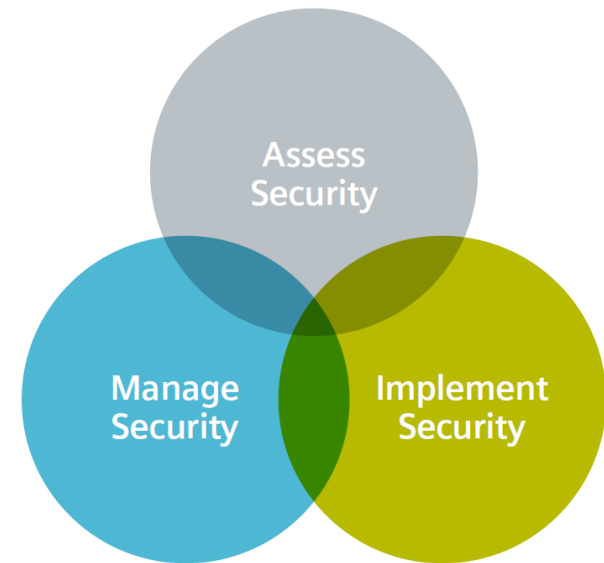


# ICS Cybersecurity Programs for Multi-national Corporations

Kaspersky Industrial Control Systems Cybersecurity  
International Summit: Safeguarding Progress

Melissa Crawford | Plant Security Services | September 28-30, 2017

# Introduction: Siemens Plant Security Services



- Siemens Plant Security Services business provides industrial companies with comprehensive expertise as well as the specialist skills and knowledge of a global network of experts for automation and cyber security.
- The scalable offer includes comprehensive consulting, technical implementation and continuous service (Manage Security). The portfolio is available for existing Siemens plants as well as for technical plants from third-party providers.



**Melissa Crawford**

*Global Cyber Security Consultant for Industrial Control Systems*

- 8 years experience global ICS/SCADA projects
- Responsible for development of cyber security strategies for multinational corporations, IEC62443 Assessments and remote incident handling



**Vladimir Vylkov**

*Principal Cyber Security Consultant*

- >20 Years Experience ICS
- Responsible for global technical consulting, risk and vulnerability assessments, business development activities for global sales



# Overview



- Introduction to MultiNational Corporations 4
- Principles of the ICS cybersecurity Program for MultiNational Corporations 5-8
- Program Rollout and Division of Tasks 9-12
- Maintenance and Monitoring Phase 13
- Reference MNC Examples: Linde and Siemens 14-21
- Closing, Contact & Security Information 22-23

# Multinational Corporations

## Common Characteristics

Production Facilities in multiple countries and continents

- Numerous facilities: 15 to 1000
- Country specific risks and regulations
- Cultural and Language barriers
- Country-specific security level requirements

