



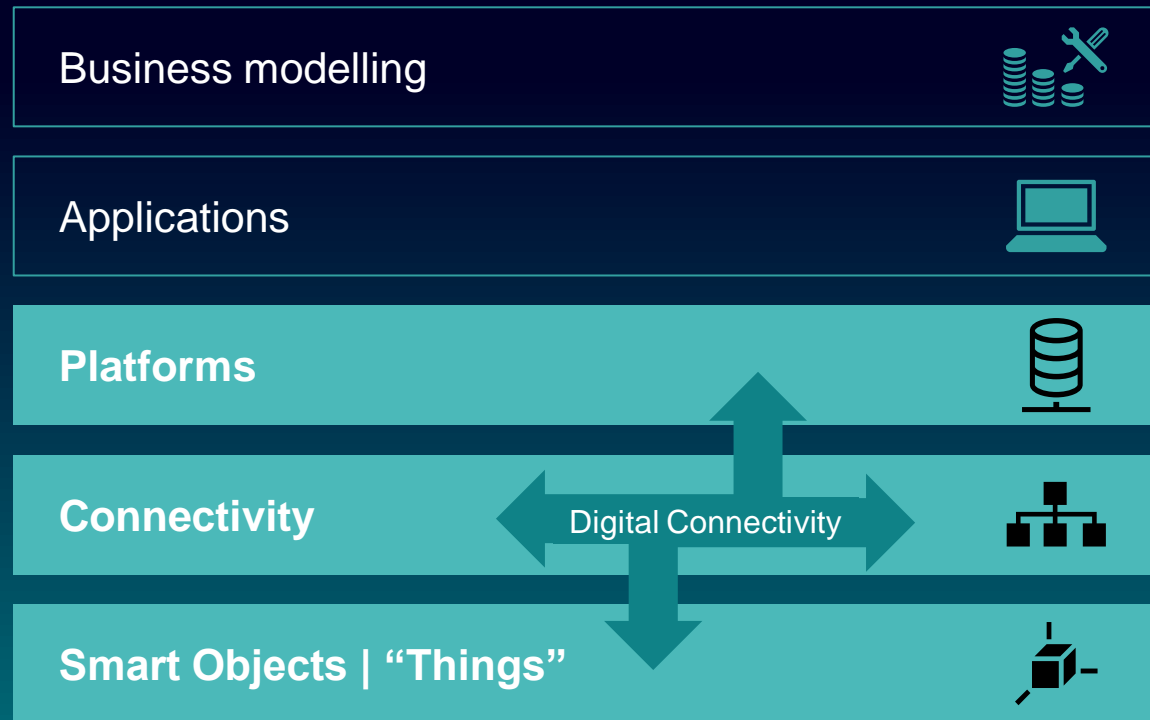
# Cybersecurity for Industrial Operations

Industrial Cybersec Forum – 9 Feb. 2023

# | What/why Cybersecurity?

**Digitalization:**  
IoT architectures are the base for your future success

## IoT Architecture



**High speed**  
Real-time communication

**High data volume**  
broad band width - GByte

**Secure connectivity**  
Robust, reliable components  
and networks

... and this requires **powerful communication networks** in industry

# 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

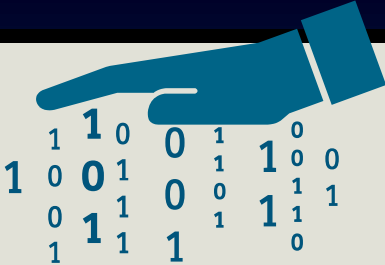
Industrial Security

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 to 15 years

ISO 27000  
(or NIST SP 800-35)

IEC 62443  
(or NIST SP 800-82)

# | NIS 2

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU)  
No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2  
Directive)



**On 9 May 2018, the EU strengthened its existing Cybersecurity legislation. 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



## Will it apply to me?



IEC 62443

Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail**, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administrations	
Space	

