food & drink federation
passionate about food & drink

WELCOME

Cyber Security
in the Food & Drink Industry

3 March 2021

@foodanddrinkfed
#FDFCyberSecurity

Current risks to the entire Supply Chain

NCSC Representative

National Cyber Security Centre

National Cyber Security Centre

UK National Technical Authority for Cyber Security

Helping to Make the UK the Safest Place to Live and Work Online

National Cyber Security Centre

National Cyber Security Centre

Connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack.

By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation).

Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

National Cyber Security Centre

What is the risk?

Networks need to be protected against both internal and external threats. Organisations that fail to protect their networks appropriately could be subject to a number of risks, including:

- Exploitation of systems
- Compromise of Information
- Import and export of malware
- Denial of service
- Damage or defacement of corporate resources

National Cyber Security Centre

Supply Chain

Most organisations will have a number of suppliers to deliver products, systems, and services but do you know what security systems they use?

Very few UK businesses set minimum security standards for their suppliers

Be aware of who may contract out to 3rd Parties

National Cyber Security Centre

Organisations Online

New Dependencies- placing more reliance on digital technology, including online services

Service agreements - It's worth reading these to be sure your have the resources in place that you think you do.

Securing devices and services - staff may need to use their own devices to access services and data, which will present new risks

Our Small Business Guide gives you five tips that will help protect your business from malware attacks. For larger organisations, the NCSC also provides detailed guidance on mobile device management, which includes BYOD approaches.

National Cyber Security Centre

five tips that will help protect your business from malware attacks

Tip 1: Install (and turn on) antivirus software

Tip 2: Prevent staff from downloading dodgy apps

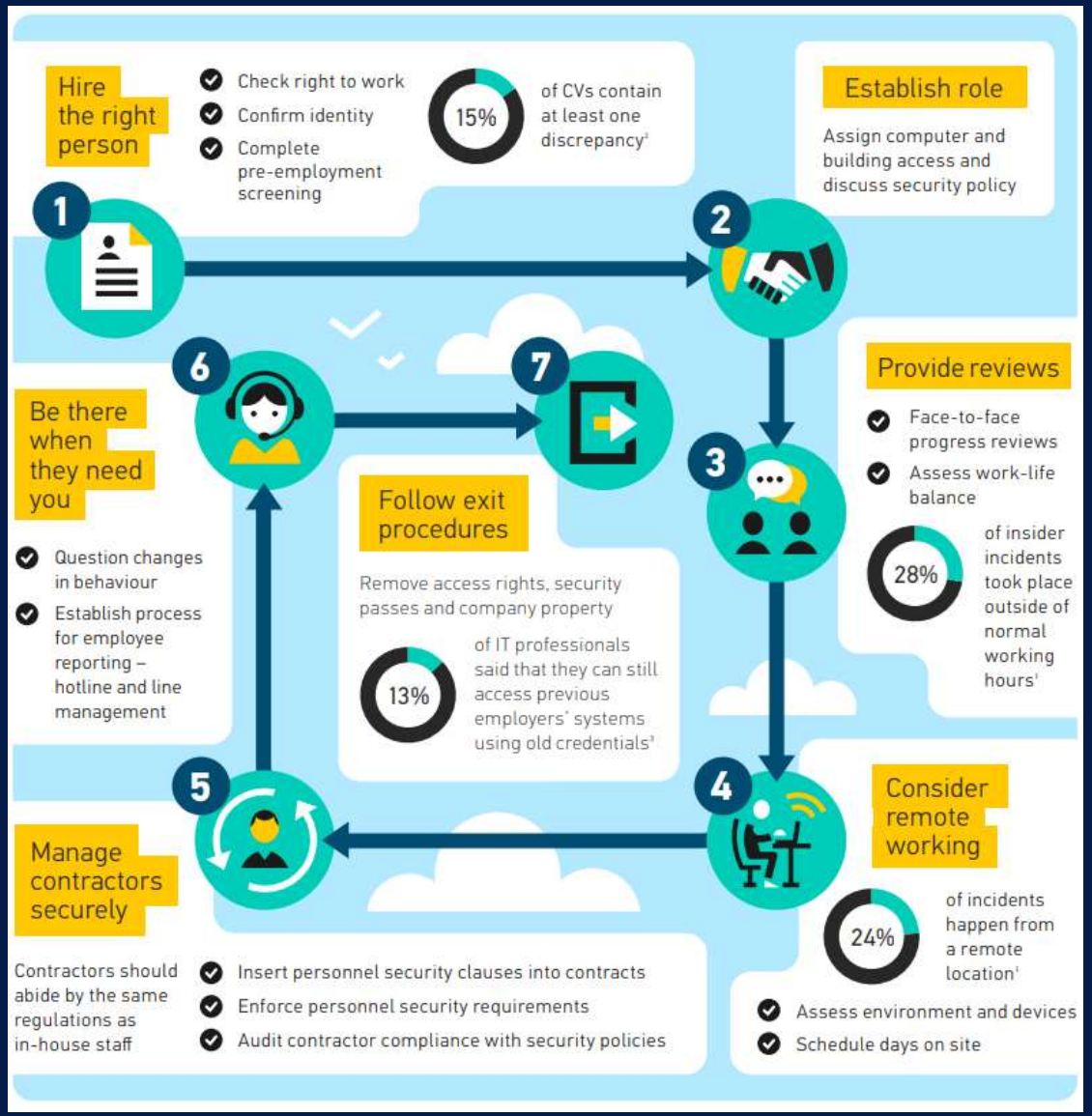
Tip 3: Keep all your IT equipment up to date (patching)

Tip 4: Control how USB drives (and memory cards) can be used

Tip 5: Switch on your firewall

National Cyber Security Centre

Personnel Security



National Cyber Security Centre

What are the benefits to good cyber security?

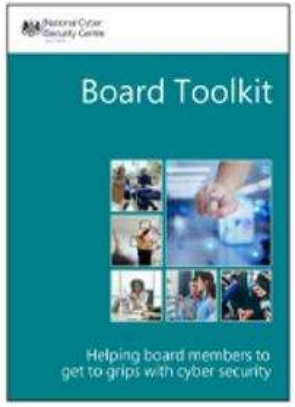
National Cyber Security Centre

- Better protect yourself, your employees and business against cyber crime
- Provide your customers with more confidence
- Empower staff to raise concerns

And….

- Everyone can do it

Top Tips for Staff



Board Toolkit

National Cyber Security Centre
a part of GCHQ

Small Business Guide & Actions

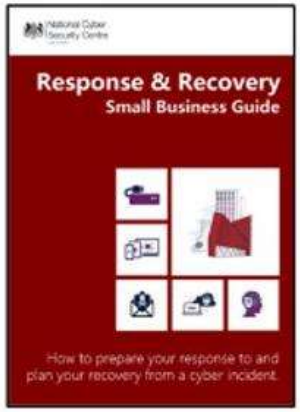
SME Newsletter

Cyber Essentials (Plus)

Cyber Aware

Exercise in a Box

NCSC Website



Response & Recovery Small Business Guide

National Cyber Security Centre

Guidance

Small Business Guide - How to improve your cyber security; affordable, practical advice for businesses.

Response & Recovery Guide - Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.

Top Tips for Staff - The NCSC's e-learning package 'Top Tips For Staff' can be completed online, or built into your own training platform.

Exercise in a Box – A free online tool which helps organisations find out how resilient they are to cyber-attacks and practise their response in a safe environment

Cyber Essentials – Cyber Essentials government backed certification scheme helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security.

National Cyber Security Centre

Thank you.

www.ncsc.gov.uk

enquiries@ncsc.gov.uk

@NCSC

National Cyber Security Centre

CyberHQ

Industrial Security

Driving Digitalisation for Food & Beverage

Paul Hingley
Principal Product Security &
Solution Officer
Siemens Digital Industries GB&I

Industrial Security

Driving Digitalisation for Food & Beverage

F&D Cyber Security Conference 2021

SIEMENS

Siemens is with its Digital Enterprise, “The innovation leader” for discrete, hybrid and process industries

Digitalization

Automation

Electrification

Digital Enterprise

Process industries | **Discrete industries**

Design | Planning | Engineering | Production | Services

Automation and industrial software for the process industries	**Industrial communication** **Industrial security** **Industrial services**	**Automation and industrial software for the discrete industries**

> 10 billion investment in M&A since 2007

Why is Industrial Security so important?