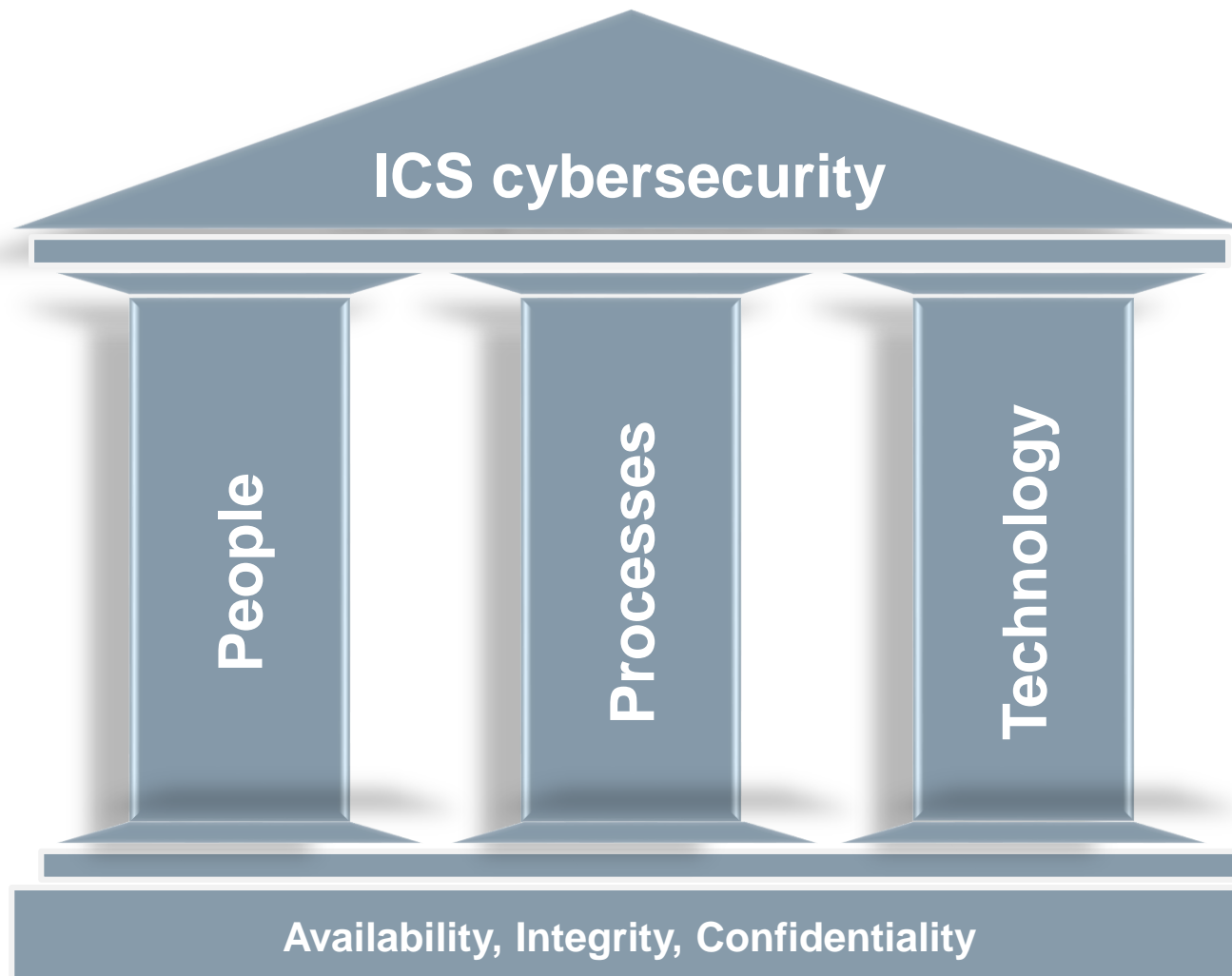
Global Headquarters and regional organizations

Localized operating procedures



Source: Shutterstock

# Pillars of Effective ICS Security Program



## People

- Formation of ICS cybersecurity competence team
- Establishing cybersecurity awareness training program for all plant personnel