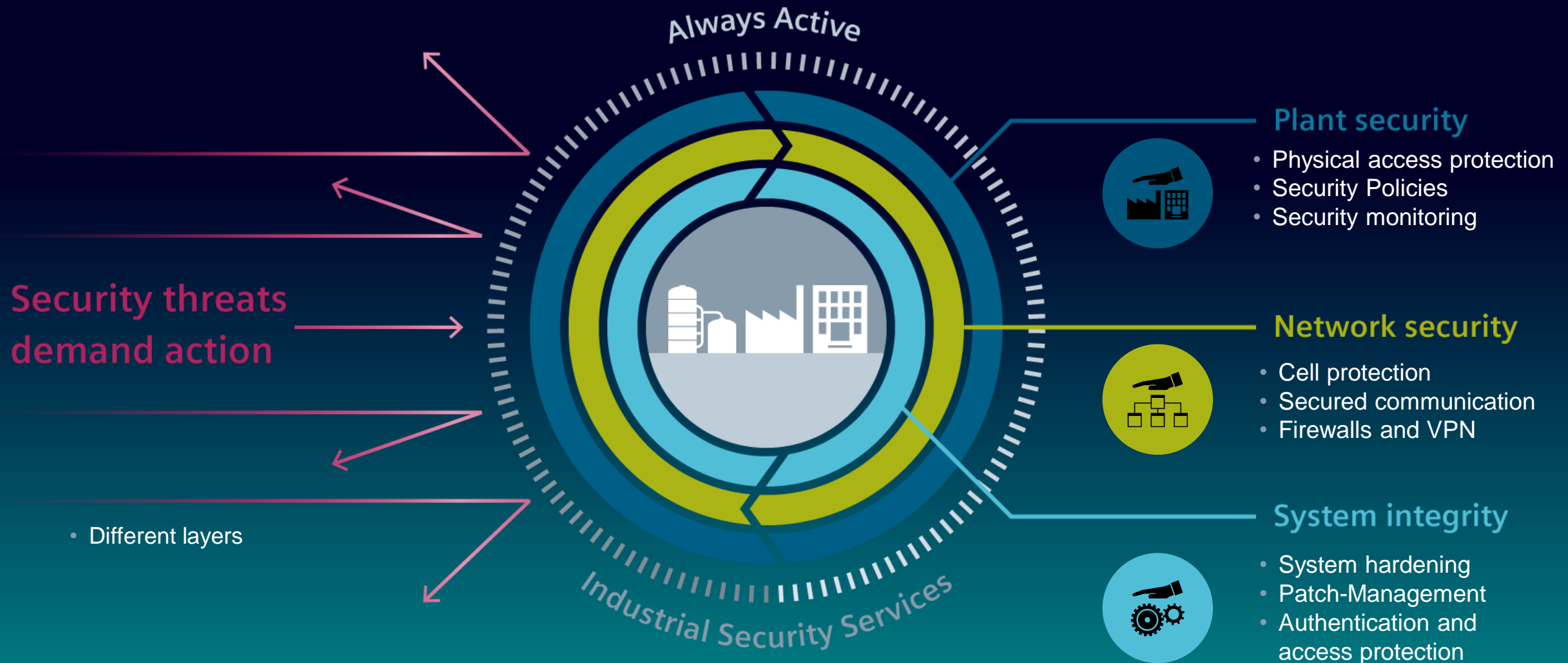
\* New types of entities in electricity: producers, NEMOs, electricity market participants providing aggregation, demand response or energy storage services

\*\* Infrastructure managers and railway undertakings including operators of service facilities (as defined in Directive 2012/34/EU)

