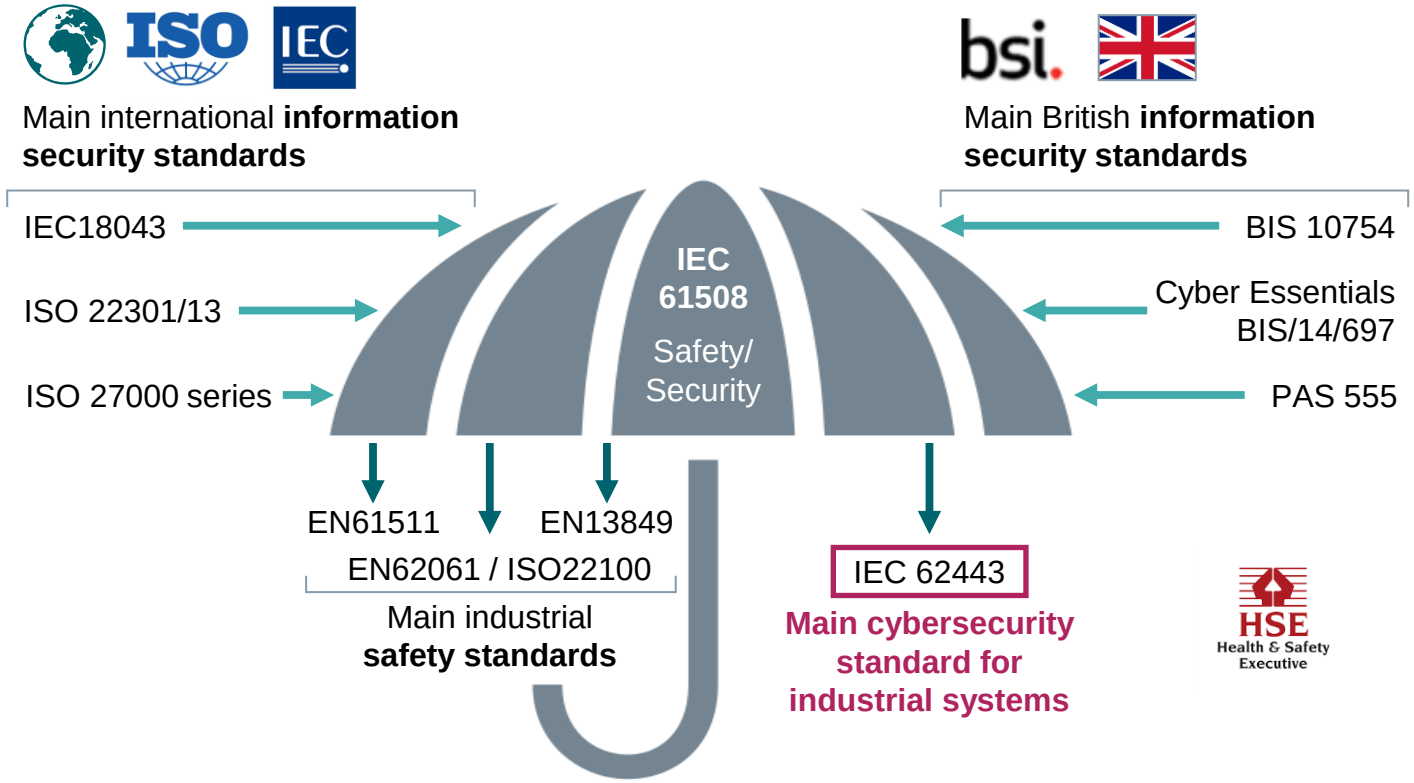
IT Security		Industrial Security
Confidentiality		**Availability and Safety**
3-5 years	**Asset lifecycle**	20-40 years
Forced migration (e.g. PCs, smart phone)	**Software lifecycle**	Usage as long as spare parts available
High (> 10 “agents” on office PCs)	**Options to add security SW**	Low (old systems w/o “free” performance)
Low (mainly Windows 10)	**Heterogeneity**	High (from Windows 95 up to 10)
Standards based (agents & forced patching)	**Main protection concept**	Case and risk based
A range in minutes is acceptable	**Availability**	Latency for control systems <300ms

The merging of national and international safety and security standards under one umbrella will broaden scope of application

SIEMENS
Ingenuity for life

Cybersecurity standards landscape and evolution

Main information security and safety standards are merging under a broader "Safety and Security" standard ...