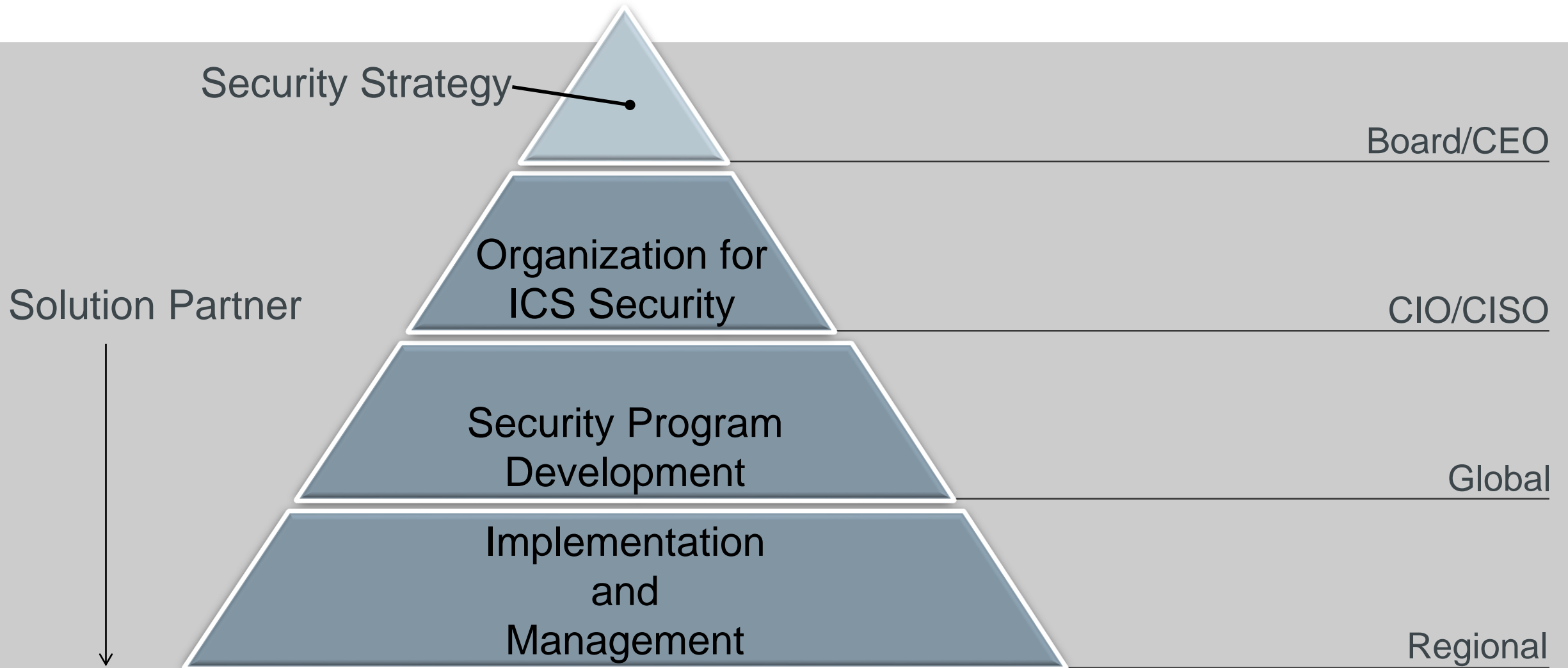
## Processes

- Establishment of effective operational processes and security guidelines

## Technology

- Identification and validation of effective technical security controls
- Continuous monitoring of the plant security and compliance status

# Top-Down Approach: ICS Security Strategy Begins with an Initiative at the Board Level



# Cybersecurity Program Principals: Basic Phases of the Program

## Phase Order

Asset  
Identification  
and Risk  
Assessment

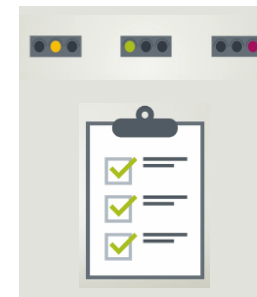
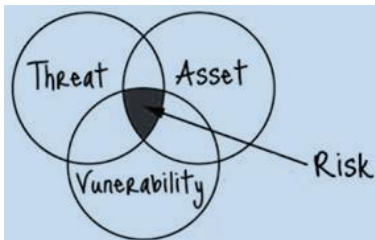
Guideline /  
Policy  
Development