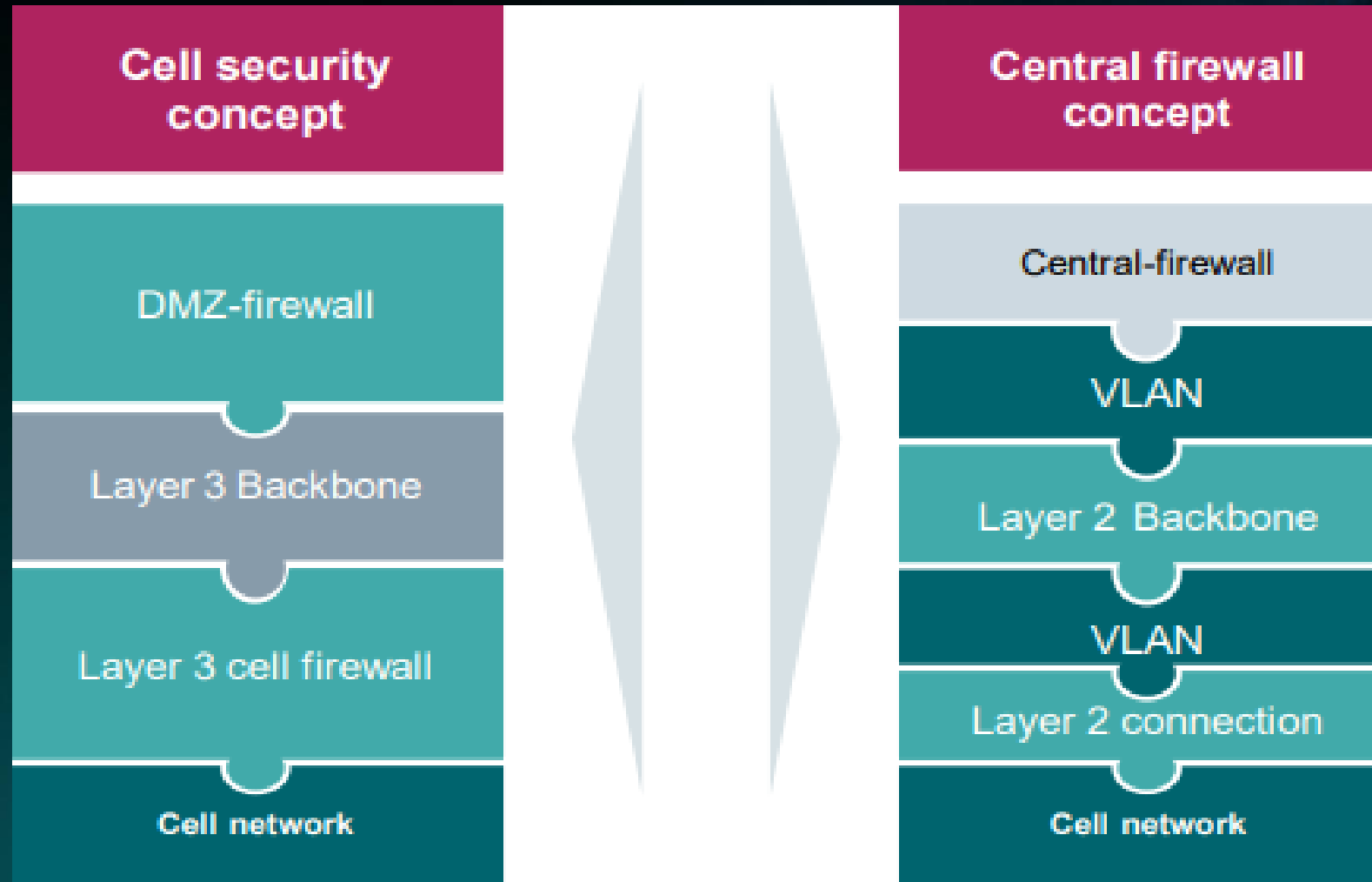
# | Siemens solutions