The market is changing based on demand for the combination of both Safety and Security Services.

Increased demand for joint security and safety audits, trainings and services, as standards initially developed for CNIs[1)] are increasingly used by traditional industrial players and standards merge

Merging and alignment of standards could see a need for upskilling of engineering personnel in order to accommodate both Safety and Security in the project design phase.

1) Critical National Infrastructure

Opportunity Risk

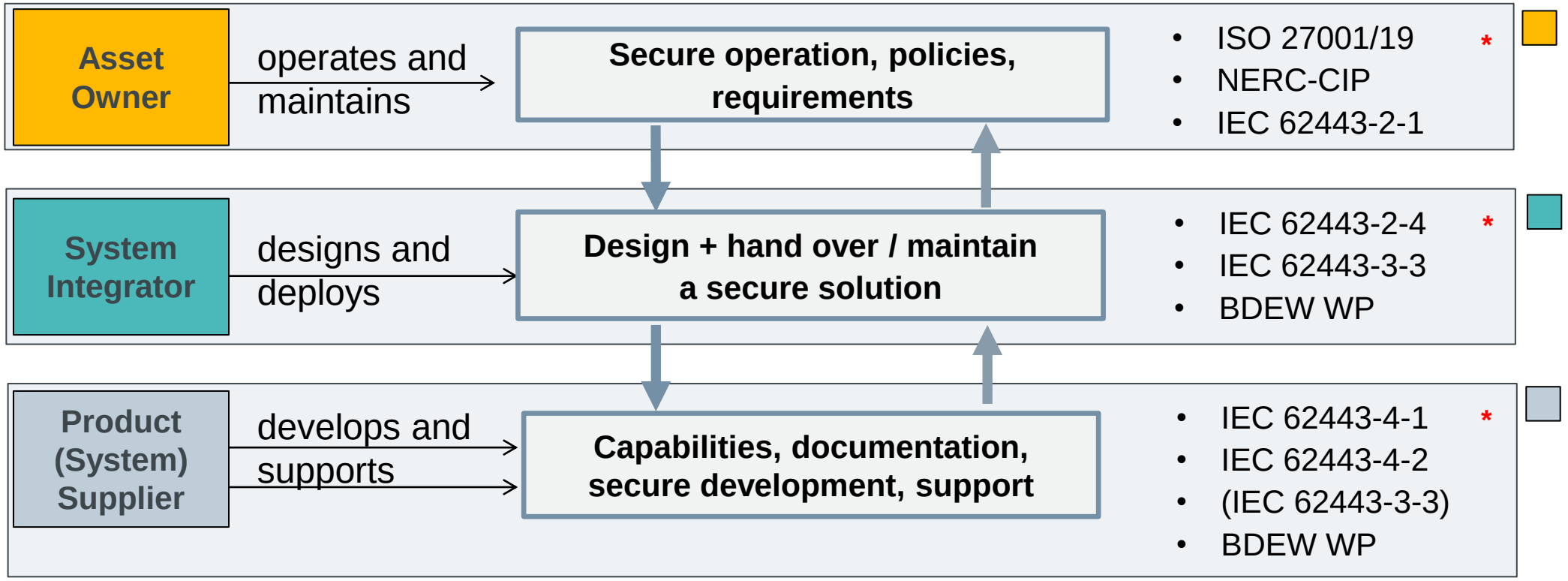
SIEMENS
Ingenuity for life

Applying IEC62443

We as SIEMENS need the capability to design, hand over and maintain secure products and solutions for our customer