Internet of Things

Secure

Benefits of Industry 4.0 must be ensured with industrial security

Vulnerabilities

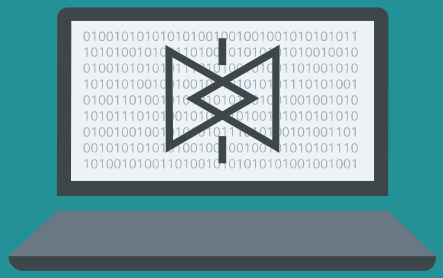
in processes and systems

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……

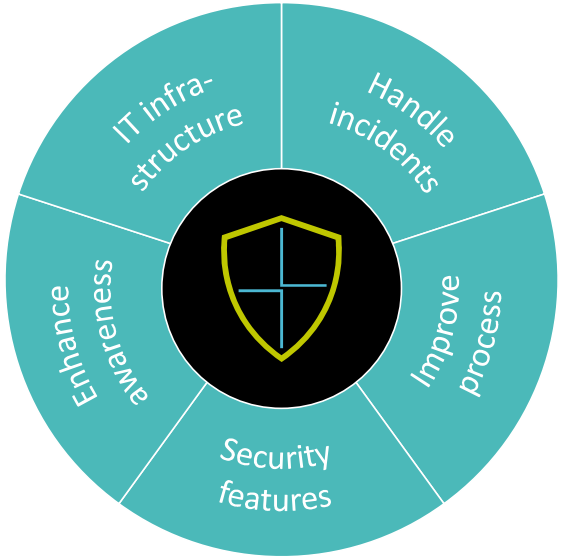
SIEMENS
Ingenuity for life

… 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?”



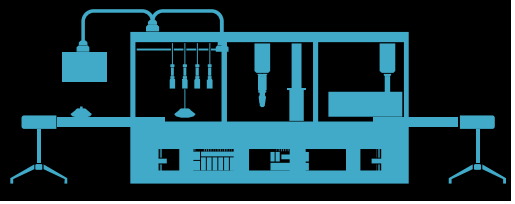
A view from the industry specific perspective
What is important for F&B customers?

SIEMENS
Ingenuity for life

Food and beverage

Secure all assets to ensure:

- Food safety and product integrity
- Plant availability
- Traceability throughout the entire production process
- Productivity, efficiency and flexibility
- Time to market reduction



Industrial Security
From what to be protected?

SIEMENS
Ingenuity for life

Protect from cyberattacks trends (e.g. Ransomware)

Deploy ransomware on a PC via mail, USB, etc.

Lock the system with the ransomware

Claim money from PC owner for unlocking

Deliver key to unlock the system

Food & Beverage Industry – is also a “Prime Target” for Cyberattacks exploiting Vulnerabilities

SIEMENS
Ingenuity for life

Reduce unplanned costs and losses

Production halted at a Cadbury factory in Tasmania

- Cadbury - Mondelez infected by ransomware („NotPetya attack“)
- The attack impacted on company growth - drop in a 3% in second quarter of 2017 meaning $100 M in losses

Ransomware attack to Arizona Beverages (iEncrypt)

- Caused over 200 networked computers and servers offline
- The attack halted sales operations for days costing millions of USD
- The company struggle to recover still two weeks later

https://www.abc.net.au/news/2017-06-28/cadbury-chocolate-factory-targeted-in-ransomware-attack/8658222

https://securityboulevard.com/2019/04/arizona-beverages-ransomware-attack-halts-sales-for-days/

Food & Beverage Industry – is also regulated and must comply with Security Standards

SIEMENS
Ingenuity for life

Comply with industry regulations

- Regional government regulation authorities:
  - BSI / KRITIS in Germany
  - DHS / NIPP in USA
  - NCSC in UK
- Security Standards:
  - ISA/IEC-62443, ISO-27001, NIST

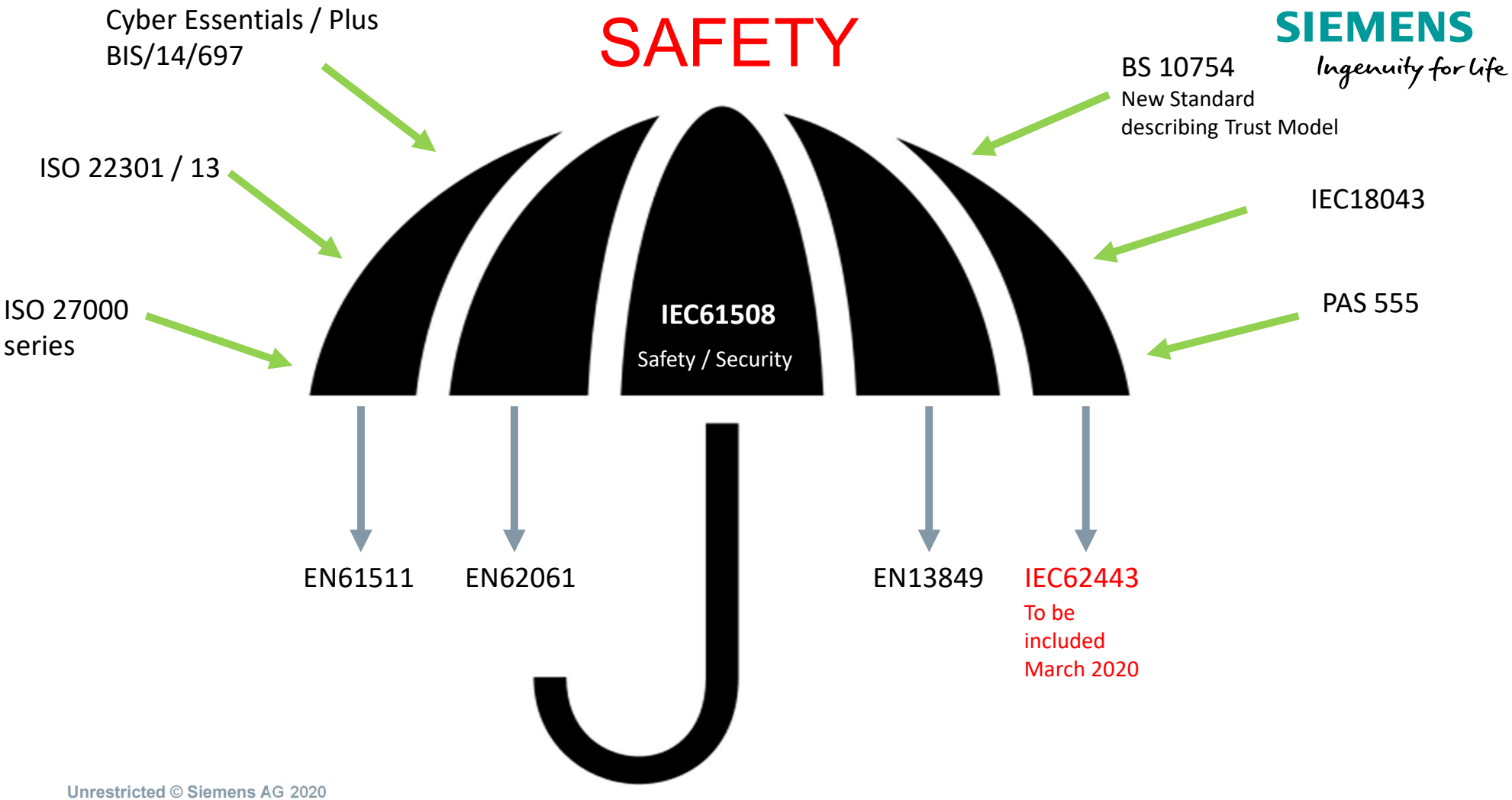
BSI: Federal Office for Information Security
DHS: Department of Homeland Security
CPNI: Centre for the Protection of National Infrastructure

KRITIS: Kritischer Infrastruktur
NIPP: National Infrastructure Protection Plan

ISA: International Society of Automation
IEC: International Electrotechnical Commision
ISO: International Organization for Standardization
NIST: National Institute of Standards and Technlogy

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

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

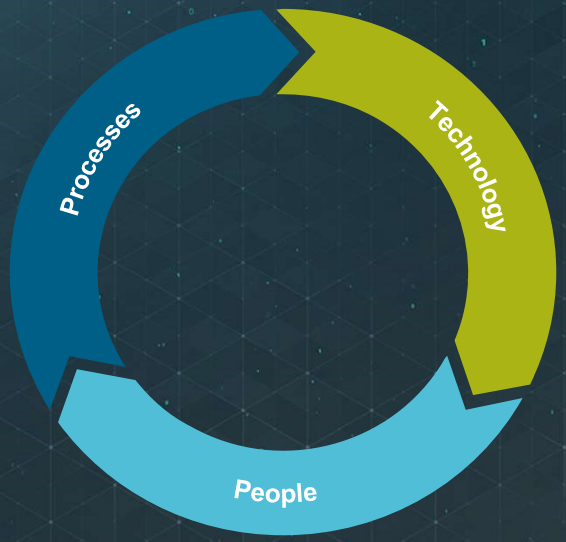


Security standards are about technology, processes and people

What must be done?