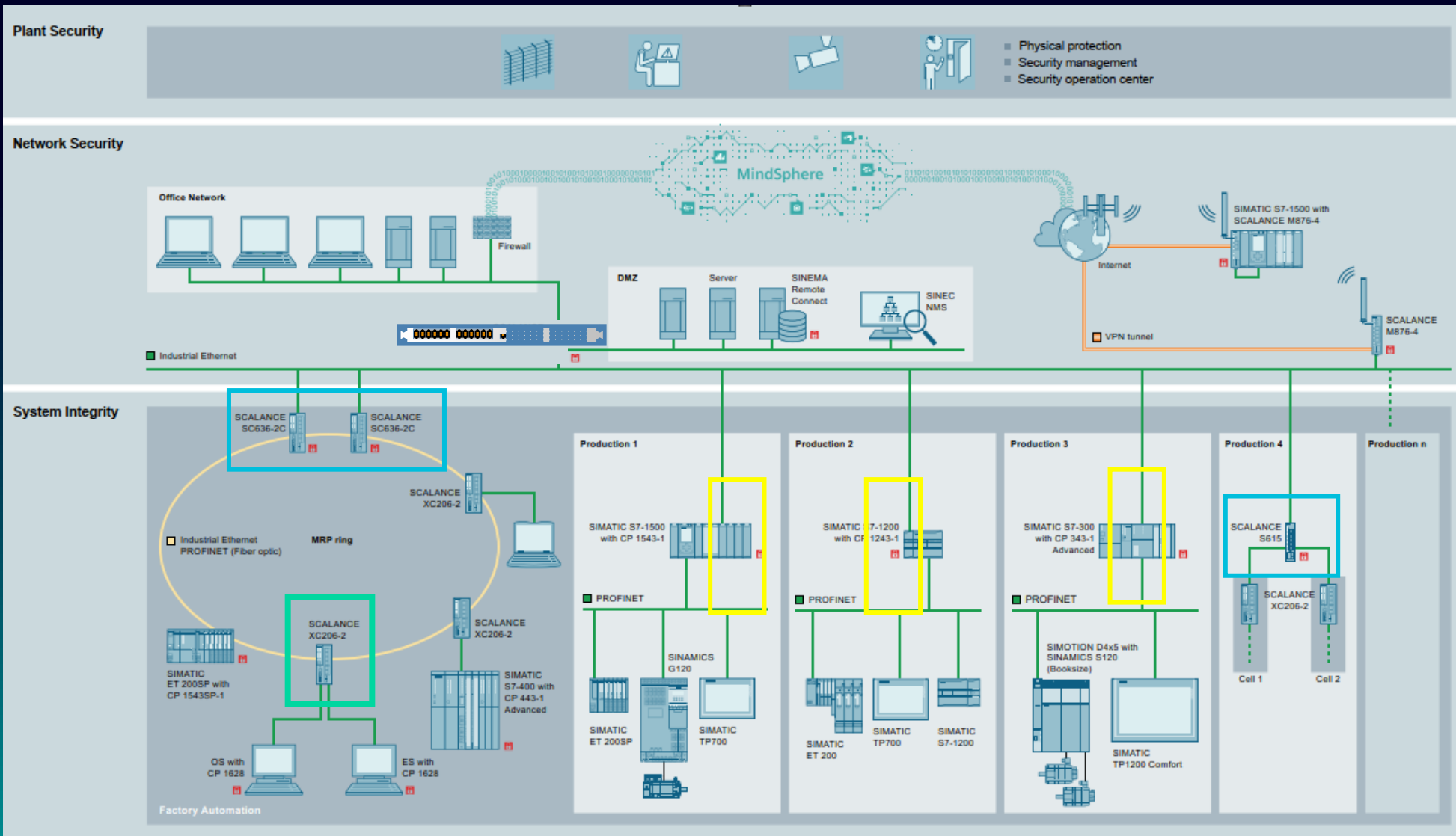
# Our holistic Industrial Security concept