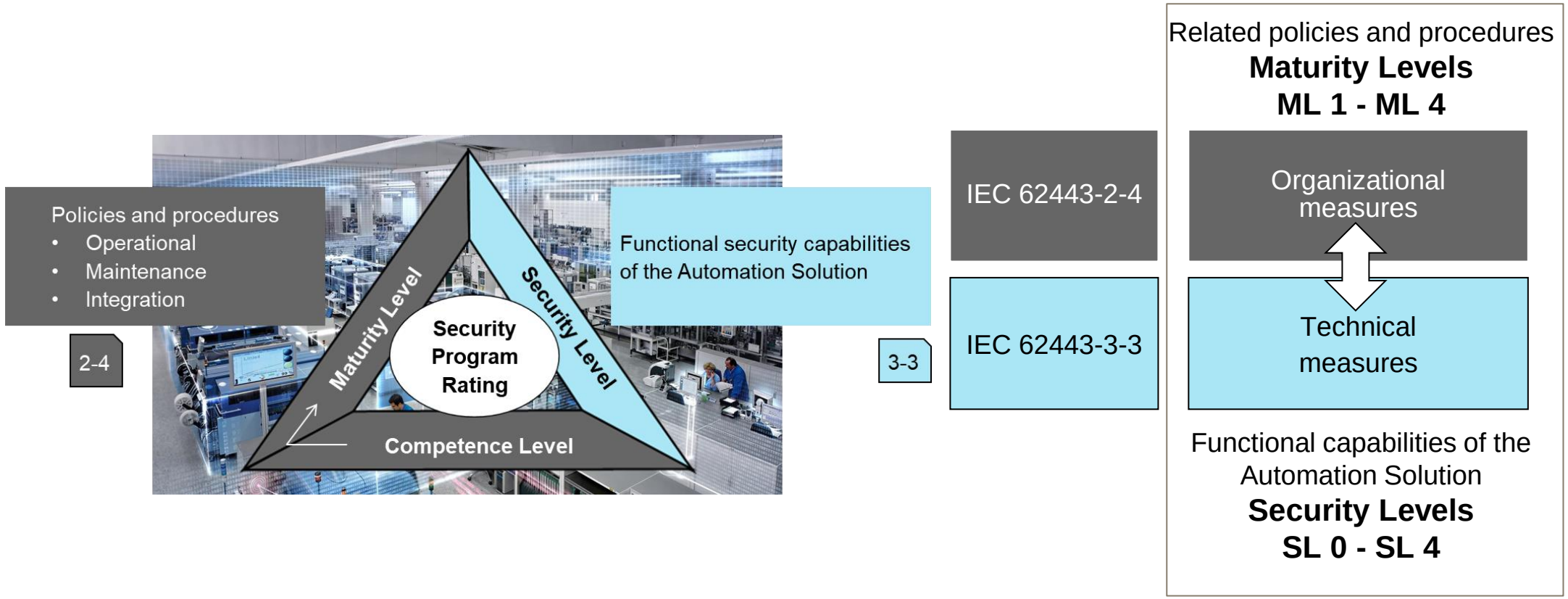
SIEMENS
Ingenuity for life

Standards define the requirements on security for product suppliers, system integrators and asset owners



* Examples of Security Requirements Standards

Using Levels in the Context of Secure Solutions



IEC 62443 Definition of SL and ML

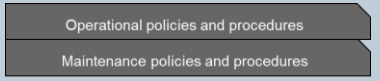
SIEMENS
Ingenuity for life

Evaluation of technical measures in the Automation Solution

SL 4	Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
SL 3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
SL 1	Capability to protect against casual or coincidental violation
SL 0	No specific requirement or protection necessary

IEC 62443-3-3 IEC 62443-4-2

Evaluation of organizational measures in operation and maintenance



ML 4	Using suitable process metrics, the effectiveness or performance improvements of the process, or both, can be demonstrated.
ML 3	A process at Level 3 is a Level 2 process that is being practiced.
ML 2	Documentation exists that describes how to manage the delivery and performance of the capability. There may be a significant delay between defining a process and executing/practicing it.
ML 1	Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner.