Awareness  
Training and  
Rollout

Governance  
and Follow-  
up Auditing

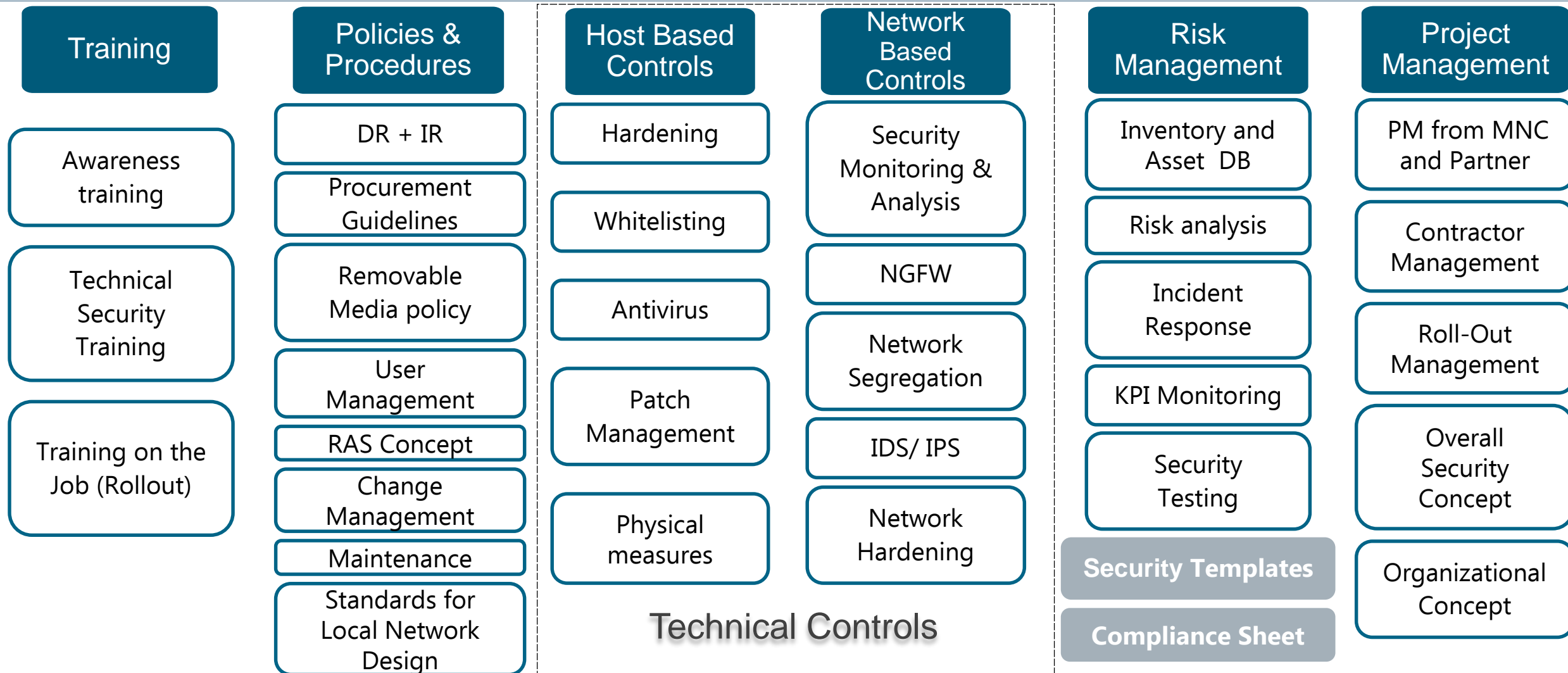
Monitoring  
Center

Built-in  
Lifecycle  
Protection  
Measures





# ICS Cybersecurity Program: Major Elements