# Bridging of IT&OT: 2 Approaches



## Cell protection with CP card + SCALANCE S

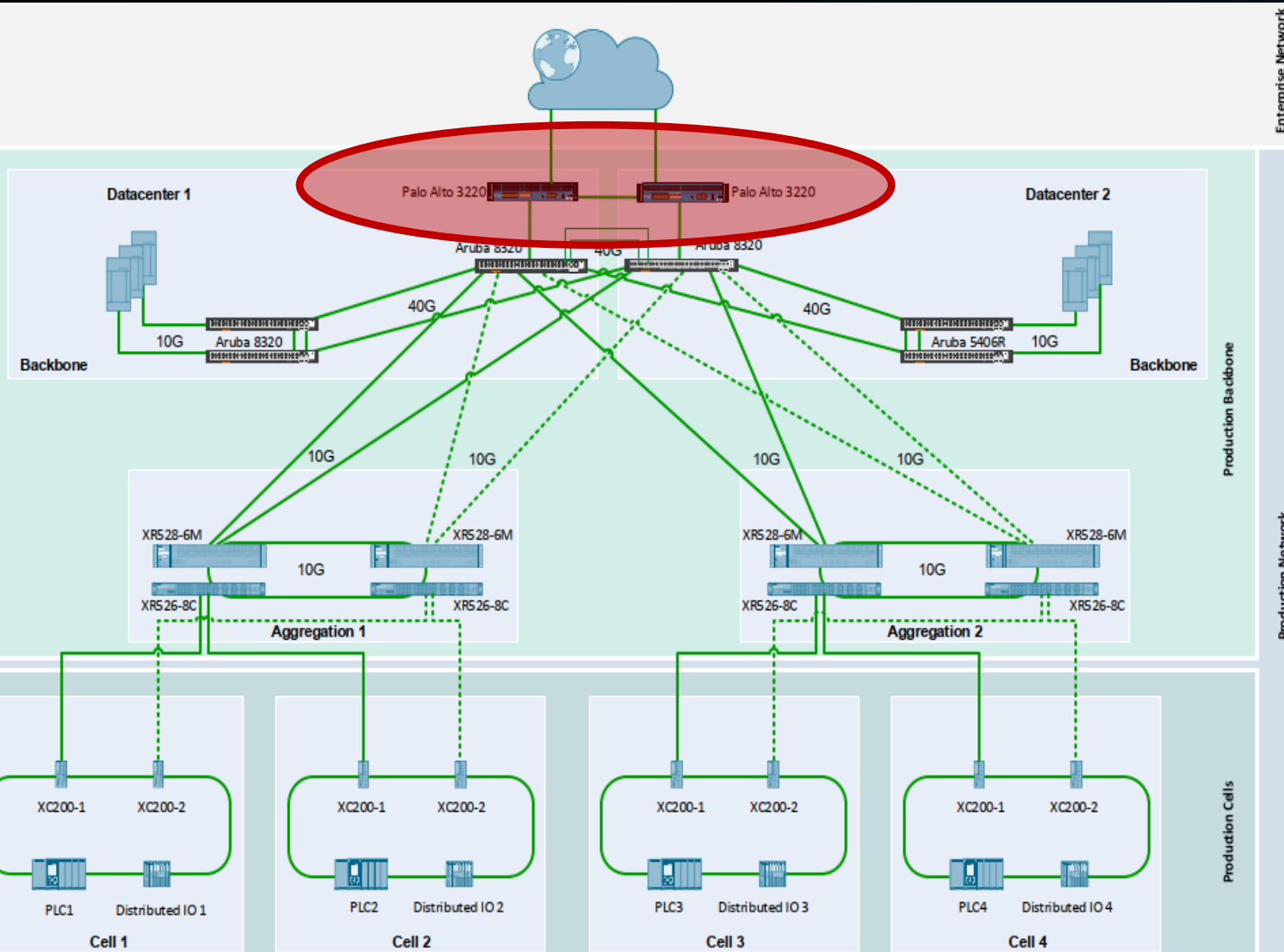


Siemens Certificates  
according IEC 62443  
Product development,  
Security SCALANCE XC-200