IEC 62443-2-4 IEC 62443-4-1

Notes:
- Maturity levels are note the same as in CMMI
- Background ML2/3 in part 2-4: Allows to show capability prior to first deployment

Future customer target requirement: IEC 62443 based Protection Levels

SIEMENS
Ingenuity for life

Assessment of security functionalities

SL 4	Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
SL 3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
SL 1	Capability to protect against casual or coincidental violation

Assessment of security processes

ML 4	Optimized – Process measured, controlled and continuously improved
ML 3	Defined – Process characterized, proactive deployment
ML 2	Managed – Process characterized , reactive
ML 1	Initial – Process unpredictable, poorly controlled and reactive.

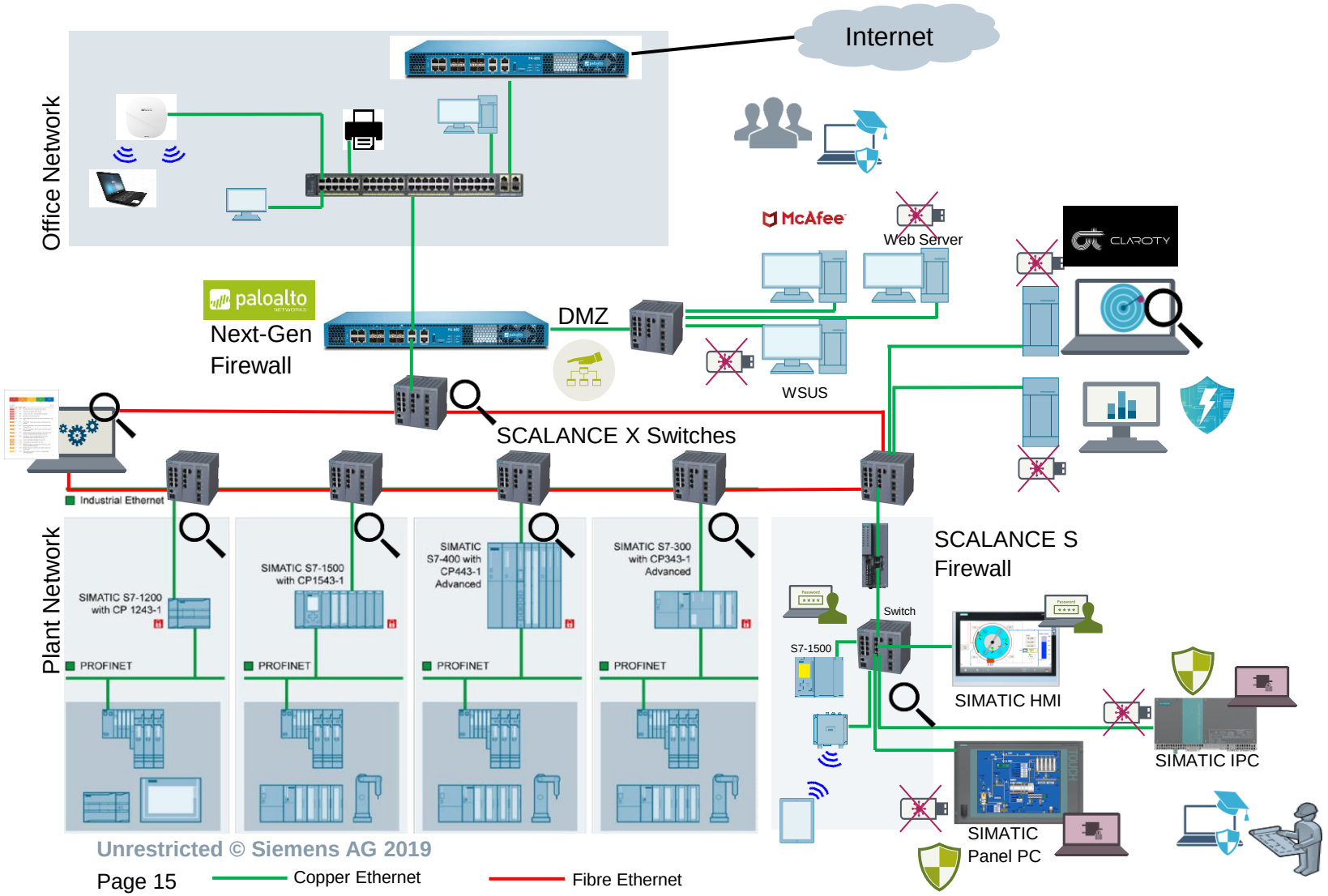
Protection Levels

PL 1	Protection against casual or coincidental violation
PL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
PL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
PL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Industrial Security Service Portfolio
Implementation Example

SIEMENS
Ingenuity for life

Customer Site (Factory Automation)



Industrial Security Services

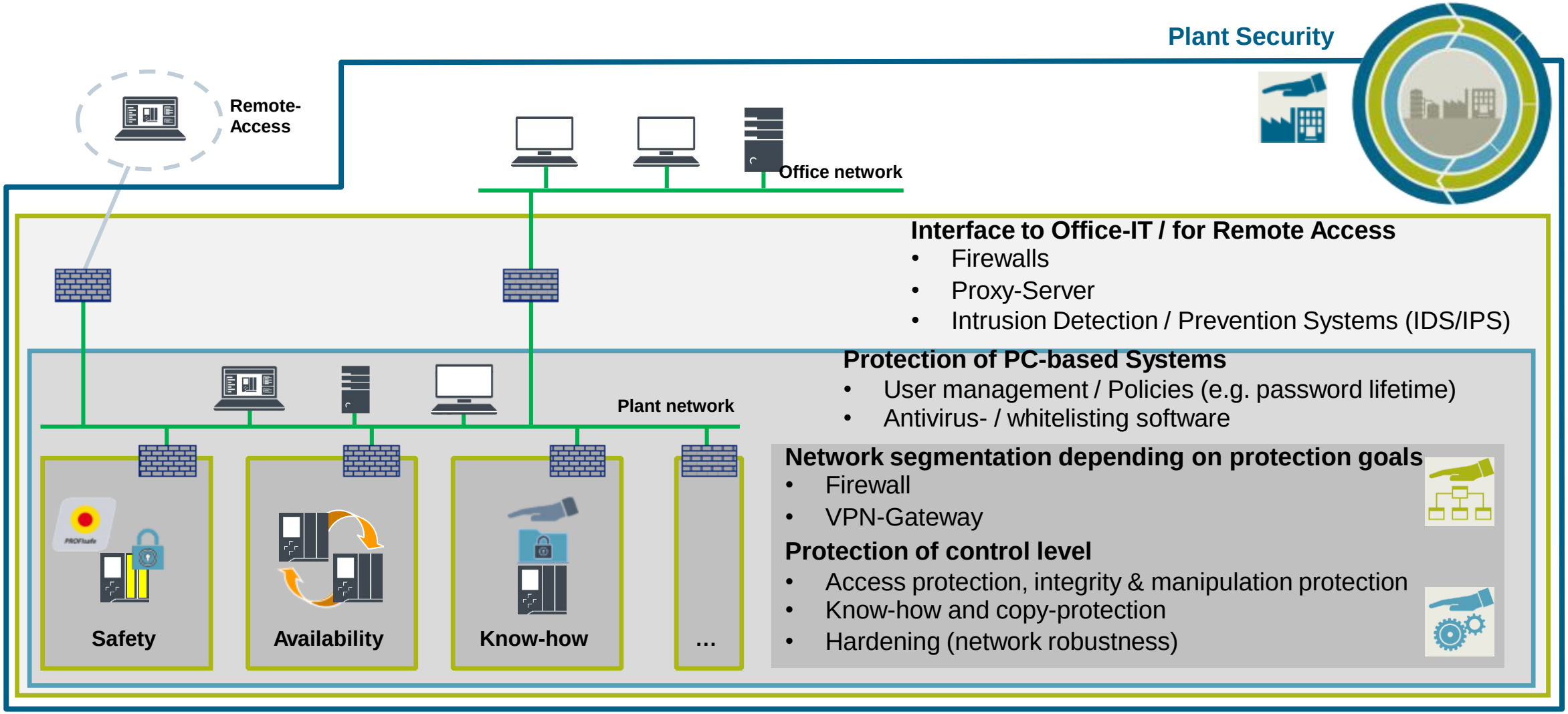
- Scanning Services
- Network Segmentation and DMZ
- Security Awareness Training, Policy and Procedures
- Antivirus and Application Whitelisting
- Firewalls and VPN
- System Hardening
- Identity and Access Management
- Windows Patch
- Security Vulnerability Management
- Industrial Anomaly Detection
- Security Monitoring