Policies and procedures

Functional security measures



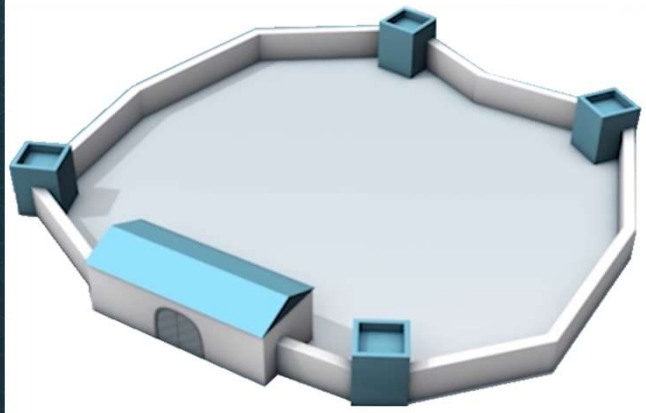
Competency

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

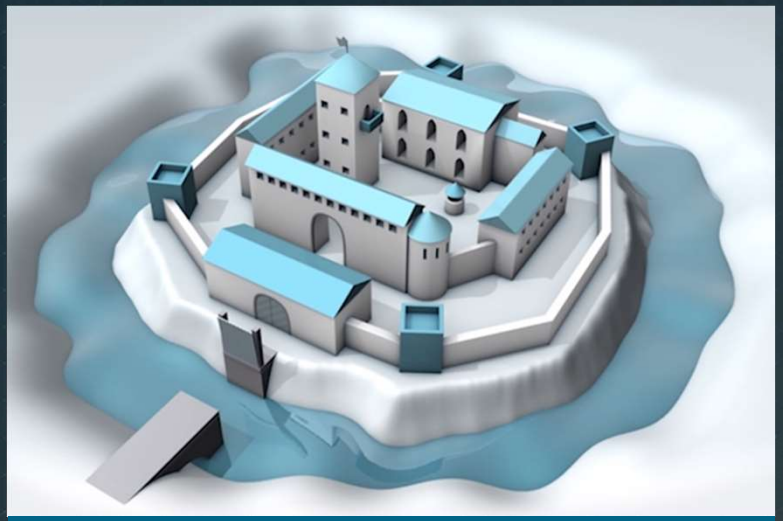
The key to a secure infrastructure:
Defense in depth

Great wall

- Impenetrable wall
- One-layer protection
- One point of attack



A single layer of defense does not provide adequate protection!



Defense in depth

- Multi-layer protection
- Each layer protects the other layers
- An attacker must spend time and effort at each transition

Industrial Security – from risk to resilience

SIEMENS
Ingenuity for life

Unprotected business

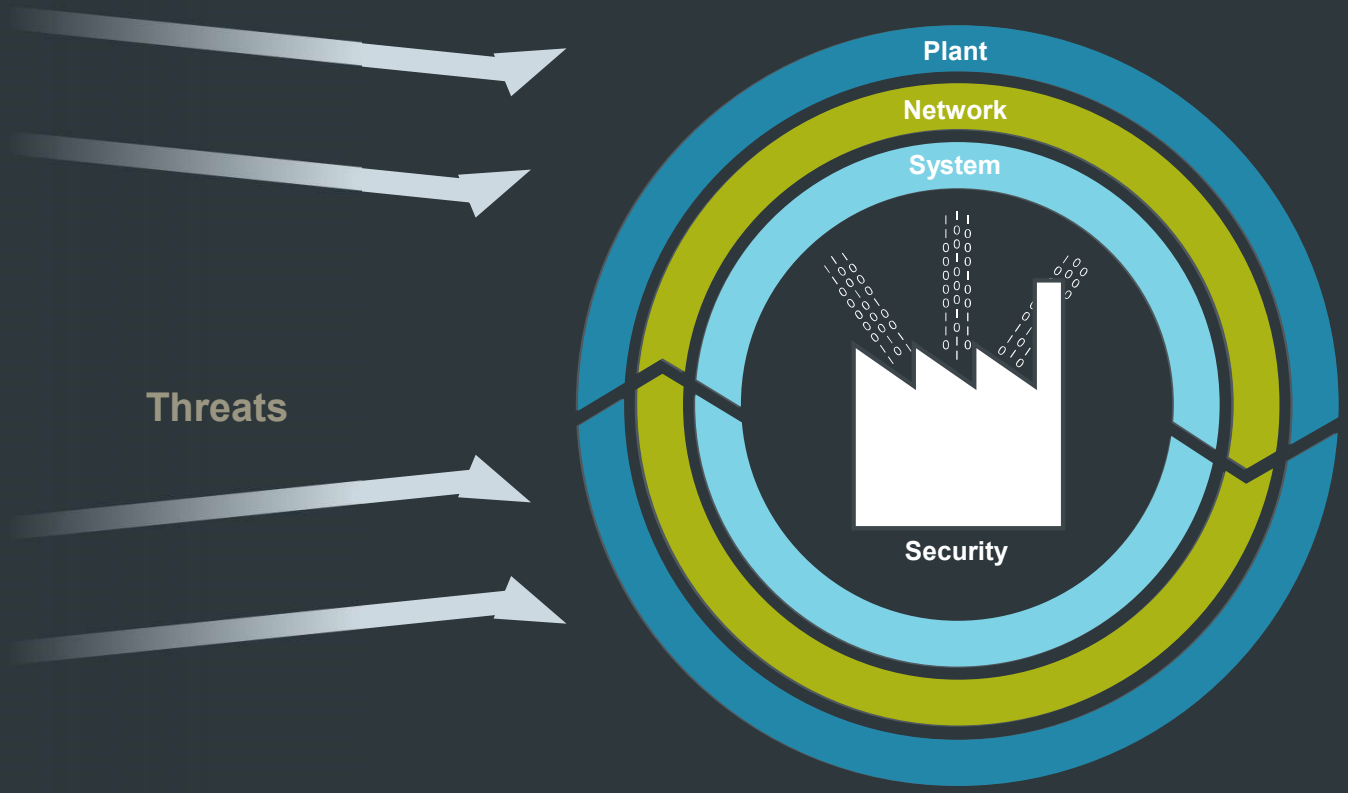
- People and assets exposed to risk
- Business vulnerable to disruptions, sabotage and theft
- Costs and liability
- Reputational damage

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

SIEMENS Defense-in-Depth-Concept (based on IEC 62443)



Plant security

- Physical access protection
- Processes and guidelines
- Holistic security monitoring

Network security

- Cell protection
- Perimeter protection
- Firewalls and VPN

System integrity

- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Siemens Industrial Security approach based on
IEC 62443 addressing the Defense in Depth concept

Main parts of IEC 62443

IEC 62443

Asset Owner

2-1, 2-4

Operational and Maintenances policies and procedures

System Integrator

2-4, 3-2, 3-3

Policies and procedures

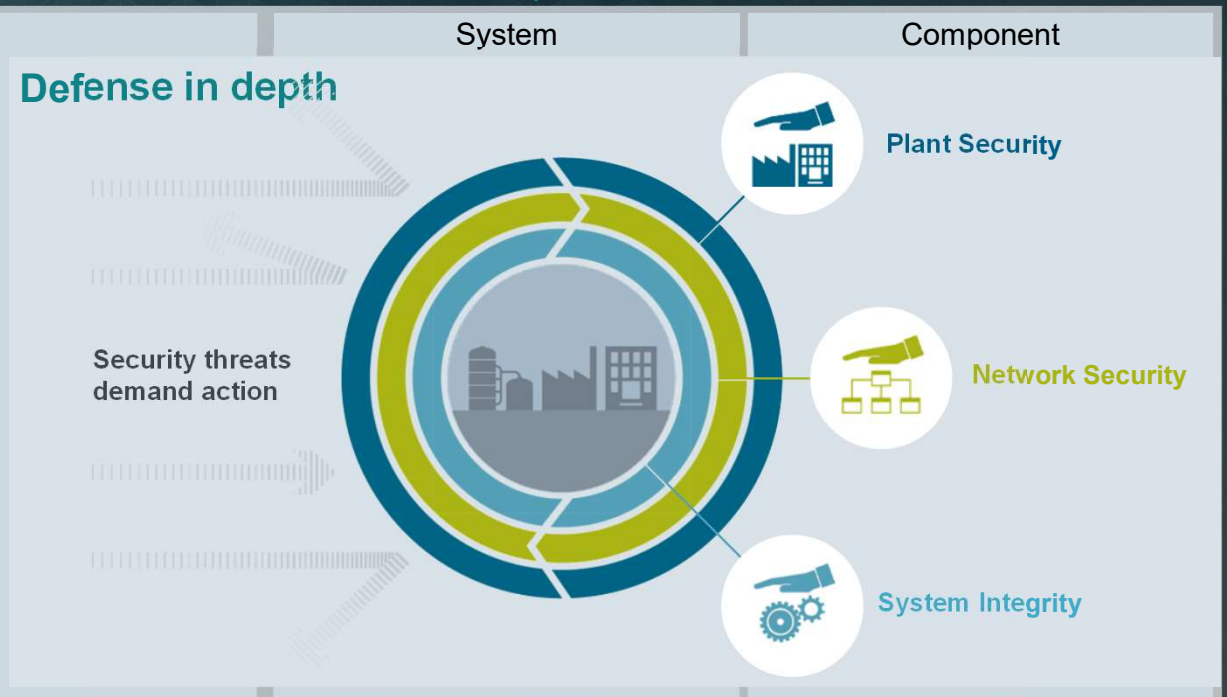
Security capabilities of the Automation Solution

Product Supplier

3-3, 4-2, 4-1

Security capabilities of the products

Development process



'Defense in Depth' involves all stakeholders: Asset Owner, System Integrator, Product Supplier

Security conformance
What is the structure of IEC 62443?

