Industrial network security by network segmentation


Digitalization
needs
Powerfull Networks

Digitalization and big/cloud data address key industry trends

Industry trends

Time to market

- Fast innovation
- More complex products
- …

Flexibility

- Individualized mass production
- Volatile markets
- ….

Quality

- Closed-loop quality
- Traceability
- …

Efficiency

- Resource & energy efficiency
- Demanded product / quantity
- …

Digitalization

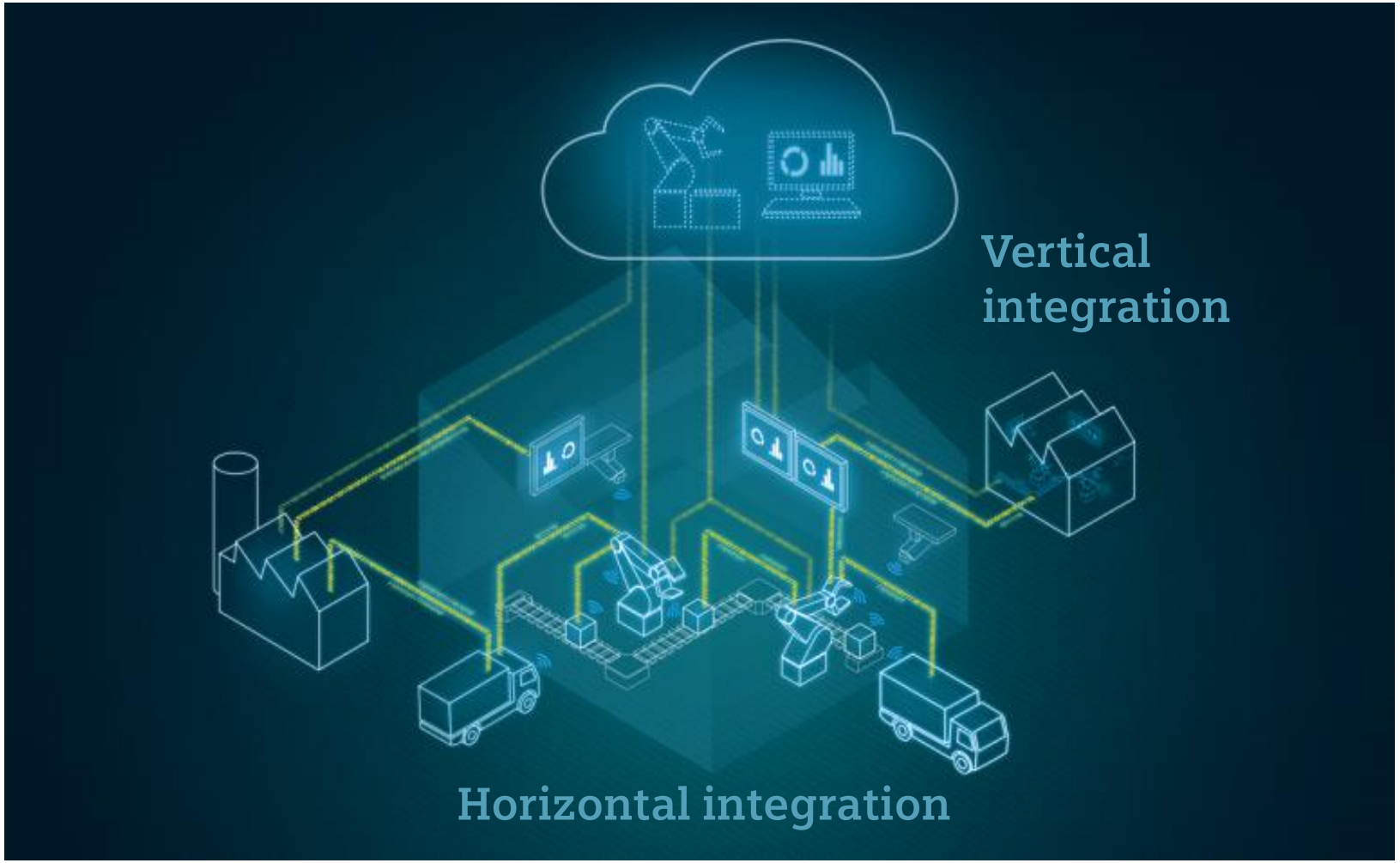
Industrie 4.0

Industrial Internet of Things (IIoT)

Cloud Data

SIEMENS

The Digital Factory needs powerful communication networks



Requirements of a production network doesn’t change

High speed
Real-time communication

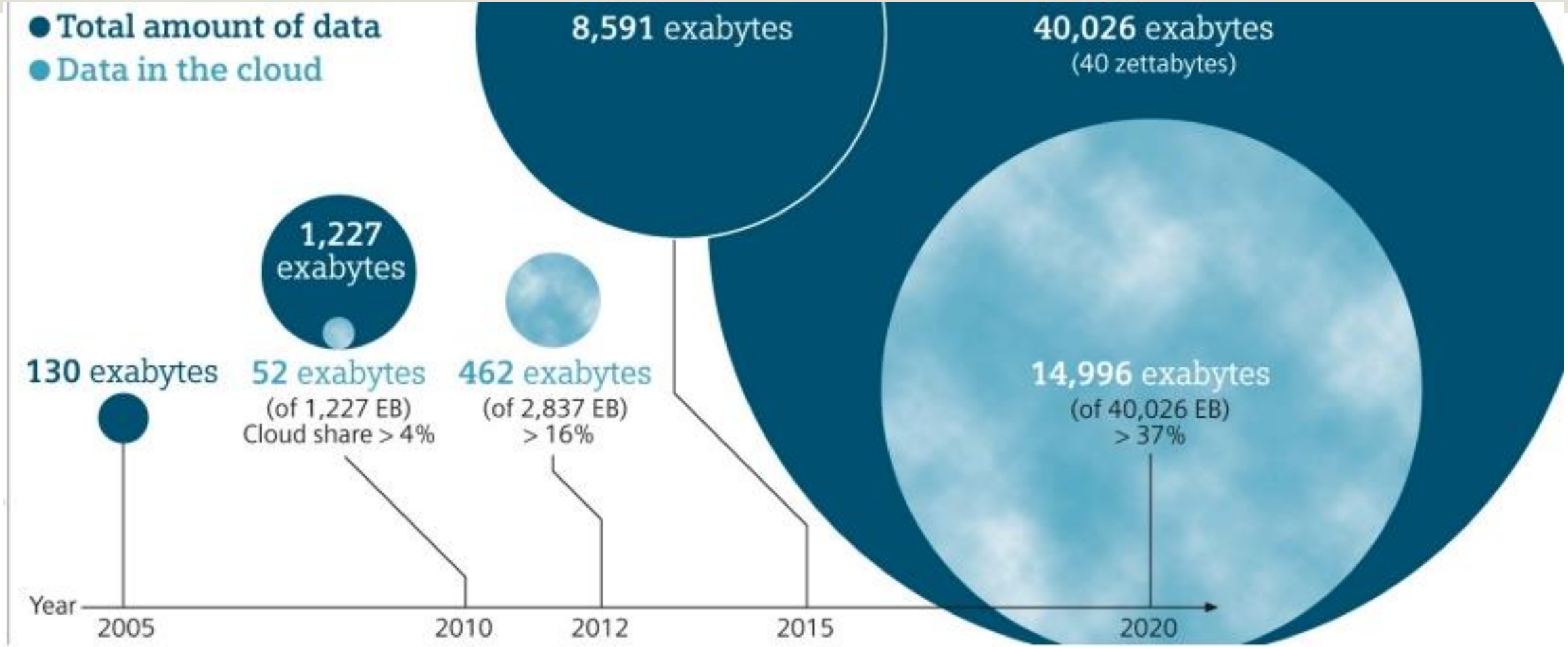
High data volume
broad band width - GByte

Secure connectivity
Robust, reliable components and networks

Smart assets
Identification solutions for communication between smart objects

SIEMENS

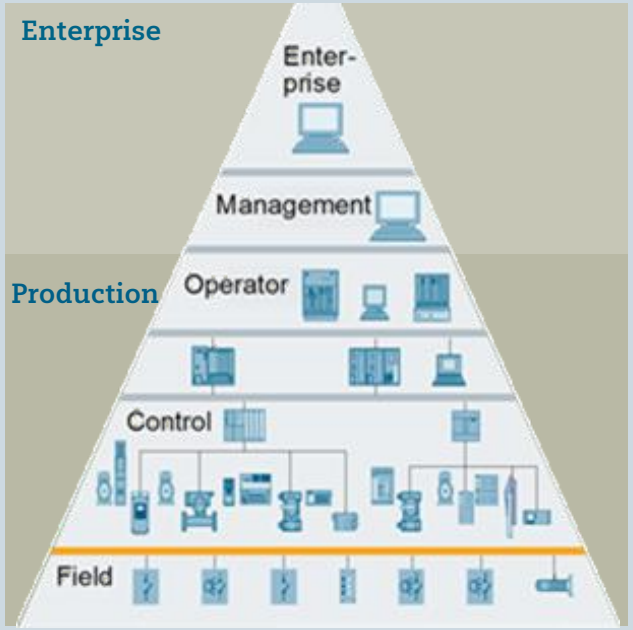
Communication – 40 x increase of data volume, 40% in the cloud