Consult
Implament
Manage

Defense-in-Depth security architecture to protect automated production plants

SIEMENS
Ingenuity for life

Plant Security



Interface to Office-IT / for Remote Access
- Firewalls
- Proxy-Server
- Intrusion Detection / Prevention Systems (IDS/IPS)

Protection of PC-based Systems
- User management / Policies (e.g. password lifetime)
- Antivirus- / whitelisting software

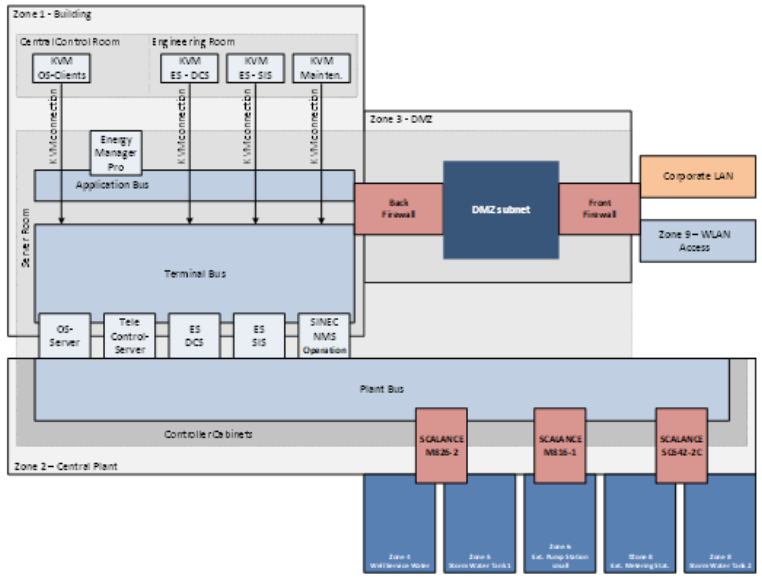
Network segmentation depending on protection goals
- Firewall
- VPN-Gateway

Protection of control level
- Access protection, integrity & manipulation protection
- Know-how and copy-protection
- Hardening (network robustness)

Secure Solution Framework
Security Design Specification

SIEMENS
Ingenuity for life

Figure 2-1- Overview of the Zones



2.2.1 Zone 1 – Building

The Zone 1 – Building is located on the Central Plant (zone 2) and contain the Central Control Room and the server room. The Terminal bus and the Application are installed only in this building.

Access to Zone 1 – Building is restricted to authorised personnel only.

2.2.2 Central Control Room

The central control room contains the Operator Workstations (OS-Client 1 - 2). The Workstations are screens that are connected via KVM extender to the respective HMI Client CPU (physical machine), as shown in the system overview. The workstations in the central control room are not connected to any IP network.