# Concept example of bridging the IT/OT network

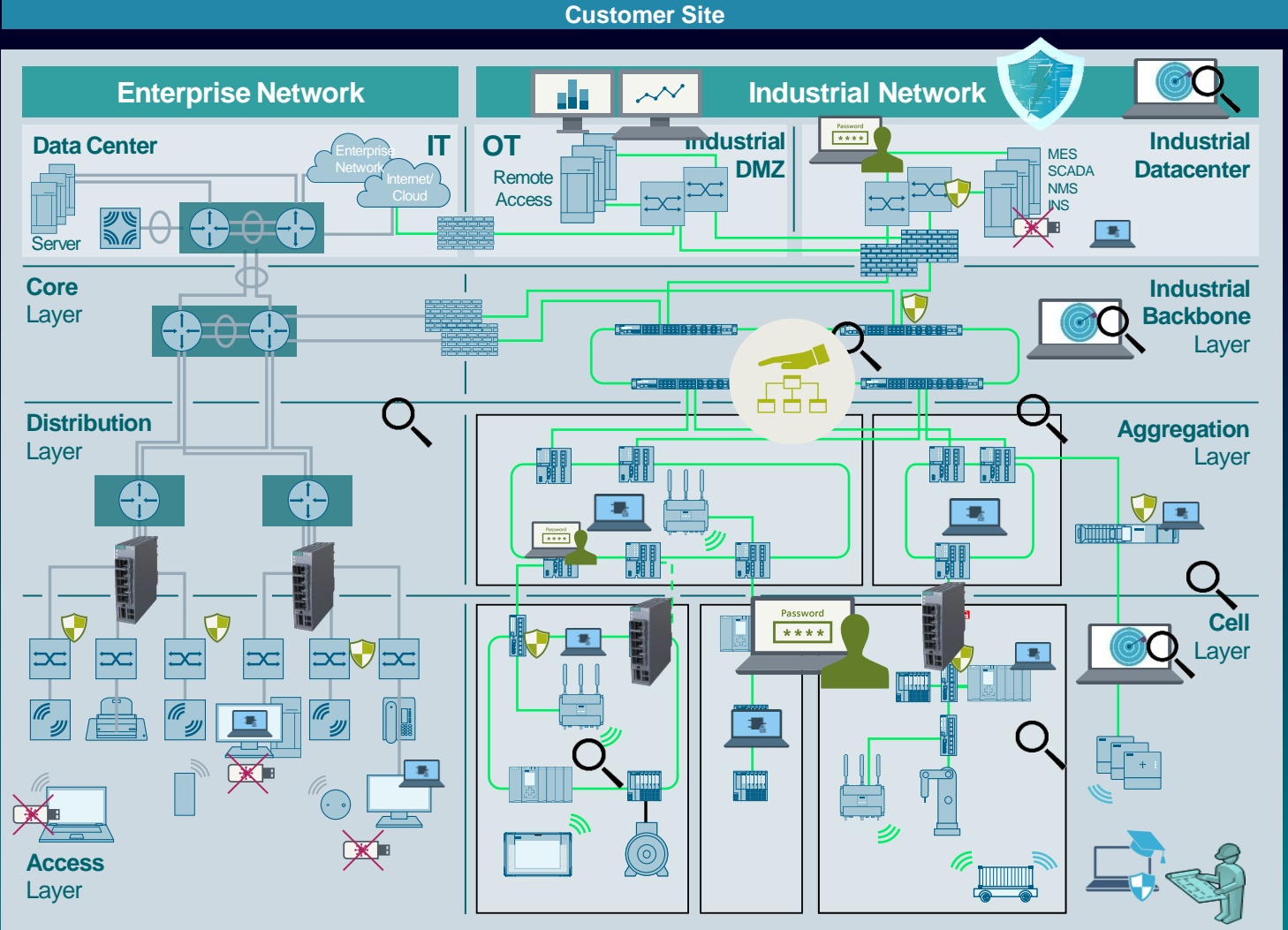
## Central FW Approach












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

# Industrial Security HOW?WHERE?WHAT?

## Implementation Example Scenario



-  **Network Segmentation and DMZ**
-  **Firewalls (NGEN/CELL) and VPN**  
**SCALANCES/Ruggedcom/PaloAlto**
-  **Centralised Mon & Man**  
**SINEC NMS**
-  **Identity and Access Management (UMC, NAC)**
-  **Centralised Patch Management**  
**Backup Mngt**
-  **Industrial Vulnerability Management**
-  **Industrial Anomaly Detection**
-  **System Hardening, Antivirus, Application whitelisting**
-  **Security Assessments**