Industrial communication networks – Network and system security

IEC 62443

1-1 General
Terminology, concepts and models

1-2 General
Master glossary of terms and abbreviations

1-3 General
System security compliance metrics

2-1 Policies and procedures
Establishing an IACS security program

2-2 Policies and procedures
Operating an IACS security program

2-3 Policies and procedures
Patch management in the IACS environment

2-4 Policies and procedures
Certification of IACS supplier security policies

3-1 System
Security technologies for IACS

3-2 System
Security assurance levels for zones and conduits

3-3 System
System sec. requirements and security assurance levels

4-1 Component
Product development requirements

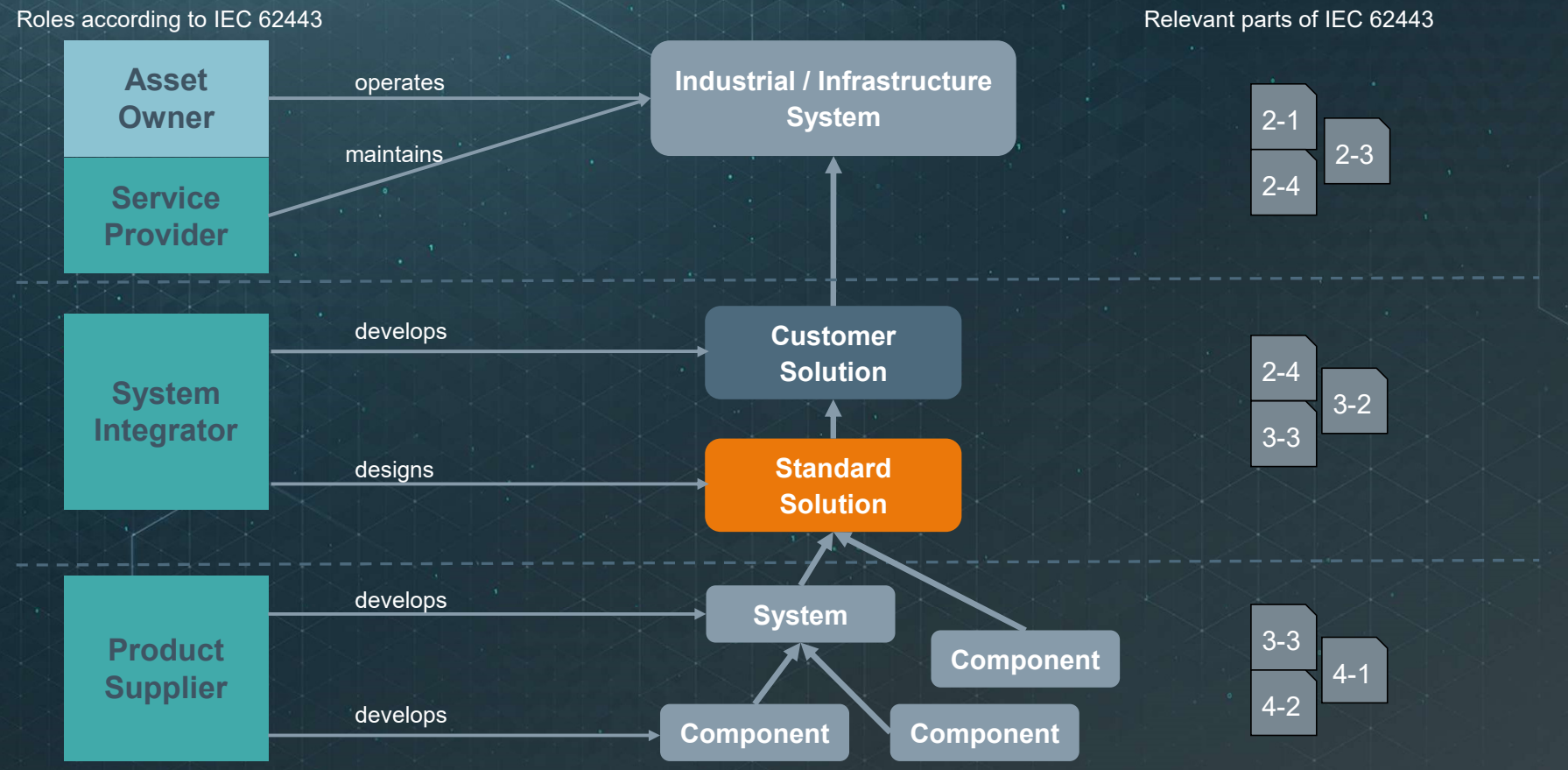
4-2 Component
Technical sec. requirements for IACS products

Definition and metrics

Processes / procedures

Functional requirements

IEC 62443 Roles and Responsibilities



Industrial Security

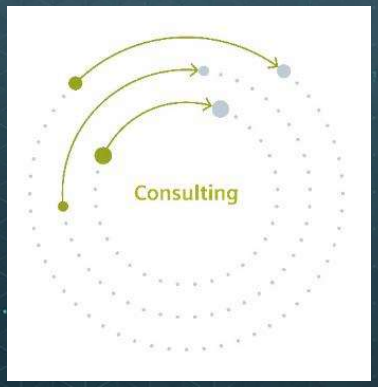
- **Already starts in R&D**

IEC 62443-4-1 and
IEC 62443-4-2 proven

Read more
Practical standards
for Industrial Security

Further info click here: LINK

Plant Security – Comprehensive Industrial Security Services



Security Consulting

Evaluation of the current security status of an industrial environment

- Security Assessments
- Scanning Services
- Industrial Security Consulting

Security Implementation

Risk mitigation through implementation of security measures

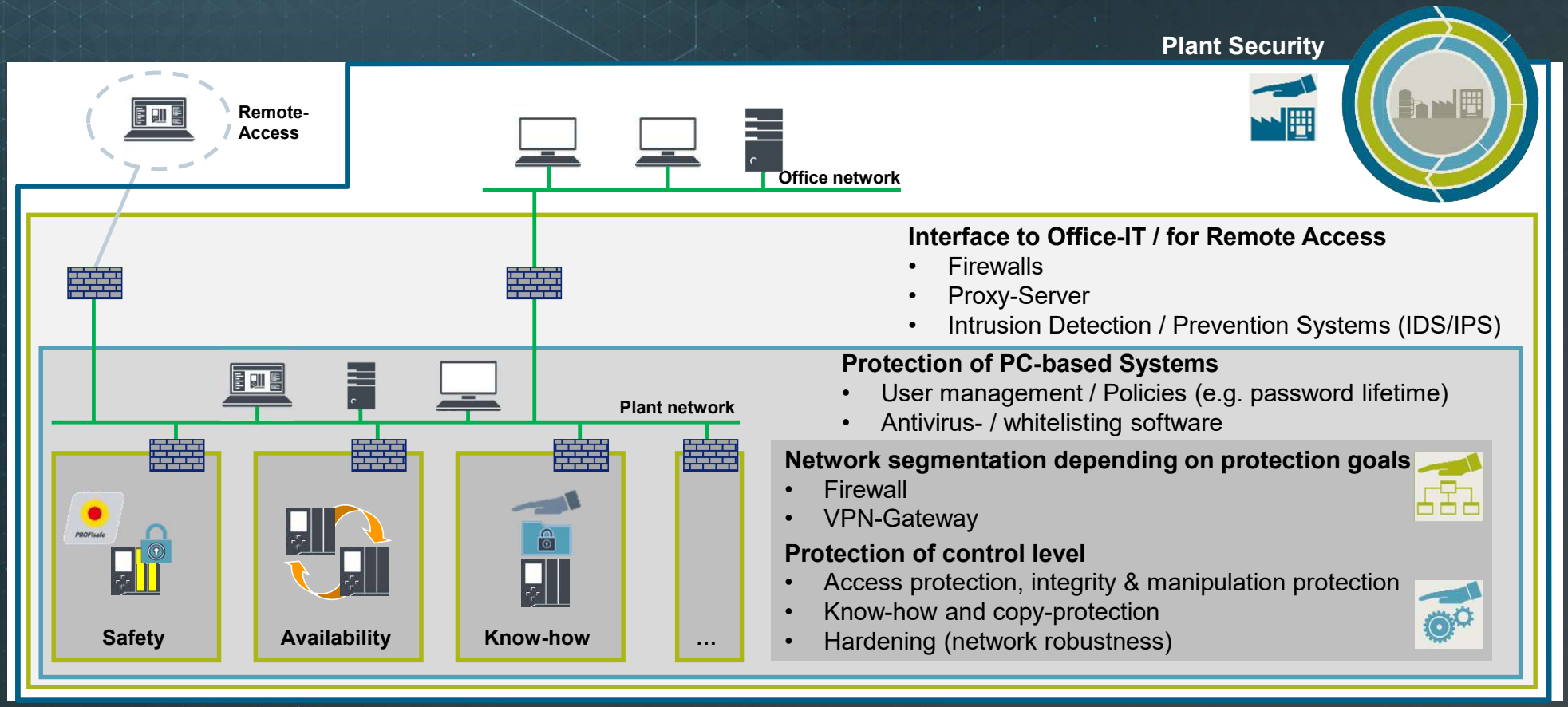
- Security Awareness Training
- Automation Firewall
- Endpoint Protection