to be Considered





# Security Rollout – Team Distribution: Take into account Geographical Location, Cultural Variations and Timezones

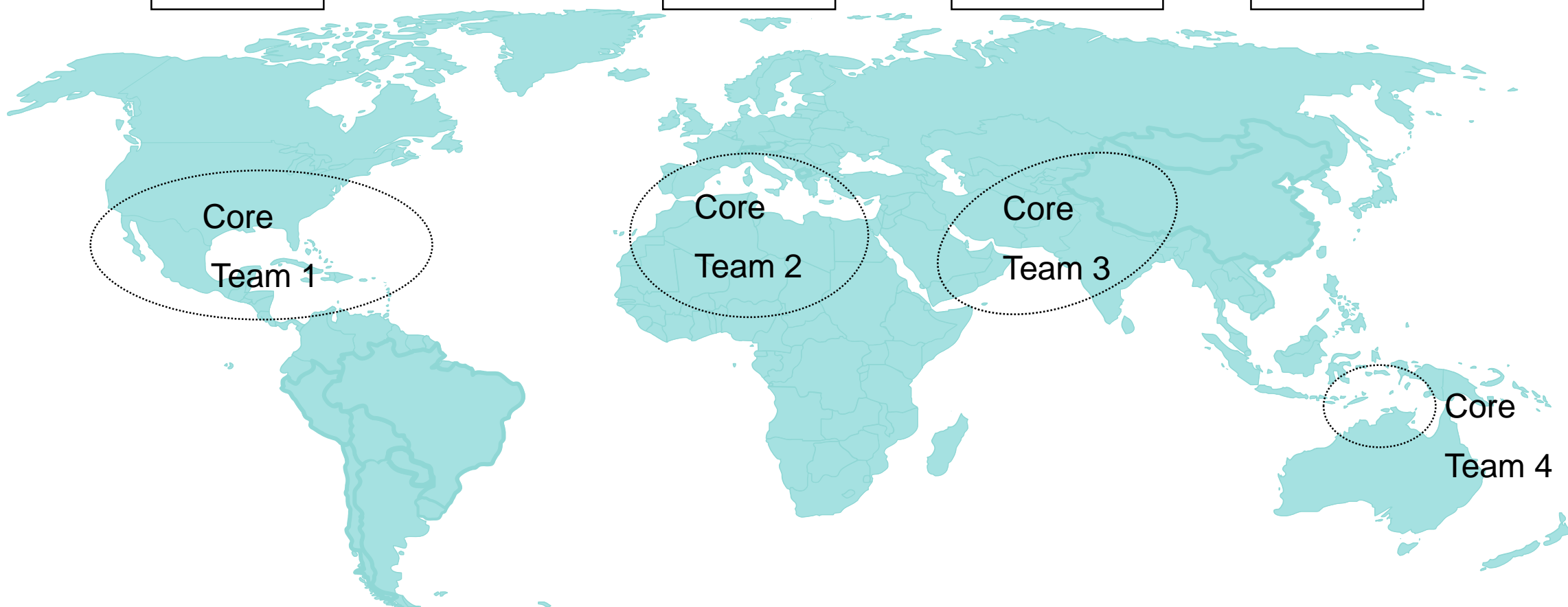
Central Coordination HQ / Project Management