Access to the central control room is restricted to authorised personnel only.

2.2.3 Engineering Room

The engineering room contains the Engineering Stations (ES) for DCS and SIS and the Maintenance Station (MS). The Workstations are screens that are connected via KVM extender to the respective ES and MS CPU (physical machine), as shown in the system overview. The workstations in the engineering room are not connected to any IP network.

Access to the central control room is restricted to authorised personnel only.

The Wireless Access Points are located where required throughout the site and provide wireless access for Tablet PCs. The tablet PC's are Siemens SPIX clients and used for monitor and control of the plant.

Connection to the Wireless Access Points will be encrypted and require wireless clients to have knowledge of the specific wireless "key". The user authentication is realized with SIMATIC Logon.

2.2.17 External Zones

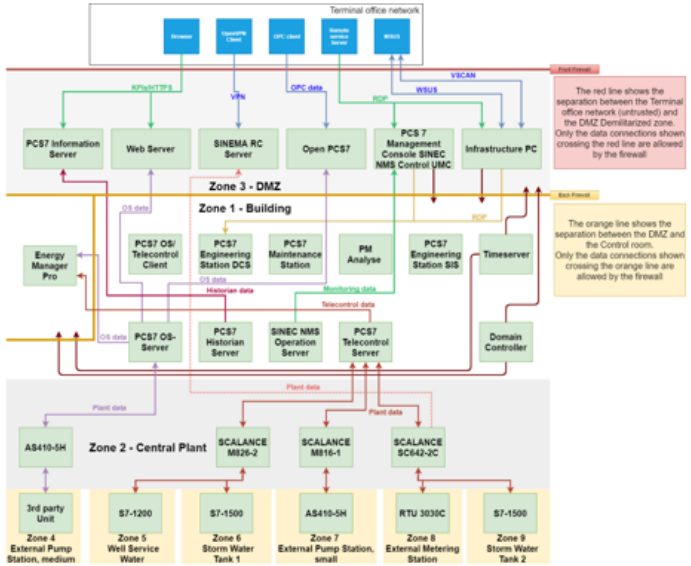
The Blueprint Wastewater Treatment Plant has only one external zone: The Corporate LAN.

This zone conventionally provides update services to the applications running in the DMZ. The associated network connections for these services are, by convention, initiated (sourced) from the DMZ to the appropriate provider (destination) in the company network. A few, limited services are initiated from the company network, to the DMZ.

2.3 DATA EXCHANGE BETWEEN ZONES

The overview of the connections and data traffic between the previously defined zones is provided in the tables that follow. An overview of the data exchange across the network zones provides figure 2.2.

Figure 2.2 - Overview of Data Exchange



Each of the zones listed in the tables below correspond to Figure 2-1.

5 IDENTITY AND ACCESS MANAGEMENT

Human user identification and authentication is provided and enforced on all interfaces which provide human user access. The human user interfaces include

- Applications with user interfaces (e.g. HMI client, web interfaces)
- Operating system accounts
- Accounts for administrative access to network devices
- Access to web interfaces of embedded devices

Centralization of account management across the solution is supported through the use of MS Active Directory Domain Controllers where personalized accounts for the Windows based machines are covered and where PCS7 application accounts are integrated with Simatic Logon. Network devices are central managed through SINEC NMS. UMC on SINEC NMS allows integration into the centralized account management.

Windows user accounts and application user accounts are managed with Active Directory and Simatic Logon. The domain controller is located on the Server panels on the terminal bus and a domain controller in the DMZ. The domain password policy is configured by Group Policy Object (GPO) scoped to the domain and rolled out to the managed Windows PCs. Password policies include e.g. password lifetime, minimum length, and minimum complexity requirements.