Security Optimization

Comprehensive security through managed services

- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC Security Service Packages

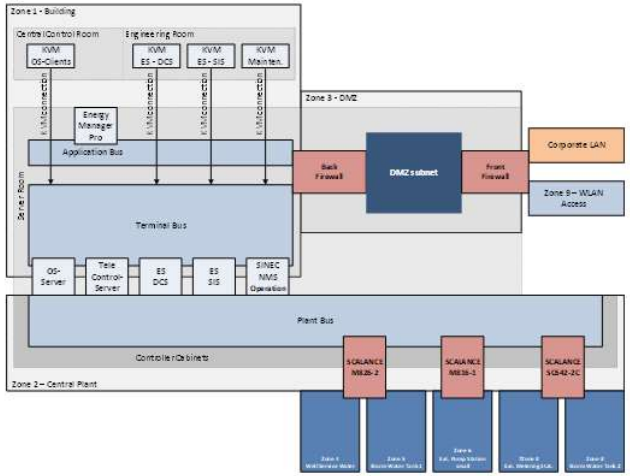
Defense-in-Depth security architecture to protect automated production plants



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

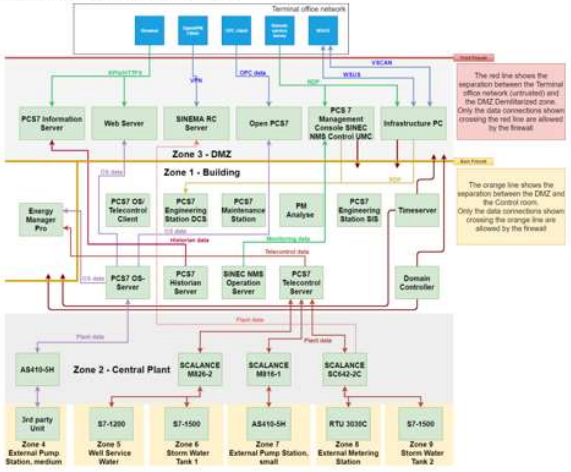
The Blueprint Wastewater Treatment Plant has only one external zone: The Corporate LAN.

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.

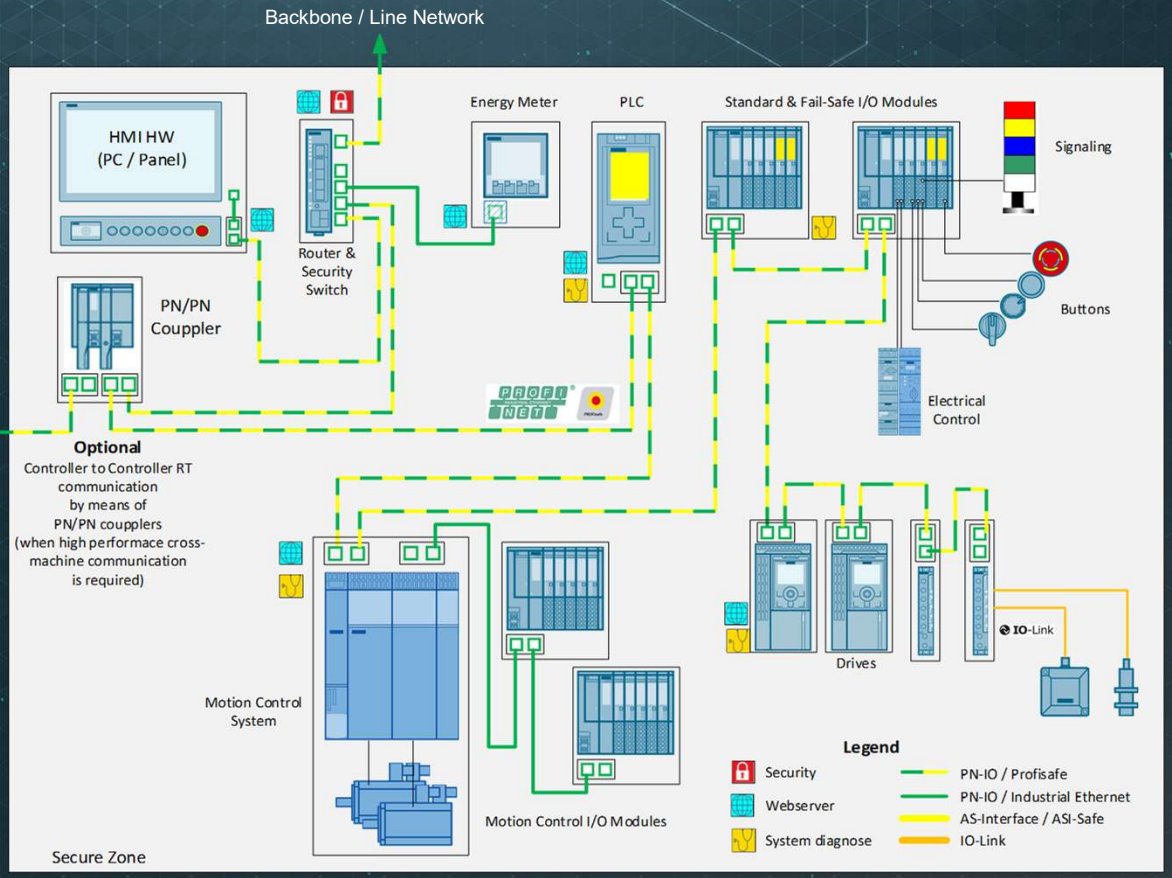
For operating system access, personalized Windows accounts and groups are used. These can be centrally managed by a domain controller where all PC based machines in the terminal bus, application bus, and DMZ networks are covered.

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.