*Americas*

*EMEA*

*Asia*

*Pacific*



# Security Rollout: Ensure Appropriate Skill-set in Forming the Core Teams

## Competence Profile of Core Team (each of the 4 Groups with 4-5 people):



**Industry Expertise**



**Project Management**




**IT Competencies**



**Site Commissioning Experience**



**Network Security Competencies**



**Integration Know-How**

# Implementation: Global and Regional Team Distribution of Tasks

## Global Tasks HQ

- Quality Assurance
  - Single point of contact
  - Ensure quality and check the proper implementation per concept during the global implementation
- Advanced Technical Support
  - Provide specific configuration details
  - Provide support in case of lack of regional resources
  - Coordinate and assess the implementation of measures applying to configuration changes
- Organizational Structure
  - Change Management Consulting
  - Security Integration into Lifecycle Management
- Training
  - Security Awareness Training
  - ICS Security Feature Training for administrators

Information  
Flow

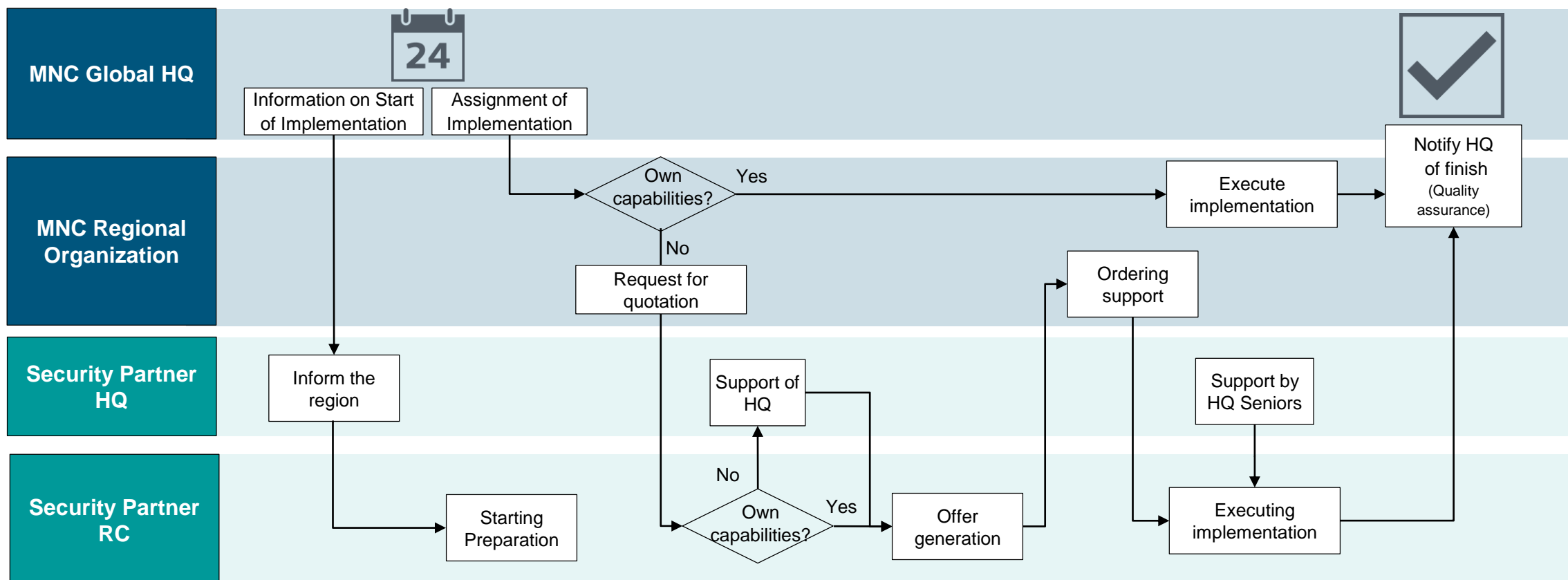


## Regional Team Tasks

- Quality Assurance
  - Single point of contact
  - Ensure quality and check the proper implementation according to **HQ** concept
- Technical Support
  - Implement specific configuration details from **HQ**
  - Get support in case of lack of regional resources from **HQ**
  - Coordinate and assess the implementation of measures applying Engineering Change Requests
- Organizational Structure from the **HQ**
  - Change Management Consulting
  - Security Integration into Lifecycle Management
- Training
  - Security Awareness Training
  - ICS Security Feature Training for administrators
  - Training Plant Personnel on the Job during Installation



# ICS Security Measures Implementation: Security Partner Synchronization



# Maintenance and Monitoring: Continuously Monitor and Adapt the Security Program to the Changing Threat Scenario

## People

- Continuous update of the training contents according to the continuous changing and growing threat landscape

## Processes

- Continuous validation of the effectiveness of the operational processes and security guidelines in place
- Compliance monitoring

## Technology

- Continuous monitoring of the plant security status
- Continuous validation of the effectiveness of the implemented technical security controls



Focus: Ensure risks are appropriately mitigated with effective measures and according with the current threat landscape

# Plant Security Reference

## Linde Gas – Industrial Security Program



### Profile

- The Linde Group is a world leading supplier of industrial, process and specialty gases.
- Linde products and services can be found in nearly every industry, in more than 100 countries.

### Challenge

- Different maturity level for industrial security at Linde Gas
- Need for holistic implementation concept

### Solution

- Development of a comprehensive program for industrial security for >600 production sites and all remote operation centers
- Support of pilot implementation in Region Germany and Asia Pacific