SIEMENS

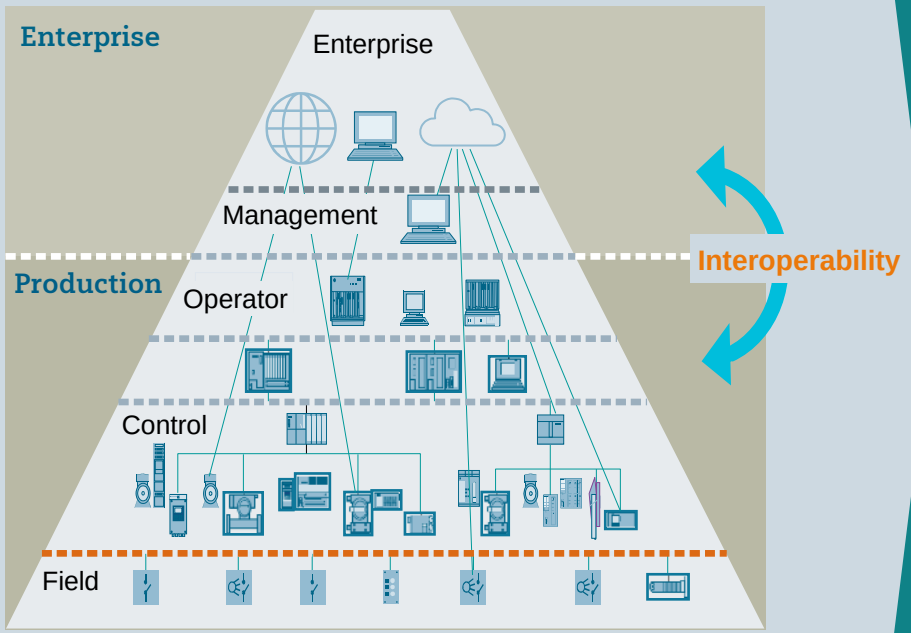
Digitalization results in enterprise and production layer to get closer connected

Yesterday: Limited interoperability



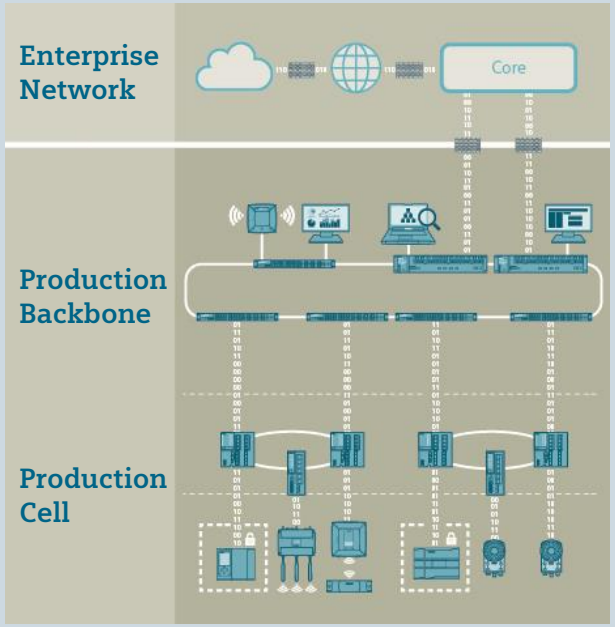
Limited communication between enterprise and production layer

Today: Arising challenges through increasing interoperability



Challenge to handle complexity of increasing communication

Future: Defined interface to handle complexity

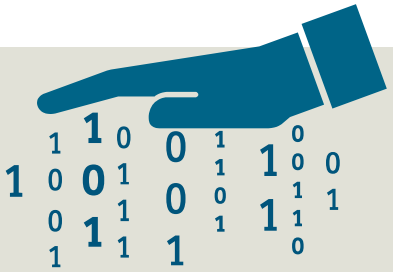


Two dedicated networks with defined managed interface

SIEMENS

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

What is it all about?
Exponentially increasing number of incidents and attacks to companies – with both IT and OT as main targets

IT-Security		Industrial Security
Confidentiality Integrity Availability		**Availability** Integrity Confidentiality
Second to minute range accepted	**Availability**	Network failure times < 300 ms
Network specialists	**Installation**	Plant commissioning personnel
Star-shaped	**Topology**	Plant-specific
Climate-controlled offices	**Location of use**	Harsh environment
Large, switches with large number of ports	**Device density**	Low, switches with fewer ports
Every 2 to 3 years	**Investment life cycle**	Min 5 to15 years

ISO 27000
(or NIST SP 800-35)

IEC 62443
(or NIST SP 800-82)

SIEMENS

Hacker attacks in the news
…more and more attention worldwide

A group of Israeli researchers demonstrated that it is possible to take over the Simatic S7 controller one of the most secure controllers in the industry.

A team of Israeli researchers demonstrated that it is possible to take control of the Simatic S7 controller without the knowledge of the operators.

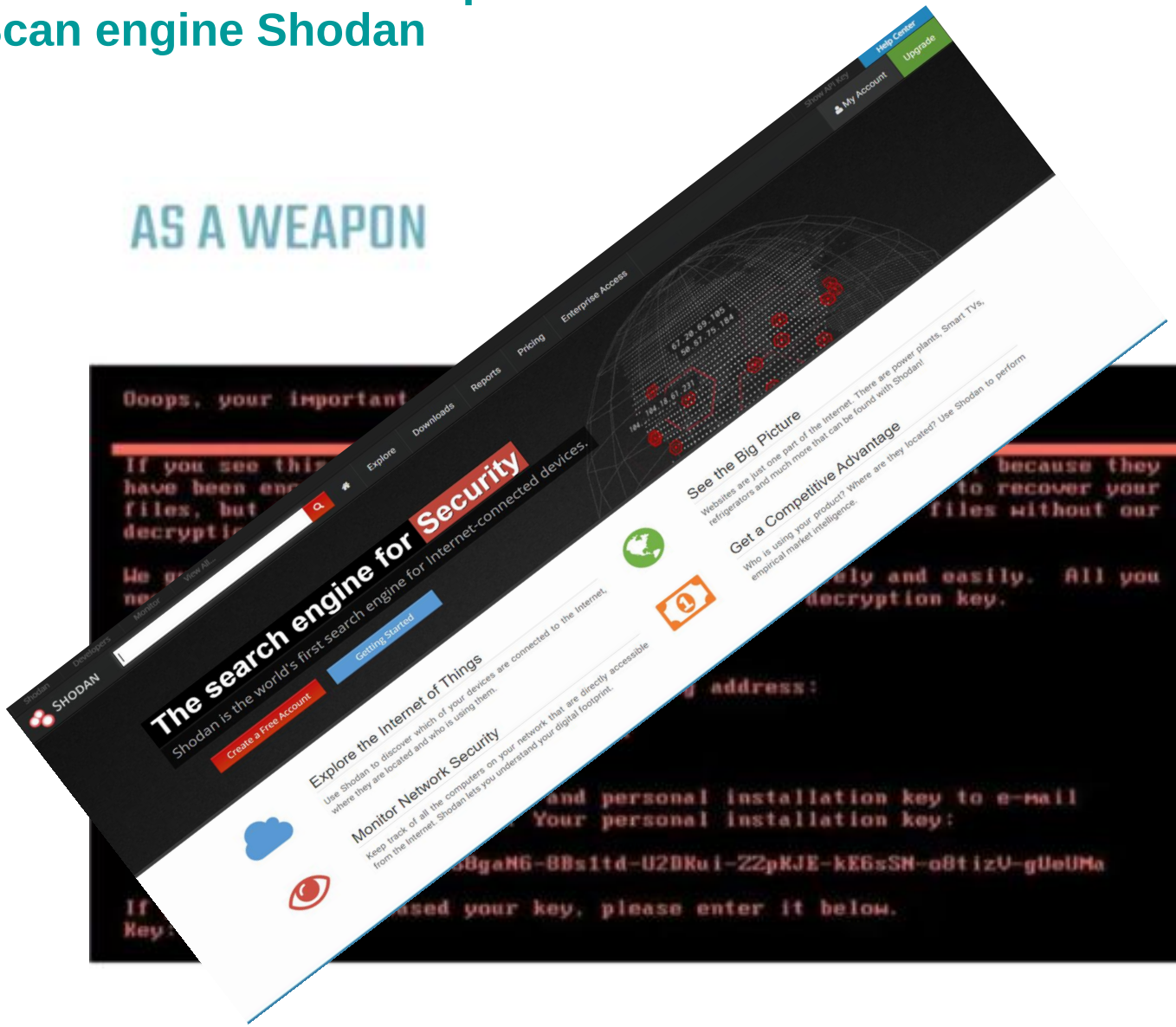
The team was composed of researchers from the Cyber Centers at the Technion and Tel Aviv University and experts from the National Cyber Arrangement.

Hackers blokkeren computernetwerk van Belgische school met ransomware

Het Atlas College in de Belgische stad Genk is getroffen door een aanval met ransomware. Volgens de directeur van de school zijn alle computers in het netwerk door versleuteling onbruikbaar gemaakt.