Network Security – F&B Use Case
Cell Protection at Machine Level

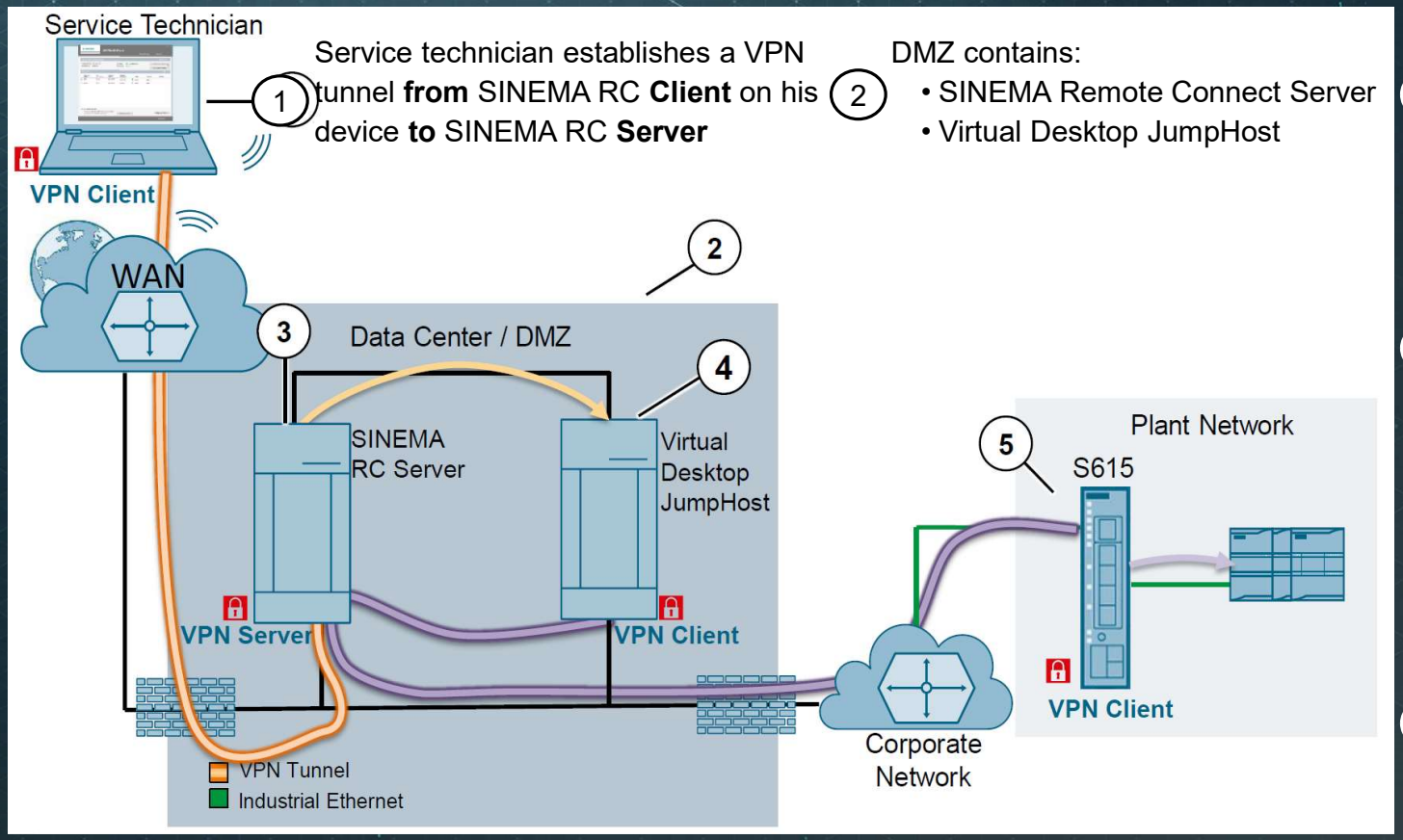


Machine Network Security Concept

Considered Aspects:

- Security – Cell Protection Concept
- Security – Remote Access, Access Protection
- Security – Norms Compliance, KRITIS
- Functional Security - Local
- Functional Security – Machines Interconnection
- C2C[1] – Realtime (PN/PN-Couppler)
- C2C[1] – Semi-Realtime (Application dependent)
- C2C[1] – Acyclic (OPC UA Client/Server)
- Standarized
- System Diagnose
- Cost-effective

Network Security – F&B Use Case
Cell Protection with SINEMA Remote Connect



1 Service technician establishes a VPN tunnel **from** SINEMA RC **Client** on his device **to** SINEMA RC **Server**

2 DMZ contains:
- SINEMA Remote Connect Server
- Virtual Desktop JumpHost

3 SINEMA RC Server has two physical separate interfaces:
- WAN: Connection to external network. Used for VPN tunnels
- LAN: Connection to internal network in DMZ.

4 JumpHost has installed:
- SINEMA RC Client
- Engineering SWs (TIA-Portal)
- Remote Desktop

Interfaces:
- LAN: Connection to external network. Used for VPN tunnels
- WAN: Connection to internal network in DMZ.

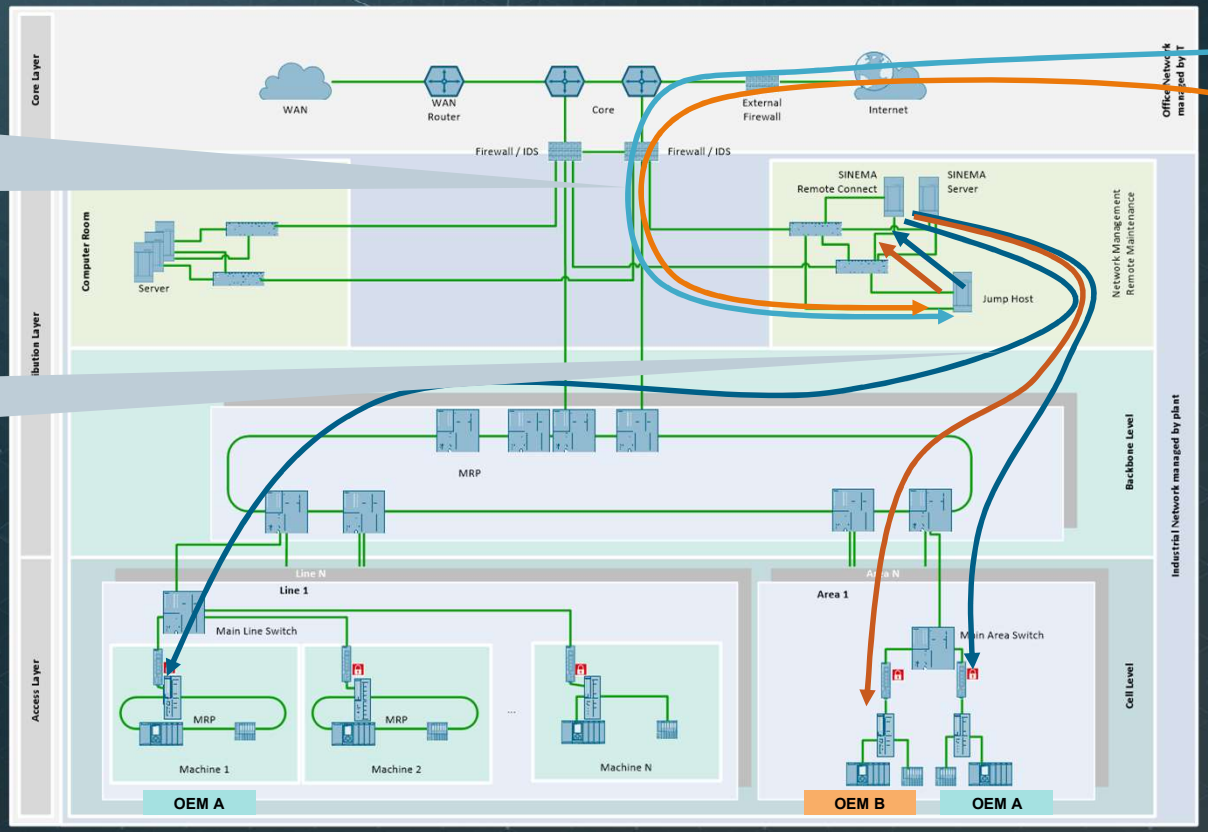
5 Scalance S615 automatically establishes a VPN tunnel to SINEMA RC Server. It protects the plant against unauthorized access.