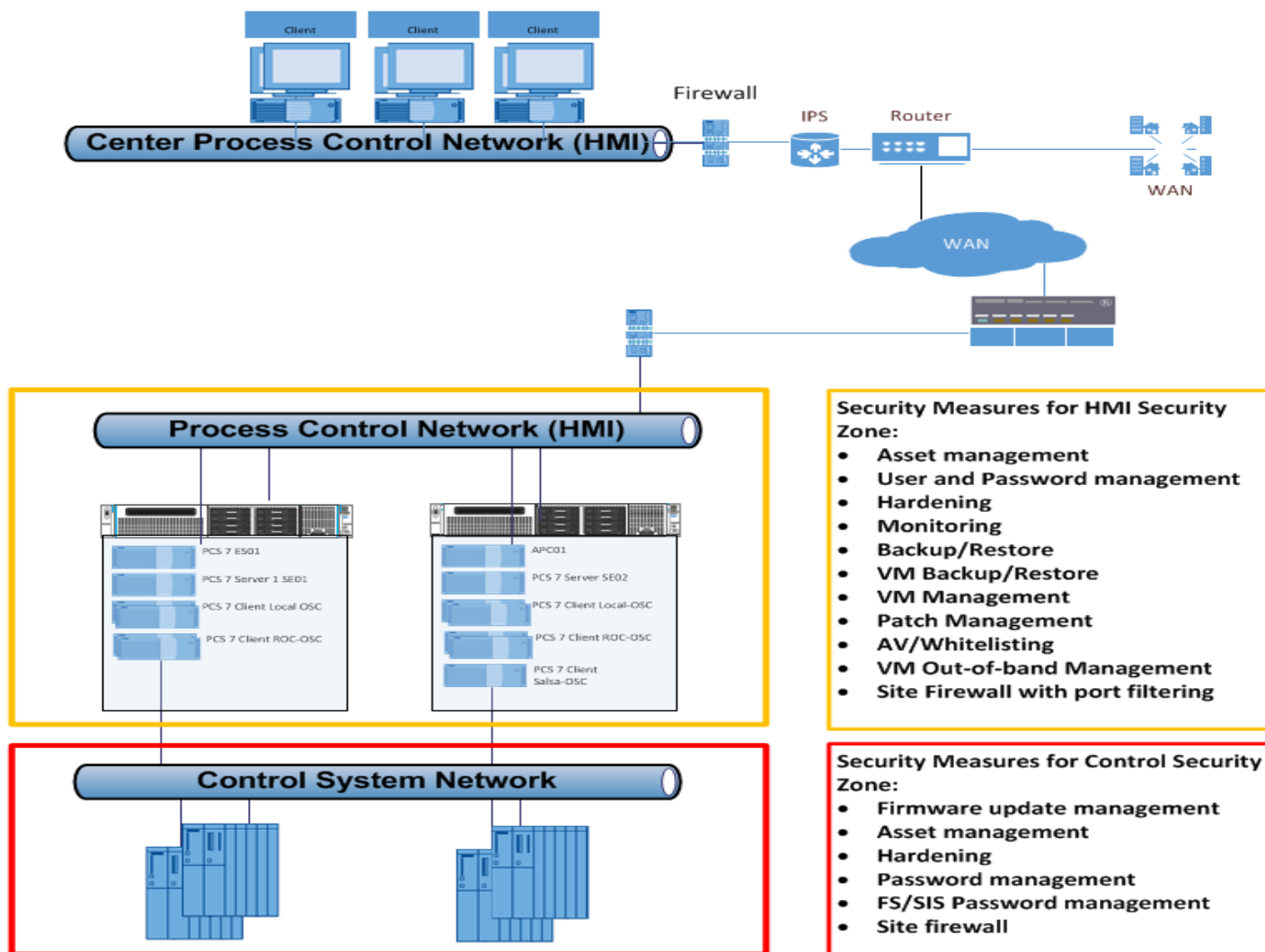
### Customer benefit

- Unified approach for a global roll out to achieve a higher maturity level for Industrial Security
- Cost effective and optimal strategy to deploy on all platforms globally (non-vendor specific)



# Plant Security Reference

## Air Separation Company Examples



# Holistic Security Concept Takes Security on the Next Level - A Holistic Approach for IT and OT

## HSC answers key questions for security in business

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

Identification of the critical business assets is a core component of the concept

### “Which level of security do I need?”

Security level drives requirements, in alignment with IEC 62443, to protect against attacks

### “How do I protect the specific assets?”

Standards based security solutions are applied to protect and monitor the critical assets

## HSC addresses 5 levers including the IT



# Protection Levels are the Key Criteria and Cover Security Functionalities and Processes

## Security functions

- Based on IEC 62443-3-3
- Security Level 1-4

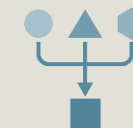


## Protection Level (PL)

Maturity Level	4					PL 1
	3					PL 2
	2					PL 3
	1					PL 4
		1	2	3	4	
		Security Level				