SIEMENS

Ransomware as a weapon
Scan engine Shodan



SIEMENS

IEC62443

On 9 may 2018, the EU strengthened its existing Cybersecurity legistlation. For operators of essential services, compliance with IEC-62443 became a must have in the EU

Energy
Electricity, Oil & Gas

Transport
Air, Rail, Water & Road (SNCB)

Banking

Financial market infrastructures

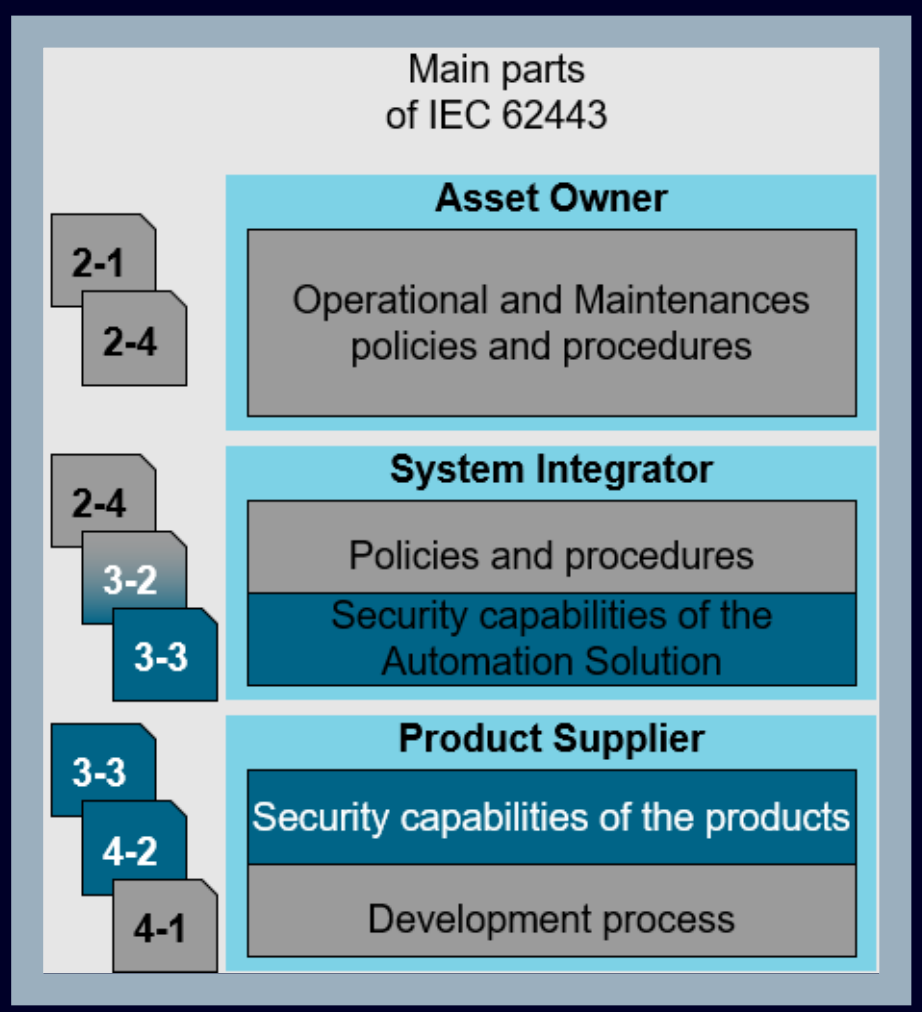
Health sector

Drinking water supply and distribution

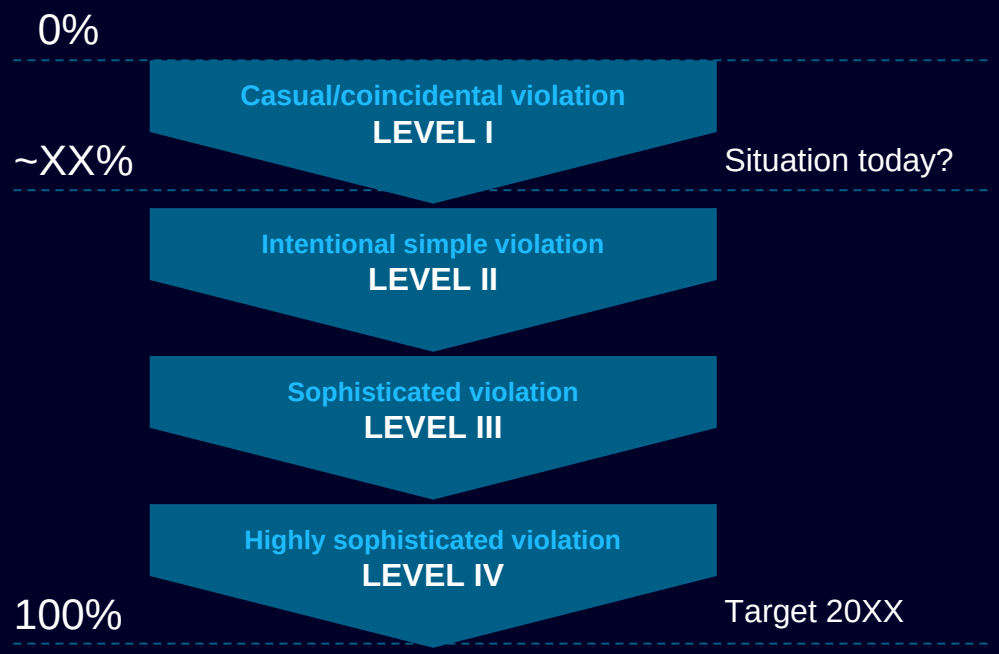
Digital Infrastructure
IXP, DNS & TLD

Digital Services
Online marketplace, search engine & cloud computing

IEC 62443 can help to look at Industrial Security from a business perspective



IV levels of compliancy with IEC 62443, based on the capability to protect against…



SIEMENS

IEC 62443
Industrial communication networks – Network and system security

General	
1-1	Terminology concepts and models
1-2	Master glossary of terms and abbreviations
1-3	System security compliance metrics
1-4	IACS security lifecycle and use-case

Policies & Procedures	
2-1	Reqiuirements for an IACS security management system
2-2	Implementation guidance for an IACS security management system
2-3	Patch management in the IACS environment
2-4	Security program requirements for IACS service providers
2-5	Implementation guidance for IACS asset owner

System	
3-1	Security technologies for IACS
3-2	Security Risk Assessment and System Design
3-3	System security requirements and security level

Component/Product	
4-1	Secure Product Development Lifecycle Requirments
4-2	Technical security requirements for IACS components

Process requirements (maturity level)

Technical requirements (security level)

Source: iacs-security.de | TÜV Hessen | bluecept GmbH

SIEMENS

We proudly promote our TÜV certificates

The foundation for secure networks : TÜV certification demonstrates the security of network components

Siemens has received TÜV certification in compliance with IEC 62443-4-2 and -4-1 for network components in the Scalance XB-200, XC-200, XP-200, XF-200BA and XR-300WG product families. Customers are therefore able to realize secure system architectures, which clearly increases the overall security of a plant.

The certification demonstrates that the product development process previously certified has been consequently applied during product development of above-mentioned SCALANCE X-product lines. It also confirms that key technical product requirements have been taken into account and implemented in the network components.

Learn more

SIEMENS

IEC 62443-3-3 Technical Gap Analysis of OT Security (1/2)

Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 *(1 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication					
SR 1.3 – Account management					
SR 1.3 RE 1 – Unified account management					
SR 1.4 – Identifier management					
SR 1.5 – Authenticator management					
SR 1.5 RE 1 – Hardware security for software process identity credentials					
SR 1.6 – Wireless access management					
SR 1.6 RE 1 – Unique identification and authentication					
SR 1.7 – Strength of password-based authentication					
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users					

Security Level (SL)

Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation	4
Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	3
Protection against intentional violation using simple means with low resources, generic skills and low motivation	2
Protection against casual or coincidental violation	1
No specific requirements or security protection necessary	0

4.2 Findings and mitigations for IEC62443-3-3 Level 2

IEC 62443-3-3 Level 2						
No	SR 1.1 RE1	Unique identification and authentication	No User or Access control implemented for windows and limited in WinCC	TP4		
No	SR 1.2	Software process and device identification and authorization	ANY-ANY - connection in DMZ	TP6		
No	SR 1.6 RE1	Unique identification and authentication in Wireless	Open unsecured network connected to DMZ	TP1		
No	SR 3.2 RE1	Malicious Code Protection on Entry and Exit points	No traffic scanning on DMZ firewall. No quarantine station.	TP2	TP7	TP7 - NGFW
No	SR 7.3 RE1	Backup verification	Images are not tested	TP9		