Network Security – F&B Use Case

Remote Access based on Cell Protection Concept

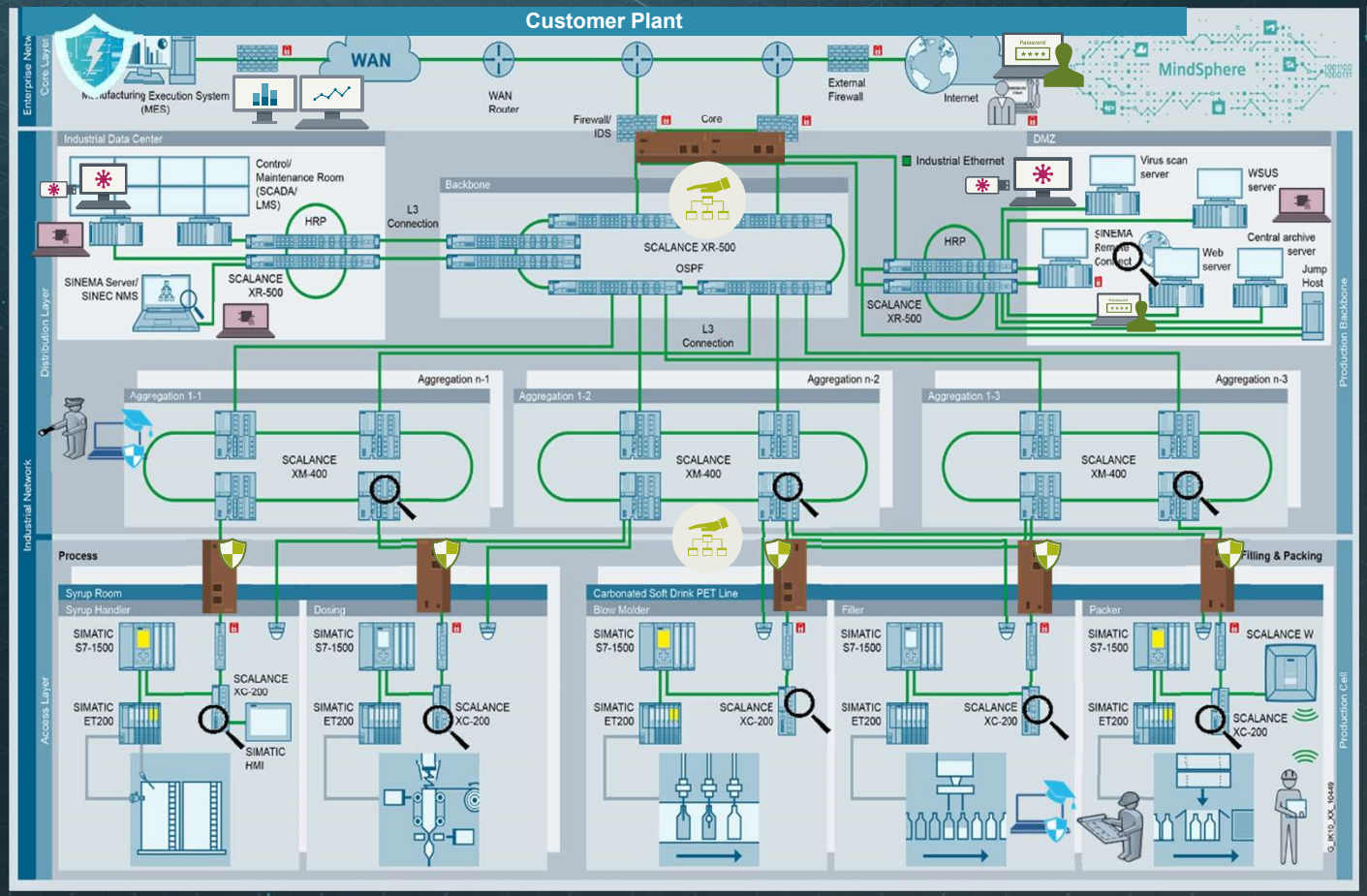
OEM A sets up a tunnel based on IT departments VPN solution and connects to the jump host

OEM A connects to specific machines using SINEMA RC



Cell protection concept, remote maintenance solution and network management

Industrial Security Services – Security Measures in F&B Plants



Implementation Elements

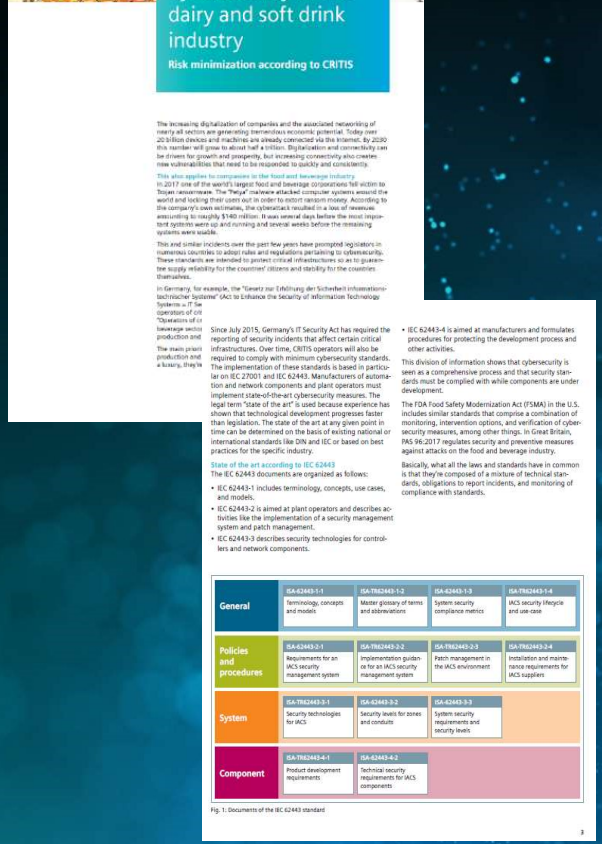
- Vulnerability Management
- Security Monitoring
- Remote Incident Handling
- Security Zones and DMZ
- Firewalls and VPN
- Patch Management
- System Hardening
- Endpoint Protection
- Industrial Anomaly Detection
- Training and Processes

Whitepaper

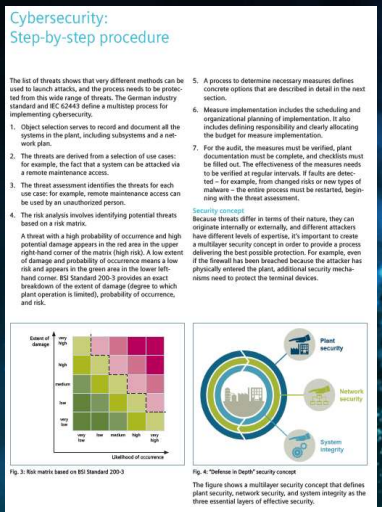
- **Cybersecurity in the dairy and soft drink industry**

Cybersecurity in the dairy and soft drink industry

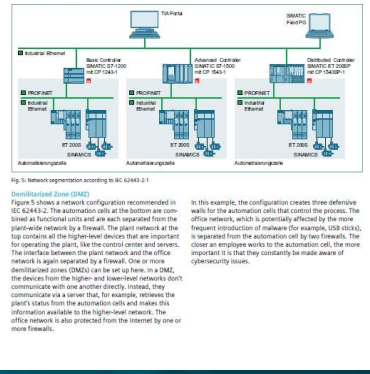
Risk minimization according to CRITIS



Cybersecurity: Step-by-step procedure



Network segmentation



Enmanuel Aparicio Velazquez | Olmo Castaneira Rios

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens AG, its affiliated companies or third parties. Their unauthorized use may infringe the rights of the respective owner.

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 constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

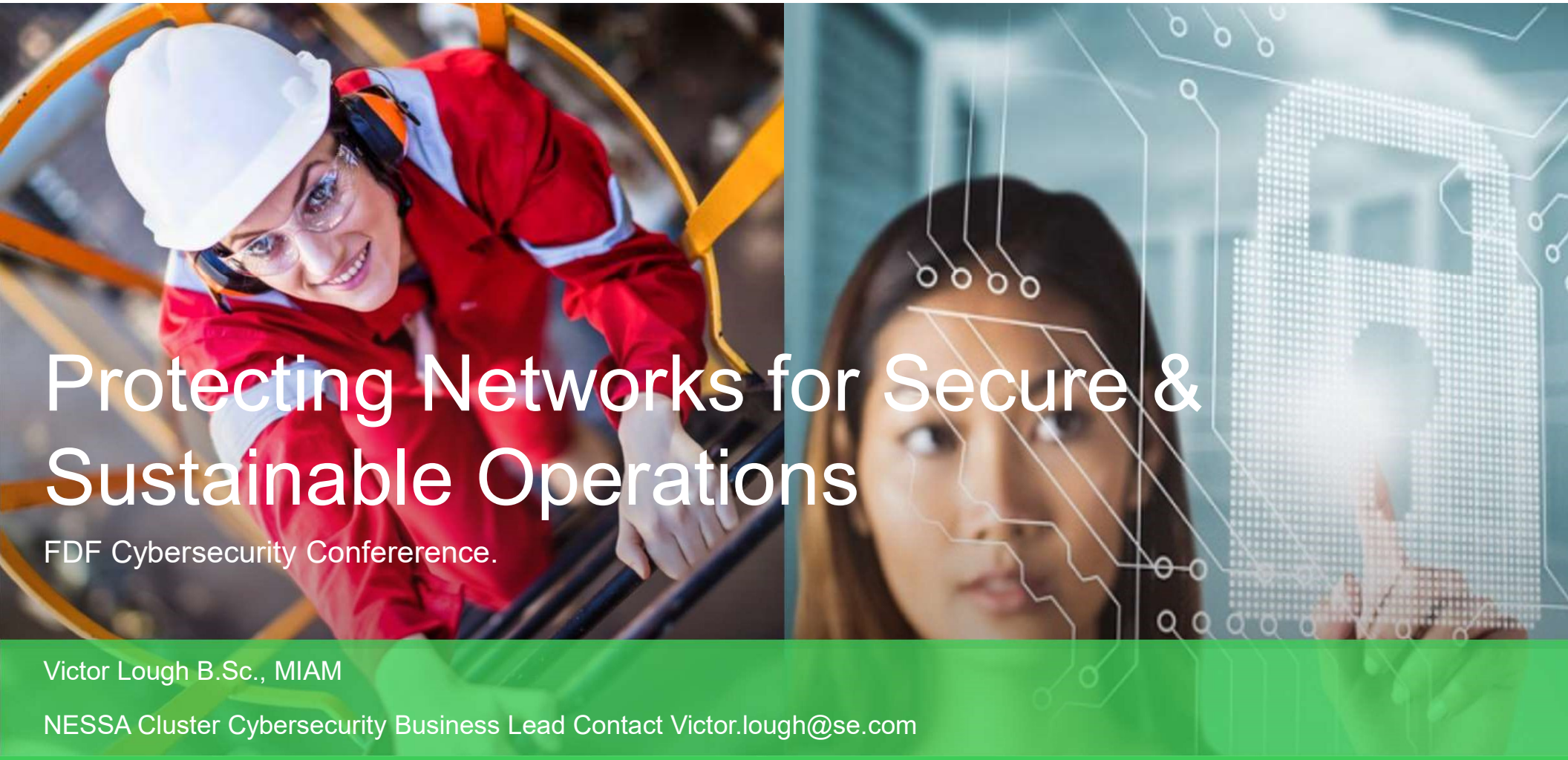
For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the 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 https://www.siemens.com/industrialsecurity.