## Security process

- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4



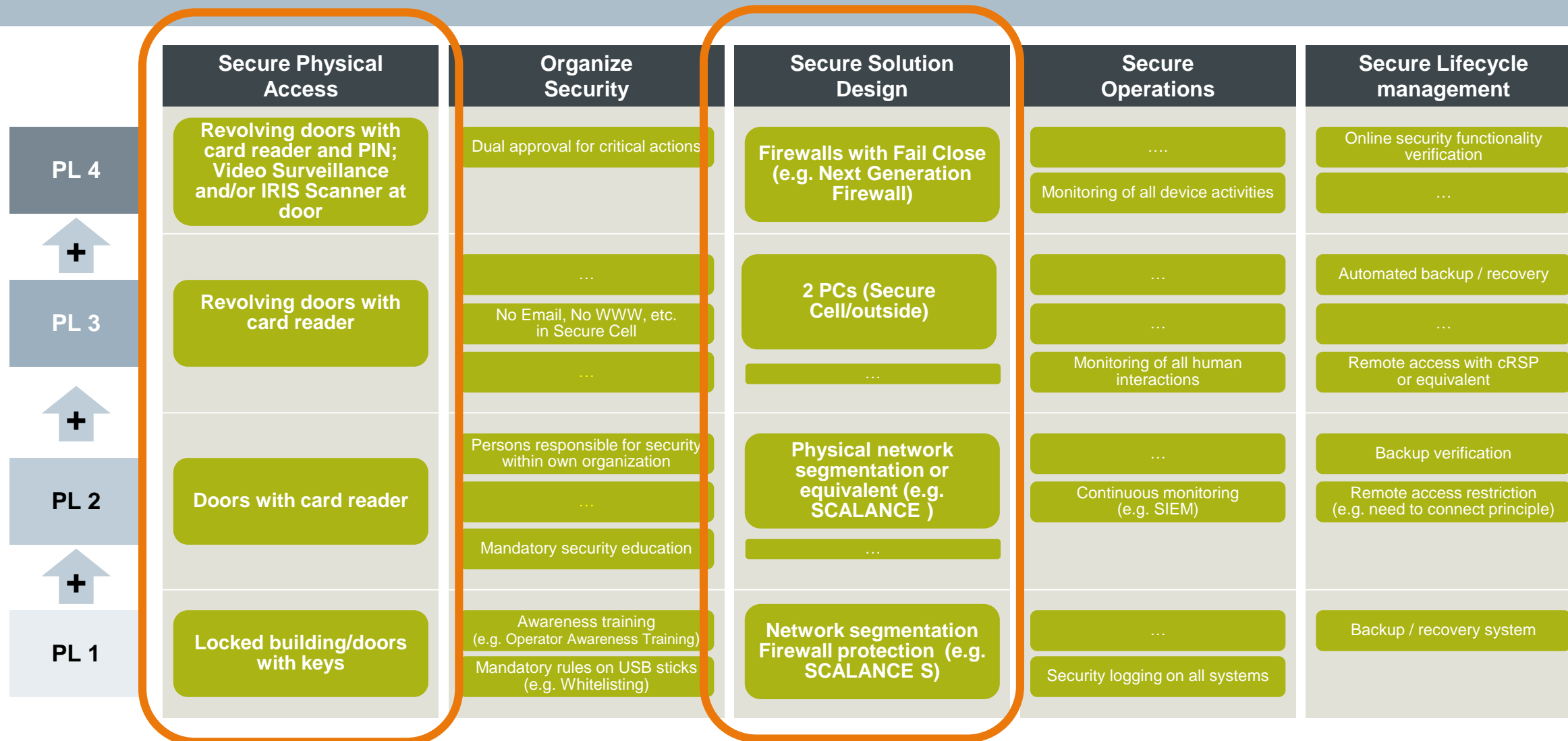


# Security in Siemens Production

- Siemens has defined a Holistic Security Concept (HSC) based upon IEC 62443 & ISO 27000
- HSC protects integrity and safeguards confidentiality of the development and manufacturing environment
- HSC measures are defined and monitored in development and production departments



# Selected HSC Security Measures from PL 1 to PL 4



# Elektronikwerk Amberg

## Implementation and operation of Industrial Security Monitoring



### Profil

Elektronikwerk Amberg is a prime example of a digital factory. The factory uses cutting-edge technologies to produce approximately fifteen million SIMATIC products each year.

### Challenge

- Highly sensitive IT-controlled processes
- Fully networked automation environment
- Comprehensive data flow and database
- Protection against industrial espionage, manipulation and hacker activities

### Solution

- Implementation of Defense in Depth with S7-1500 and SCALANCE S using TIA Portal.
- Monitoring of security-relevant events
- Monthly status report on plant and system security
- Recommendations for optimizing the level of protection

### Customer benefit

- Protection of networks and TIA components according to the defense-in-depth security concept
- Solid, in-depth security information thanks to Security Information and Event Management (SIEM)
- Continuous optimization of the security concept



# Plant Security Services Reference

## Sinopec Qingdao Refinery – Secure PCS 7 solution



### Profile

- The Sinopec Qingdao Refinery is a super-large refining and petrochemical complex with a distillation capacity of 10 million tons per year
- It produces gasoline, kerosene, diesel, LPG, polypropylene and styrene

### Challenge

- Operations without disturbances: Protect against all kind of disturbing viruses
- Smooth implementation
- Largest standalone industrial security project worldwide

### Solution

- Development of a security solution for the PCS 7 environment including DMZ, Firewall, Anti-Virus, Patch Management, User Management and System hardening
- 2 weeks implementation during downtime of the plant

### Customer benefit

- Continuous protection of plant: reduce risk and maintain production availability
- Zero incidents or infections after the project: 18 months of safe operation
- Blueprint for Chinese petrochemical customers

# Closing Remarks, Questions, Contact



## **Siemens AG**

Digital Factory  
DF CS DS

Postbox 3240  
91050 Erlangen  
GERMANY

## **Melissa Crawford**

Global cybersecurity Consultant for Industrial Control Systems  
Digital Factory / DE / Plant Security Services

E-mail: [melissa.crawford@siemens.com](mailto:melissa.crawford@siemens.com)

**[siemens.com/plant-security-services](https://siemens.com/plant-security-services)**

# Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit **<http://www.siemens.com/industrialsecurity>**.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **<http://www.siemens.com/industrialsecurity>**.