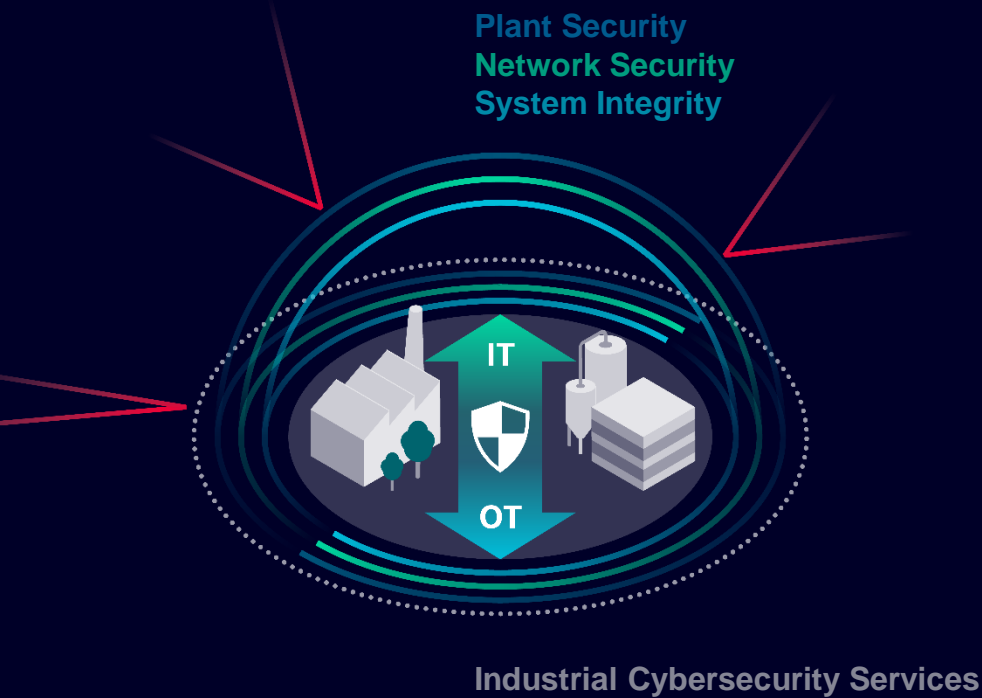
# Industrial Cybersecurity Services



# Cybersecurity for Industry: Offering from Siemens

## Defense in Depth

based on IEC 62443



### Siemens products and systems offer integrated security



Know-how and copy protection



Authentication and user management



Firewall and VPN



System hardening, continuous monitoring and anomaly detection

### Siemens Industrial Cybersecurity Services



Transparency about the current security status



Increased security level by closing security gaps



Long-term protection through continuous security management



# Industrial Cybersecurity Services: End-to-end approach



[www.siemens.com/icss](https://www.siemens.com/icss)

## Plant Security Services

- Security Assessments
- Scanning Services
- Industrial Security Consulting
- Security Awareness Training

*Transparency about the current security status*

## Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Industrial Anomaly Detection
- SINEC NMS

*Increased security level by closing security gaps*

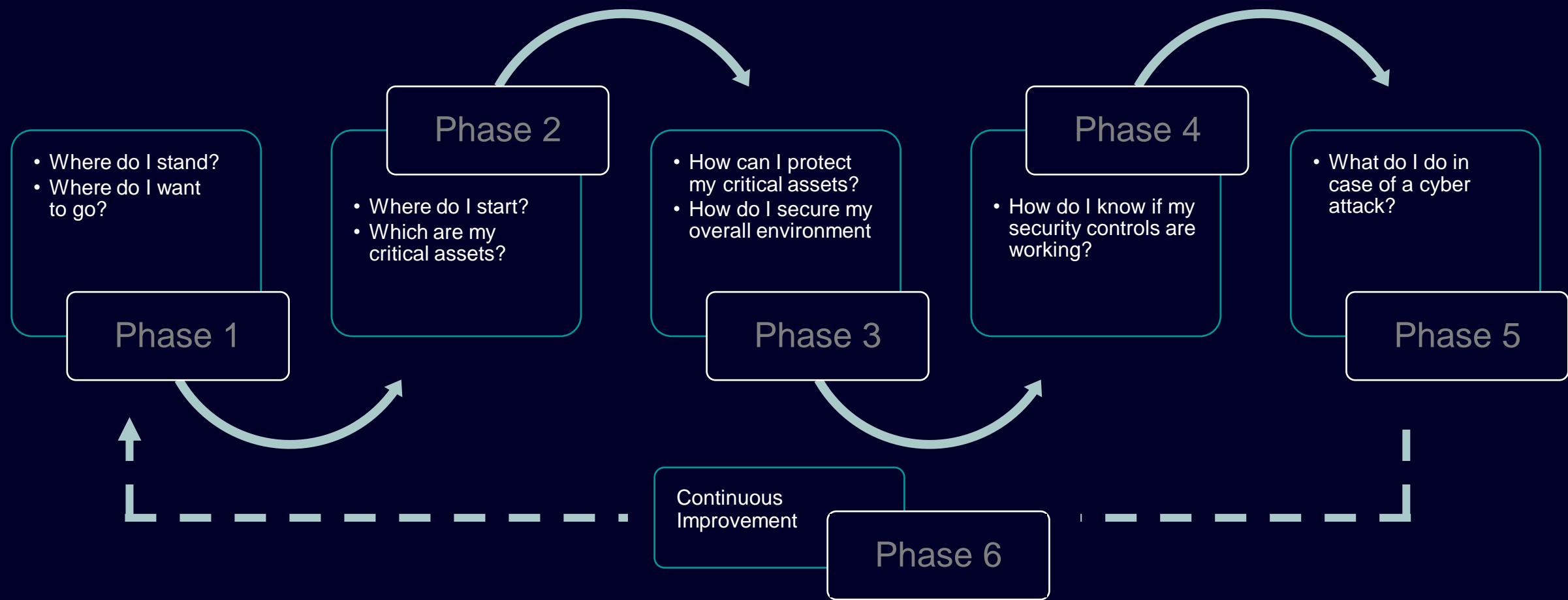
## System Integrity Services

- Endpoint Protection
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC DCS / SCADA Infrastructure
- SIMATIC Security Service Packages