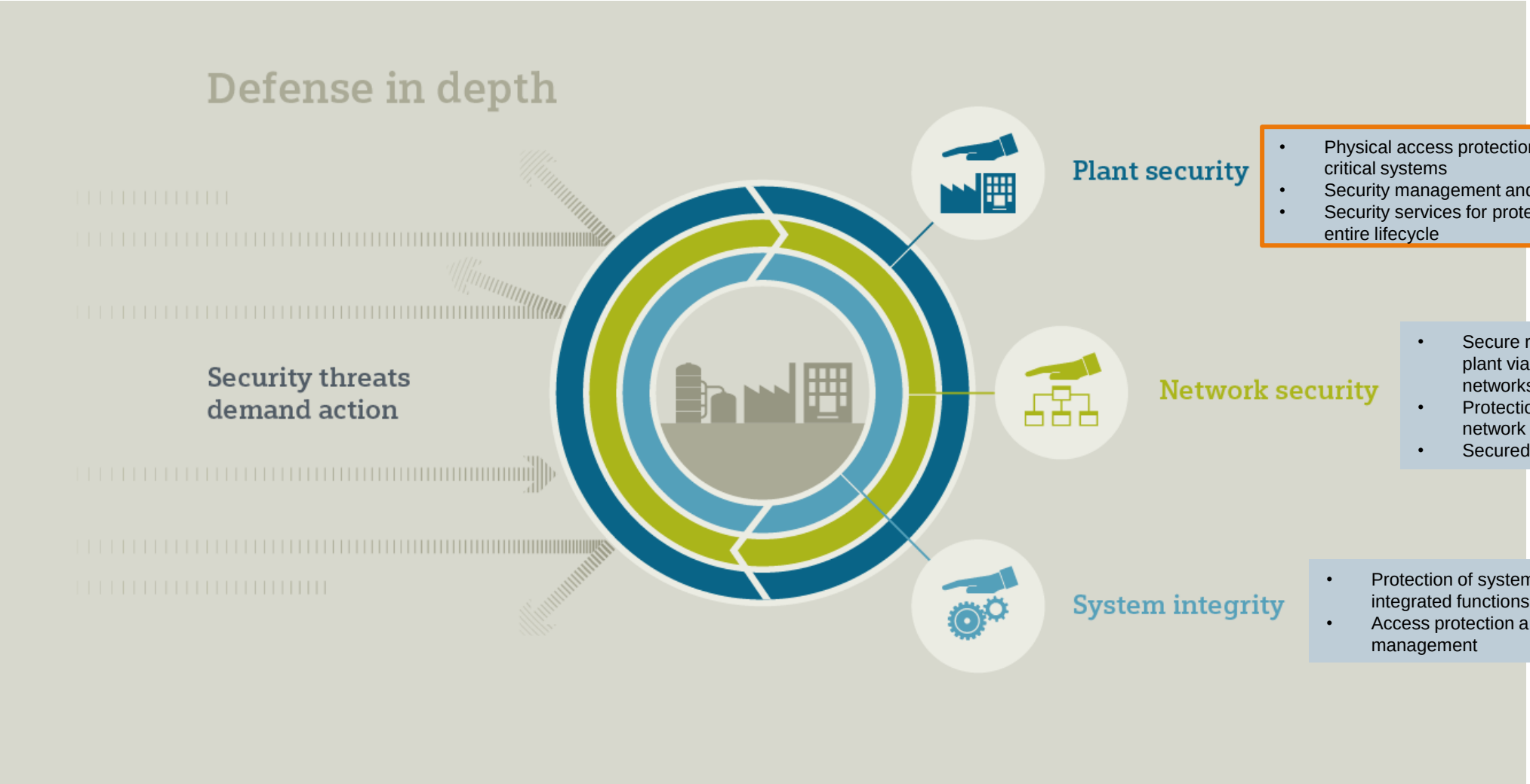
Failed requirements | **Findings** |

SIEMENS

SIEMENS
Ingenuity for life

Siemens Solutions

Industrial Security
The Siemens Solution



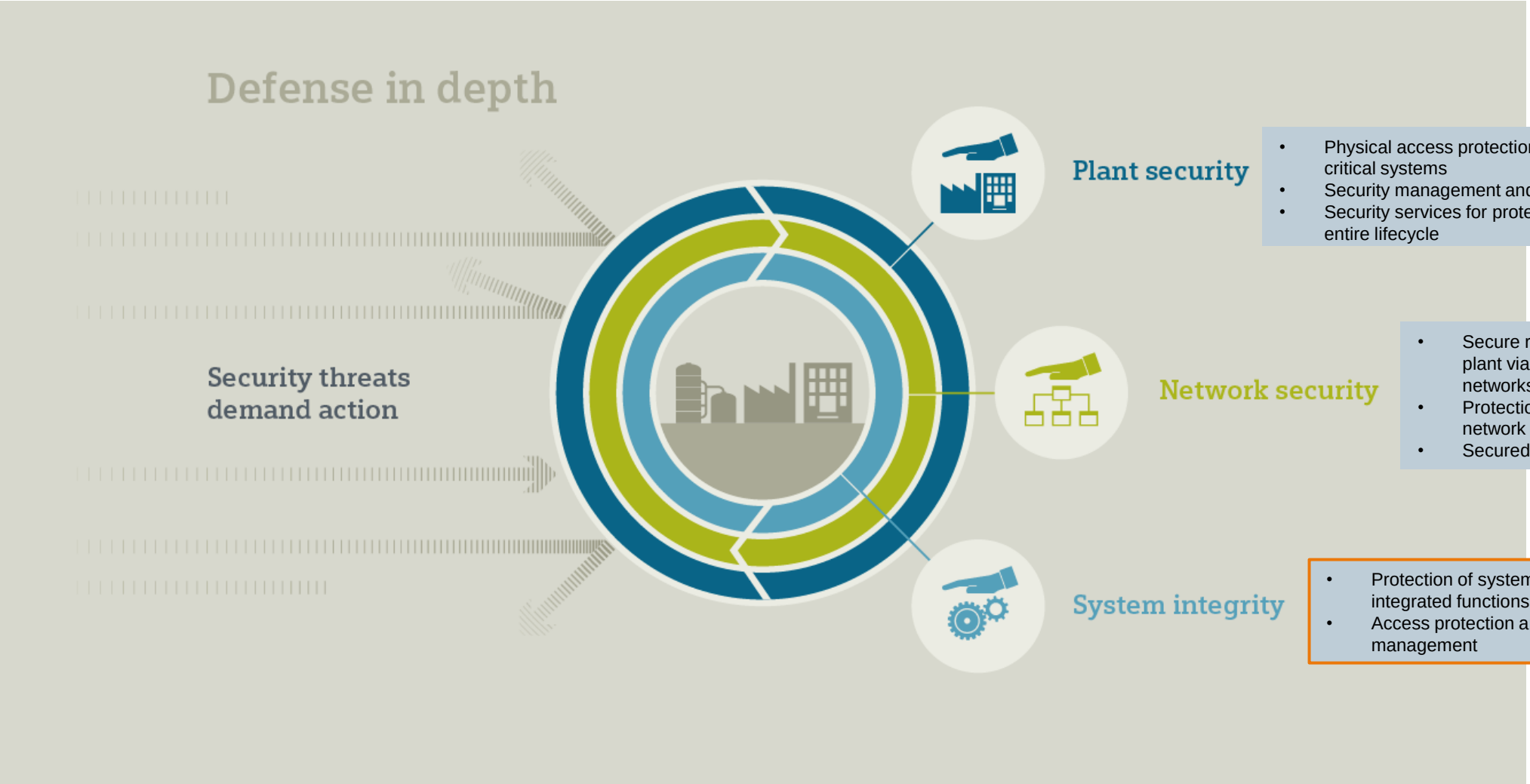
- Physical access protection to the plant and critical systems
- Security management and policies
- Security services for protection of a plant's entire lifecycle

- Secure remote access to the plant via the Internet or mobile networks
- Protection of the plant / machine network through segmentation
- Secured communication

- Protection of system integrity through integrated functions
- Access protection and rights management

SIEMENS

Industrial Security
The Siemens Solution



- Physical access protection to the plant and critical systems
- Security management and policies
- Security services for protection of a plant's entire lifecycle

- Secure remote access to the plant via the Internet or mobile networks
- Protection of the plant / machine network through segmentation
- Secured communication

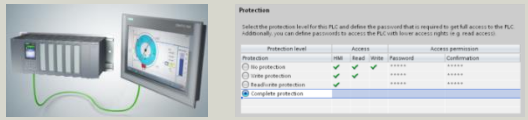
- Protection of system integrity through integrated functions
- Access protection and rights management

SIEMENS

System Integrity

System hardening for all SIMATIC S7-1200 and S7-1500 controllers

Access protection (authorization levels)
… prevents unauthorized access to controllers



Know-how protection (locking of blocks)
… prevents reading, writing, modifying

Copy protection (program linkage)
… prevents unauthorized copying

SIEMENS

System Integrity

Secure communication with SIMATIC controllers (only for the new generation)