The password must contain at least three of four character types:

- Uppercase—for example, A to Z
- Lowercase—for example, a to z
- Numeric—0 to 9
- Nonalphanumeric—symbols such as !, #, %, or &

The Group Policy Objects (GPO's) for the project are defined in the document

Table 4-3 – Firewall rules

No.	Document No	Description
1	E504_wwtp_gpo_wins2016_v1.1.0_hardening	Group Policy Objects (GPO's)
2		

5.1 AUTHENTICATION MECHANISMS FOR USERS AND COMPONENTS

For application level access (e.g. to PCS 7 Runtime), user authentication and account management is handled by SIMATIC Logon. SIMATIC Logon authentication is based on Windows domain groups, managed with Active Directory. All personal user accounts at components are assigned to domain groups.

For operating system access, personalized Windows accounts and groups are used. These can be centrally managed by a domain controller where all PC based machines in the terminal bus, application bus, and DMZ networks are covered.

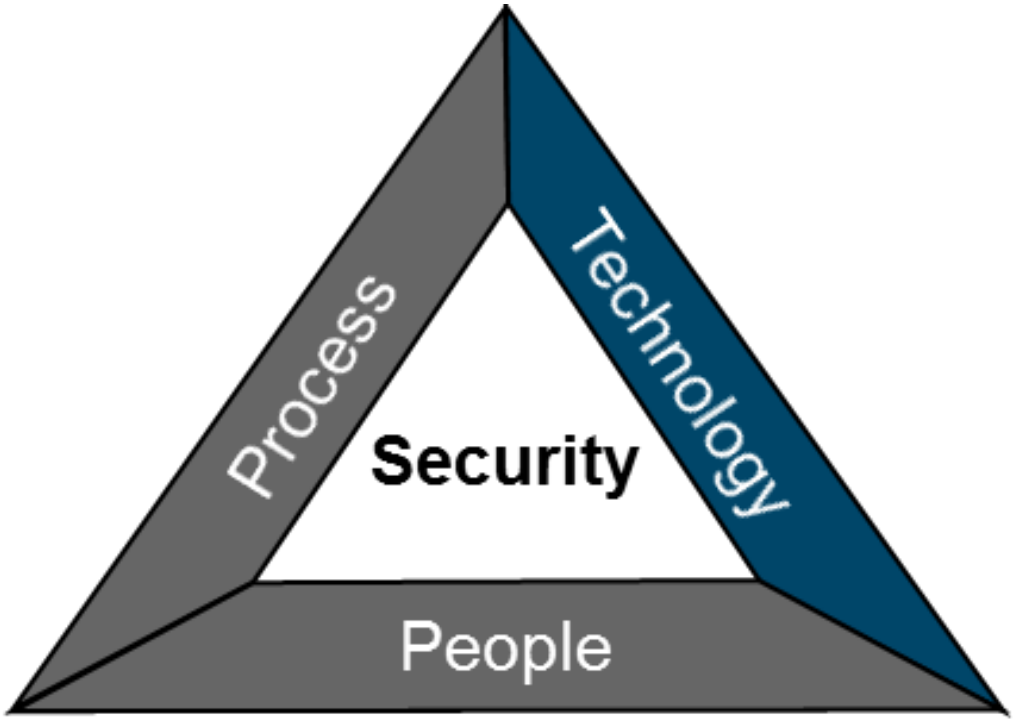
Exceptions to personalized (unique) accounts depend on configuration and operational procedures. These typically include accounts for machines that must be permanently operational and are used by several persons. An example could be an OS client, for operator control and monitoring.

Secure access to network devices is described in section 4.4 and can be integrated with the Active Directory managed groups and users through SINEC NMS and UMC. This covers administrative access to the SCALANCE devices.

For centralizing authenticated user access to SCALANCE network devices SINEC NMS is used. SINEC NMS supports a UMC feature for user management with capability to integrate with the overall Active Directory service.

Security is about technology, processes and people

SIEMENS
Ingenuity for life



A holistic security protection concept has to include technology, processes and people

SIEMENS
Ingenuity for life

Thank You & Questions

Paul Hingley

paul.Hingley@siemens.com

07808 822265