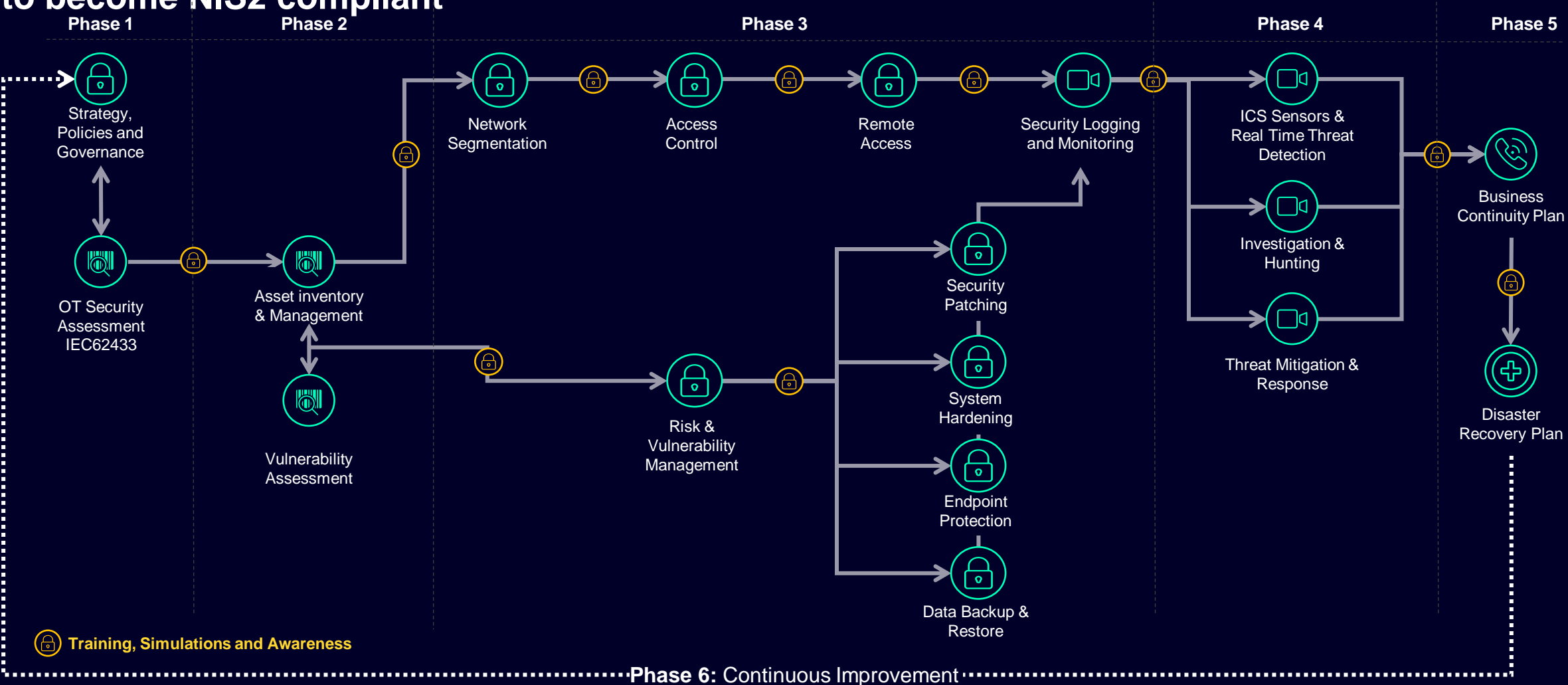
*Long-term protection through continuous security management*

# OT Cybersecurity Program

## How to get started?



# OT Cybersecurity Roadmap to become NIS2 compliant



# | Contact

## Speakers

Gregory Putman  
Sales specialist Industrial Networks & Security  
Mobile +32 499 99 40 30  
E-mail [Gregory.Putman@siemens.com](mailto:Gregory.Putman@siemens.com)



Amaury Poncin  
Sales specialist Digital Enterprise Services  
Mobile +32 474 61 24 56  
E-mail [amaury.Poncin@siemens.com](mailto:amaury.Poncin@siemens.com)



Koen Pauwelyn  
Security Sales Specialist  
Digital Industries – Digital Enterprise Services  
Mobile + 32 476 46 83 37



E-mail [koen.pauwelyn@siemens.com](mailto:koen.pauwelyn@siemens.com)

G. Gezellestraat 121  
1654 Huizingen  
Belgium

[www.siemens.com/icss](http://www.siemens.com/icss)