Secure Open User Communication

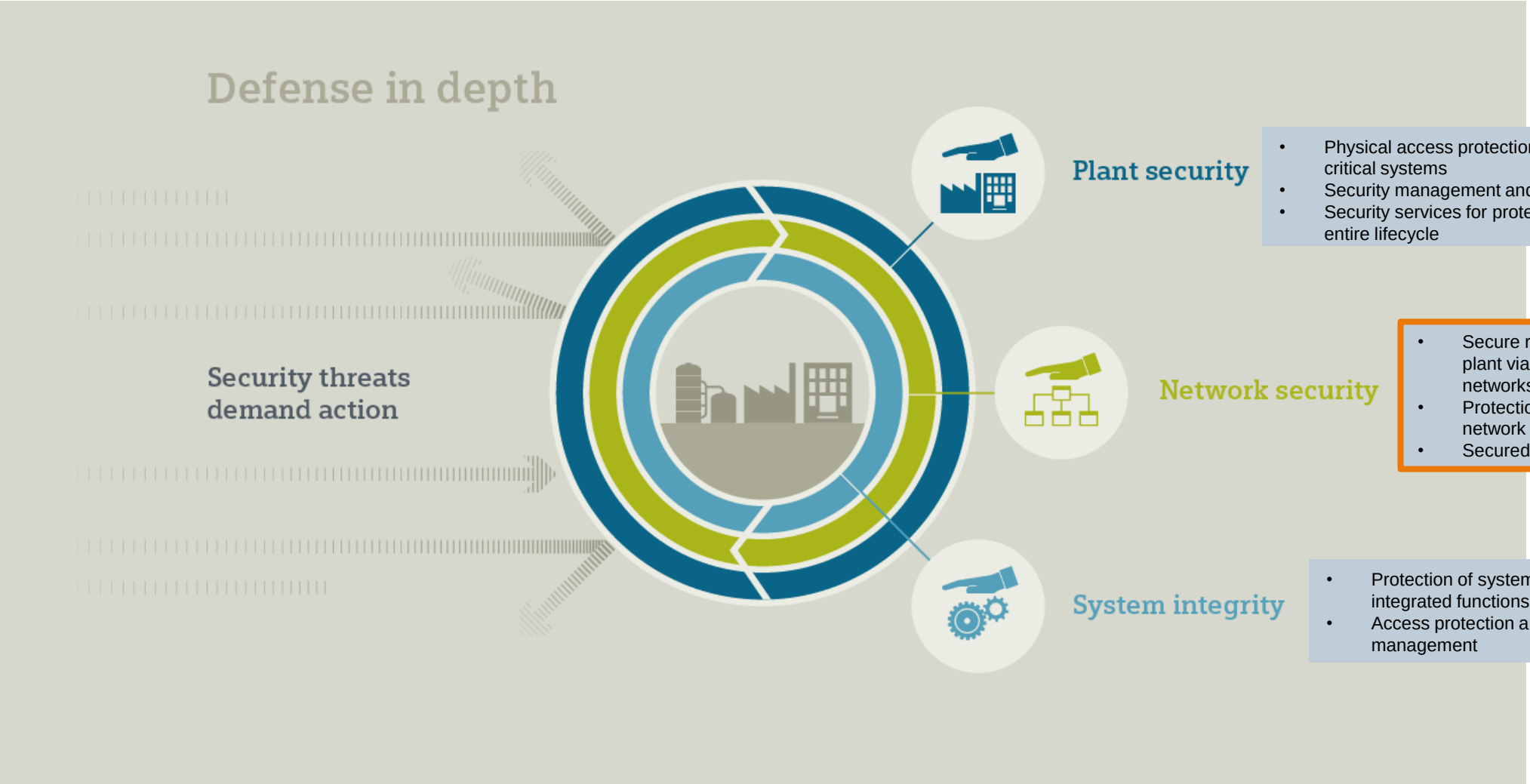
… secure communication via TLS (Transport Layer Security)

OPC UA Data Access Server

… secure connection to higher-level systems

SIEMENS

Network security



- Physical access protection to the plant and critical systems
- Security management and policies
- Security services for protection of a plant's entire lifecycle

- Secure remote access to the plant via the Internet or mobile networks
- Protection of the plant / machine network through segmentation
- Secured communication

- Protection of system integrity through integrated functions
- Access protection and rights management

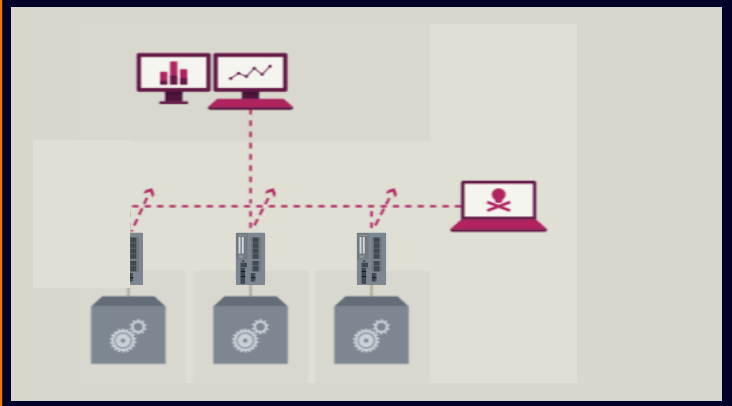
SIEMENS

Network Security Use Cases

Cell protection/Segmentation

Devices without own network security functionality can be protected within an automation cell.

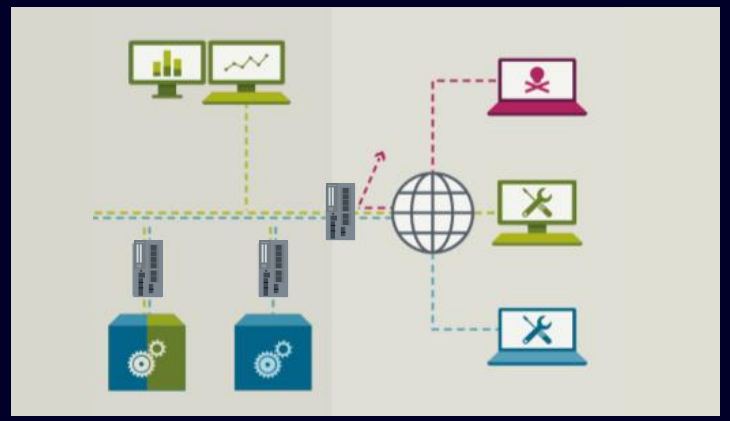
➔ Access to automation cell is secured by firewall mechanisms.



Remote access

Secured remote access via the Internet or mobile networks to avoid espionage and sabotage.

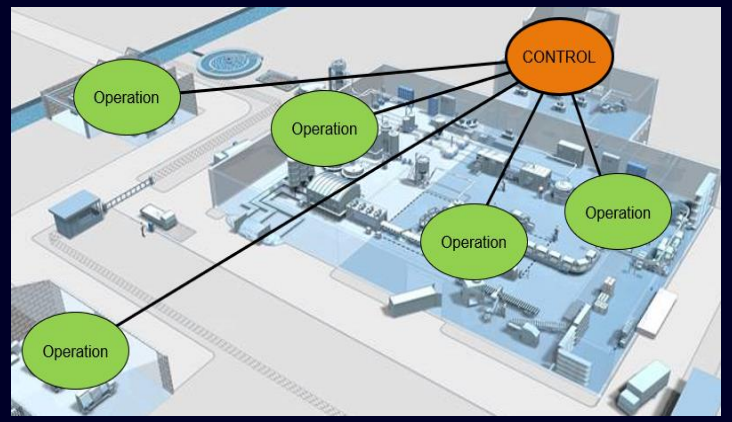
➔ Encryption of data communication and access control to dedicated end devices.



Software Solutions

Increased protection by means of monitoring, management

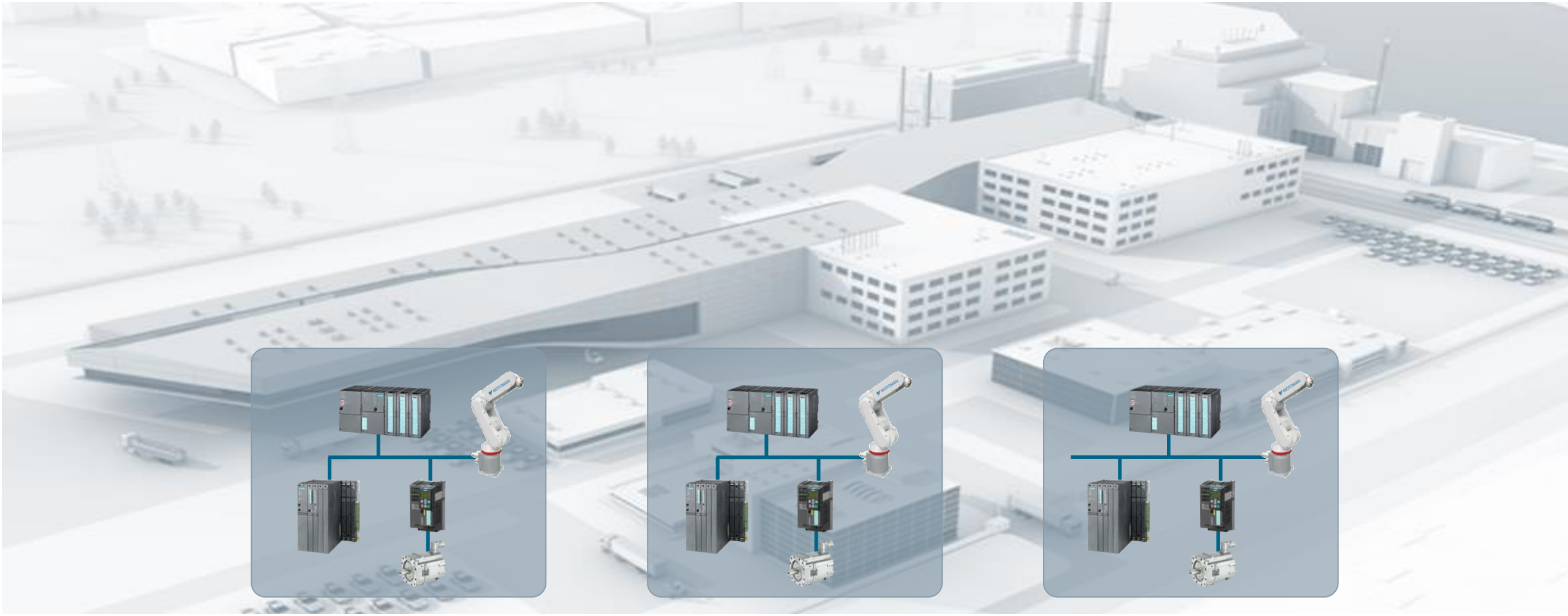
➔ Monitoring, faultmanagement, patchmanagement, firewallmanagement



SIEMENS

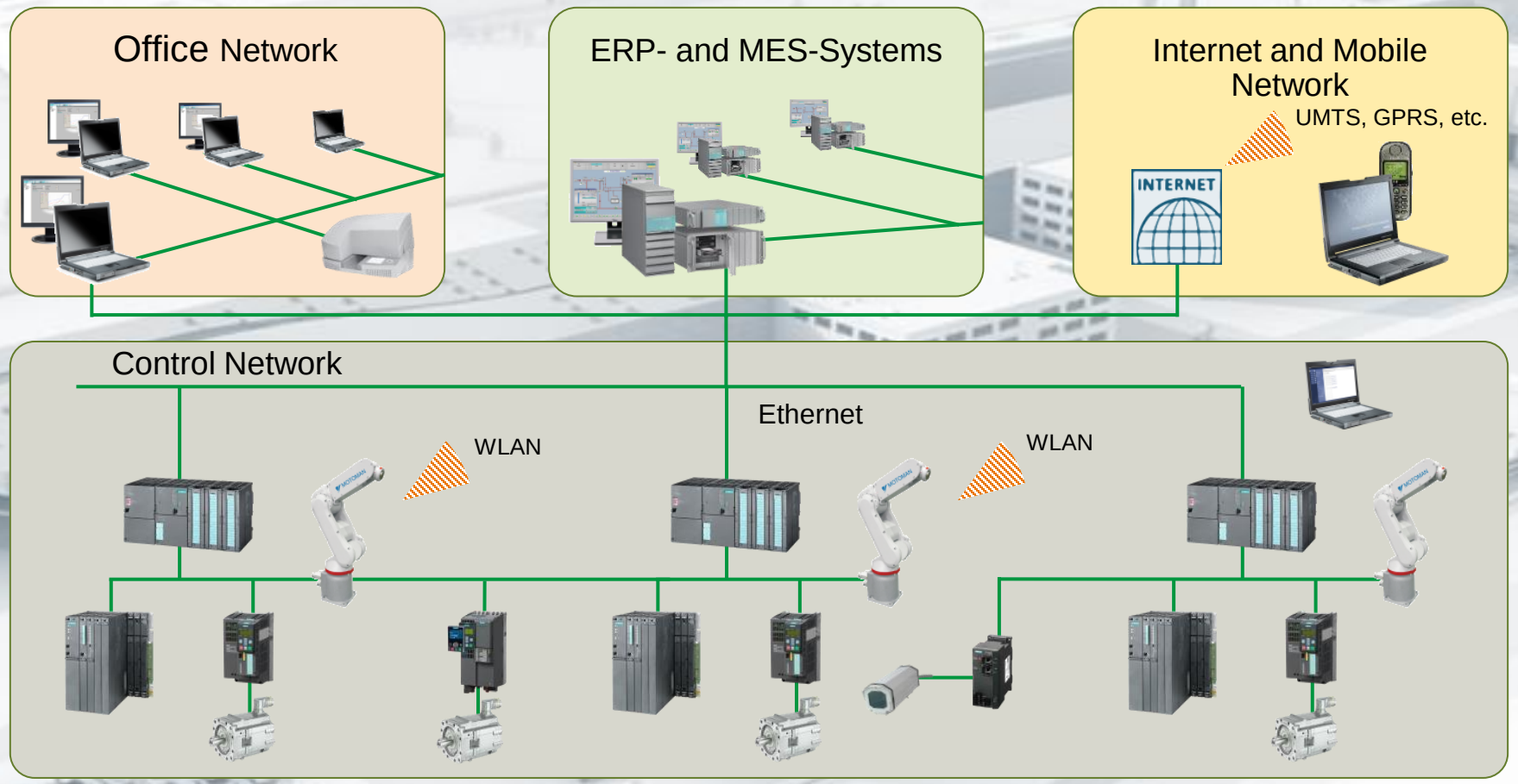
Network security

We come From isolated production islands…



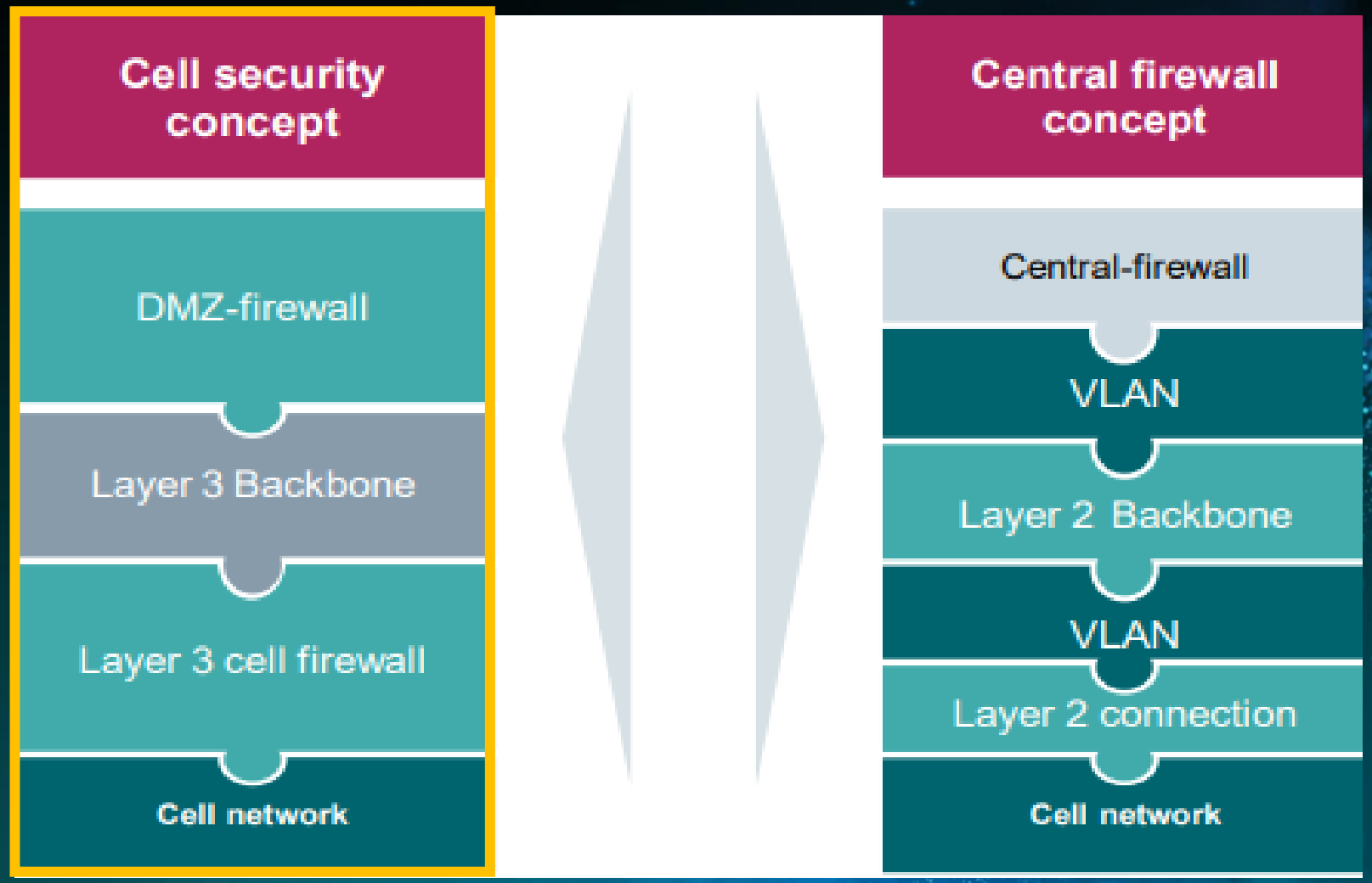
SIEMENS

Now everything will be connected!

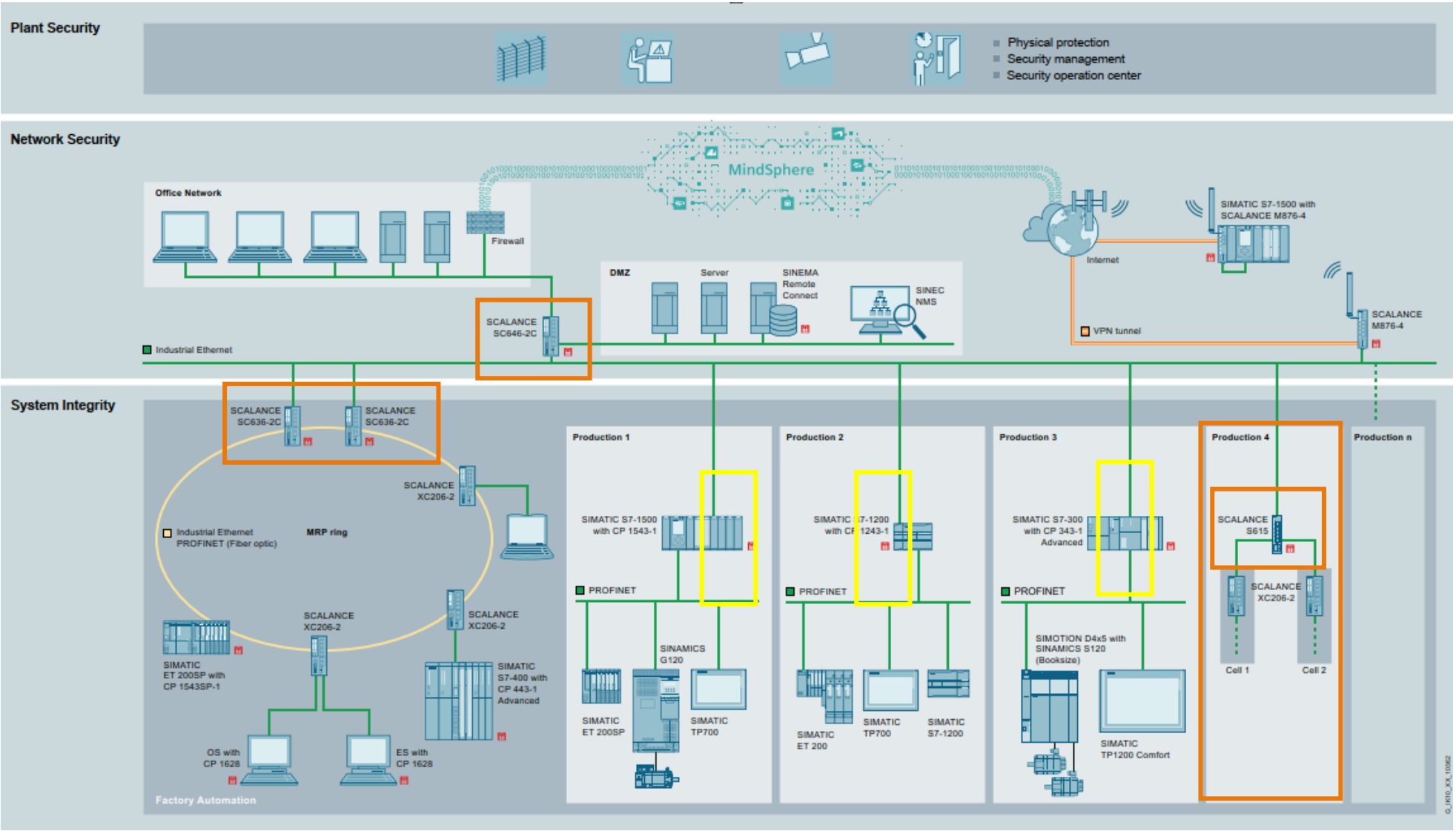


SIEMENS

Bridging of IT&OT: 2 Approaches



Cellprotection with CP card + Scalance S



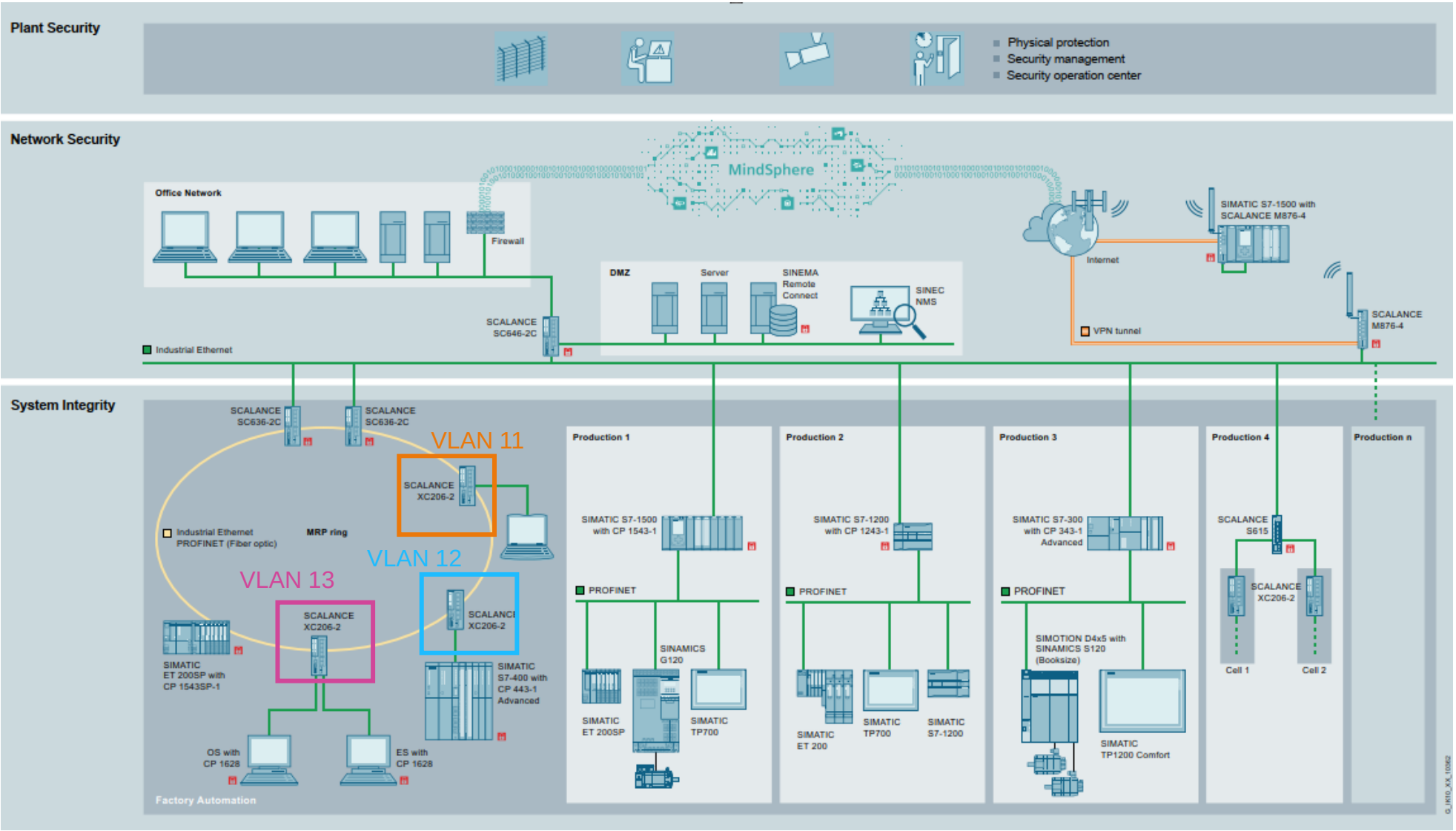
SIEMENS

Network Security
SCALANCE S - Portfolio

Interfaces	10/100 Mbps	10/100/1000 Mbps	
Firewall/routing	**100 Mbps**	**200 Mbps**	**600 Mbps**
VPN	**35 Mbps**	**55 Mbps**	**120 Mbps**
Firewall **NAT** **VPN**	**S615** Maximum: 64 rules 20 VPNs 	**S612, S623, S627-2M** Maximum: 256 rules 128 VPNs 	**SC642-2C, SC646-2C** Maximum: 1000 rules 200 VPNs 
Firewall **NAT**		**S602** Maximum: 256 rules 	**SC632-2C, SC636-2C** Maximum: 1000 rules 

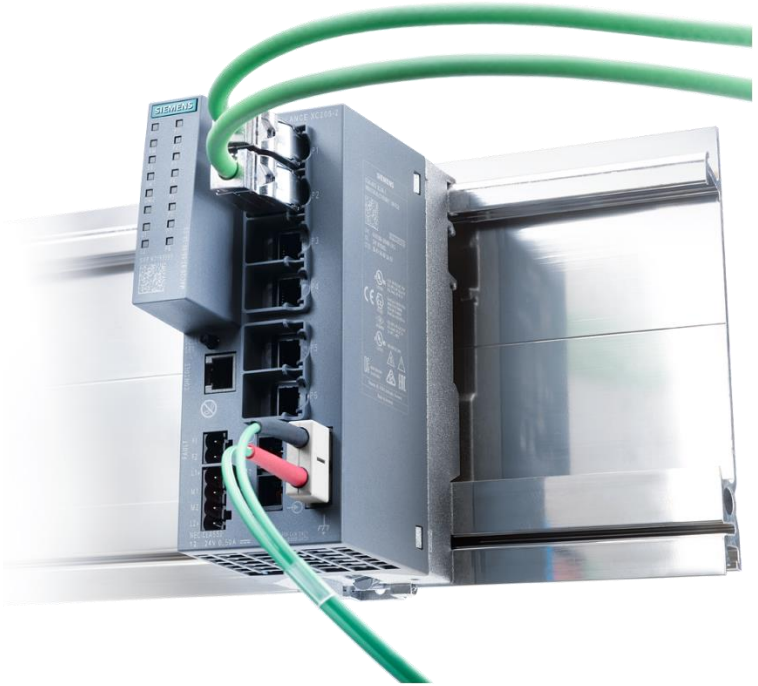
SIEMENS

Cellprotection with VLAN’s



SIEMENS

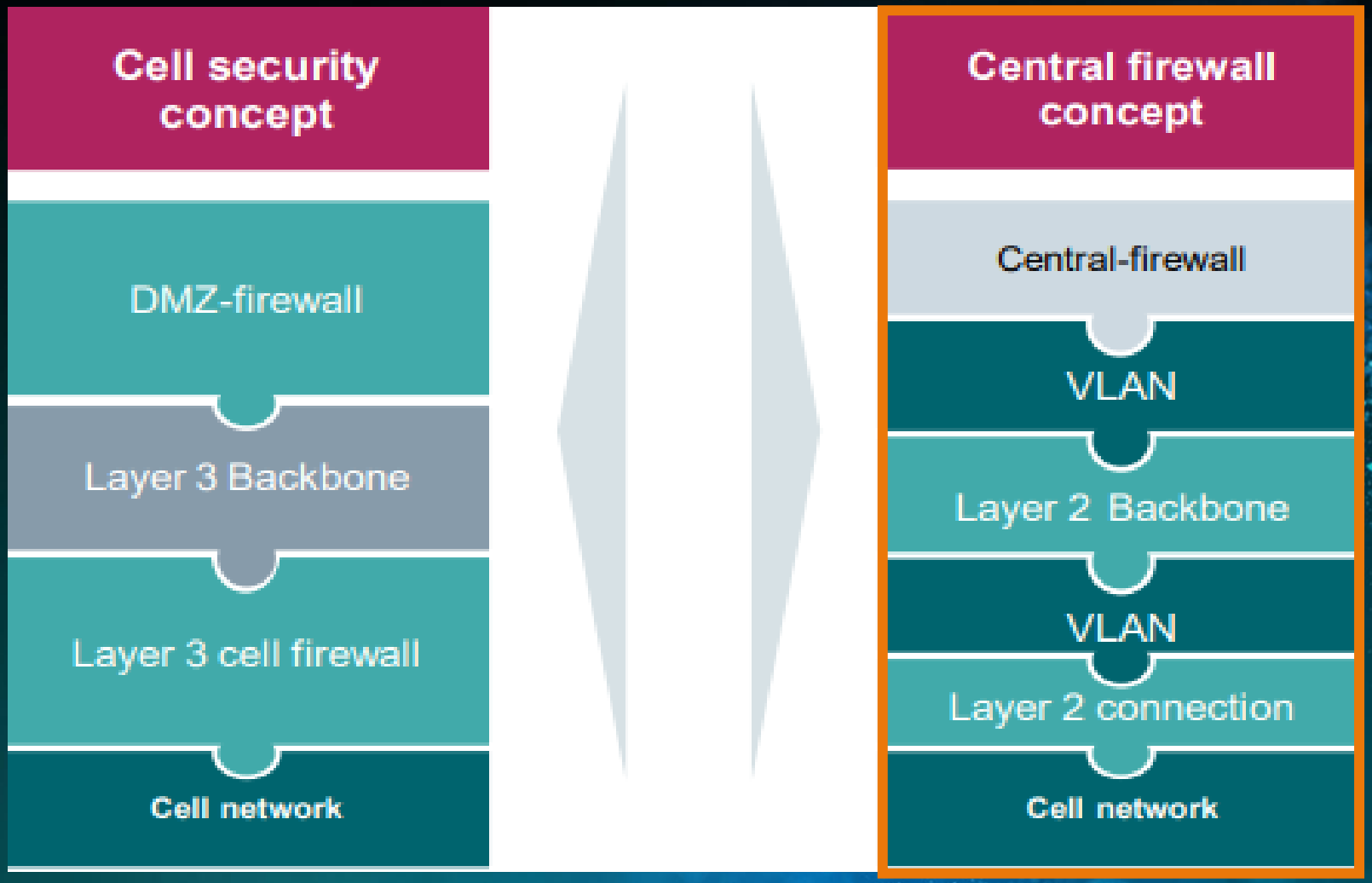
SCALANCE XC-200
IEC62443



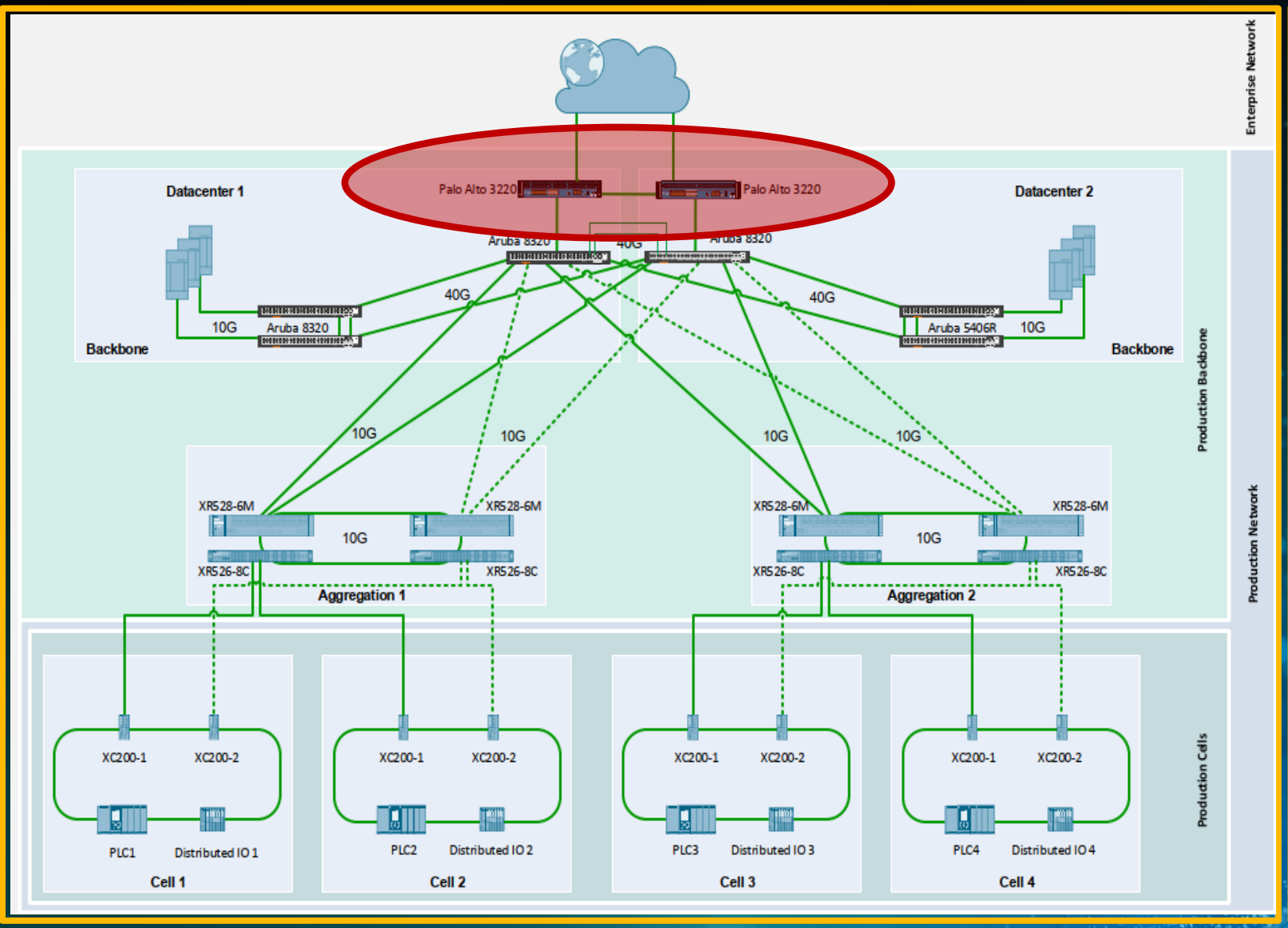
IEC 62443 Requirement	Product features / fulfilment
• User accounts / user identification	• Local or • central via RADIUS and UMAC
• Network segmentation / restricted data flow	• On Layer 2 with VLAN´s • Not inteded use as e.g. Firewall
• Network / Security monitoring	• Syslog client • SNMPv3
• Back up / Restore	• Locally via C-Plug • (remote) admin via SSH (+?)
• Securing the management plane	• WBM via HTTPS by default • SSH by default (or telnet ?)

SIEMENS

Bridging of IT&OT: 2 Approaches



Concept example of bridging the IT/OT network



Central FW Approach

- Interconnection IT/OT via NGFW
- L3 connection with 10Gbps
- Field network,1 Gbps
- Powerfull Central FW
- Network changes Independant from FW
- Propagation of errors posible
- Centralised Manageability
- Communication depends on logical infratstructure

Thank You

SIEMENS

Contact

Published by Siemens NV/SA

Bart Boumans
Sales Specialist Industrial Communication
Digital Industries - DCP
Guido Gezellestraat 123
1654 Huizingen
Belgium
Mobile +32475828585

E-mail bart.boumans@siemens.com