Protecting Networks for Secure and Sustainable Operations

Victor Lough
Business Lead Cyber Security
Nessa Cluster
Schneider Electric



Protecting Networks for Secure & Sustainable Operations

FDF Cybersecurity Confererence.

Victor Lough B.Sc., MIAM

NESSA Cluster Cybersecurity Business Lead Contact Victor.lough@se.com

Life Is On Schneider Electric

Your Speaker today – Victor Lough Cyber Security Business Lead.

~ 35 + yrs in OT, 20 yrs with Schneider-Electric

- Lead Technician Marine Seismic Exploration
- Program Manager & Regional Sales Manager Strategic Solutions
- 2006 Performance Services incl Cyber & Wireless solutions
- Information Assurance for CNI Networks
- Chair E3CC Schneider-Electric collaboration Subgroup
- **2019** Schneider-Electric announced “Net Zero by 2025 Sustainability challenge”

Life Is On | Schneider Electric

Cyber Security & Sustainability What is it?

Assess

Act

Manage

- The collection of **PEOPLE, PROCESSES, TECHNOLOGY AND PREPAREDNESS** that can be used to sustain the user, the organization, its assets, the cyber environment and the wider public.

Re-purposed from ONR Office for Nuclear Regulation Security statement

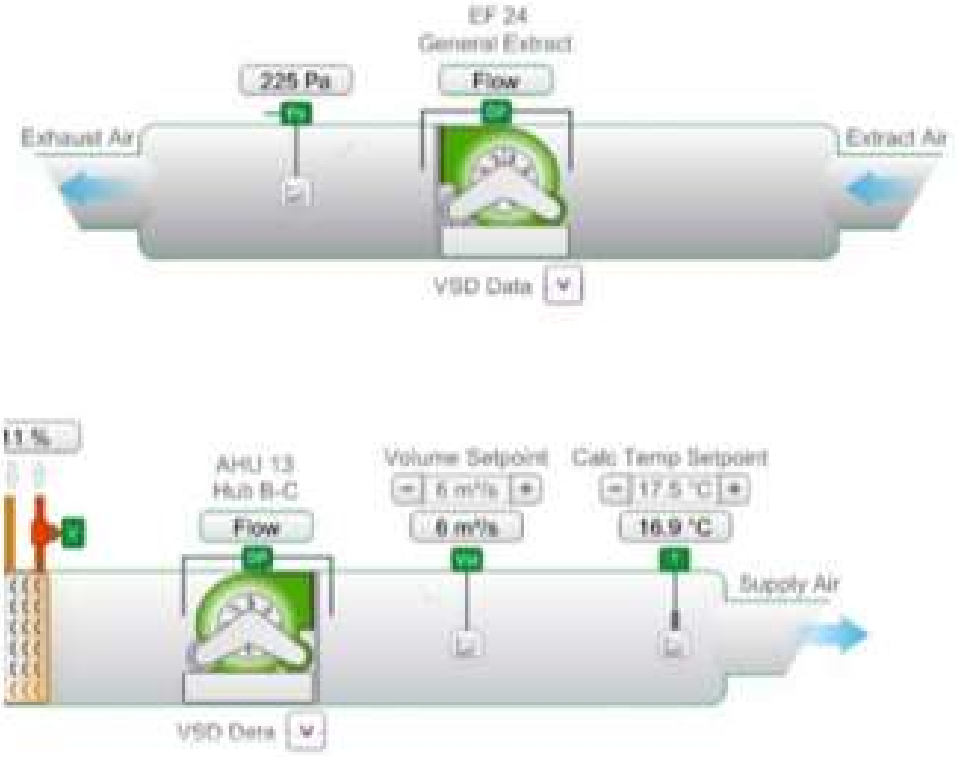
Life Is On | Schneider Electric

Sustainability is not achieved with an Air Gap

" After we implemented the wireless solution, we went up to 75% shift occupation – this resulted in a 25% increase in production."

Mike Spronkmans,
Manager, Technical Operations, Arkema Rotterdam
Arkema Rotterdam 2012

Sustainability Drives Connectivity



EU “Nearly Zero 20/10/31/ Directive

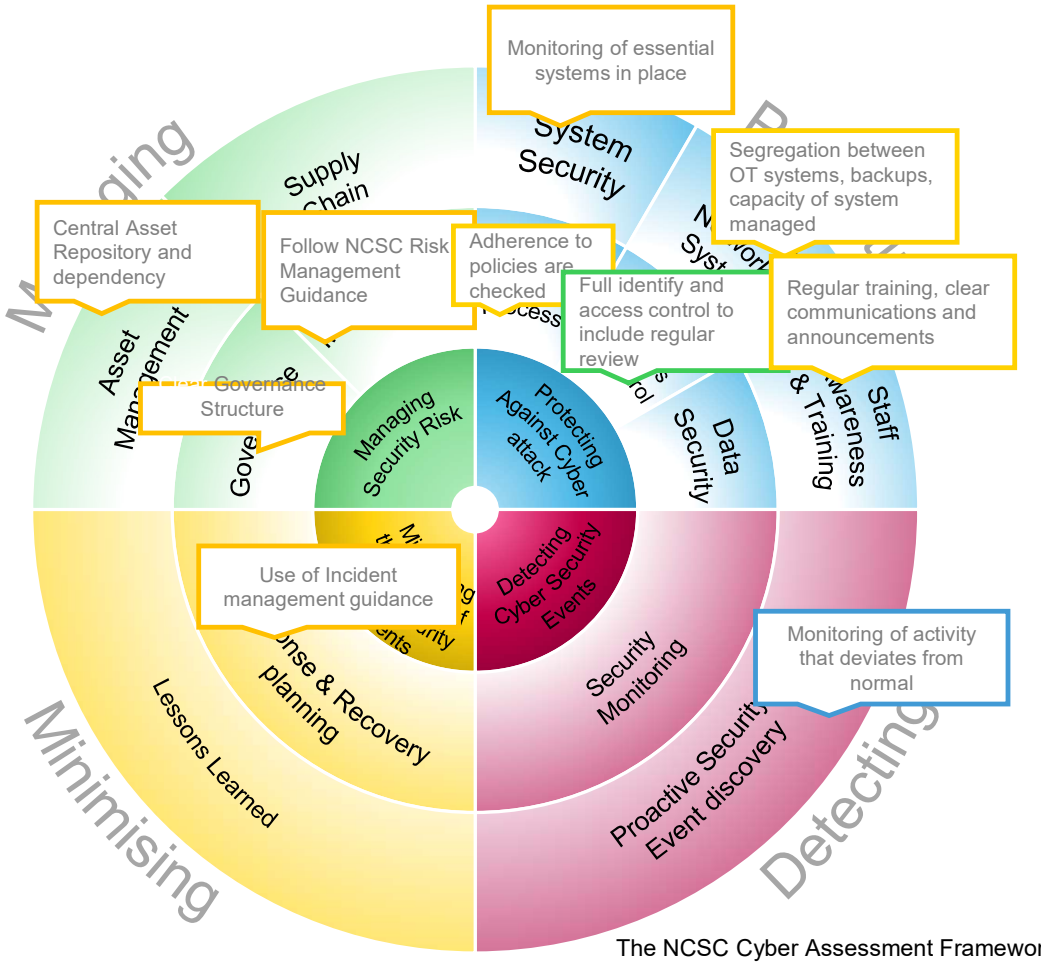
“The plant can be operated remotely … with site wide web access”.

“The BMS shall operate over the clients IT Network …”

“The web-browser access shall be totally robust and the possibility of remote 'Hacking' into the system shall be completely eliminated. ”

Life Is On Schneider Electric

Why Regulation is helping ?



The NCSC Cyber Assessment Framework CAF 3.0

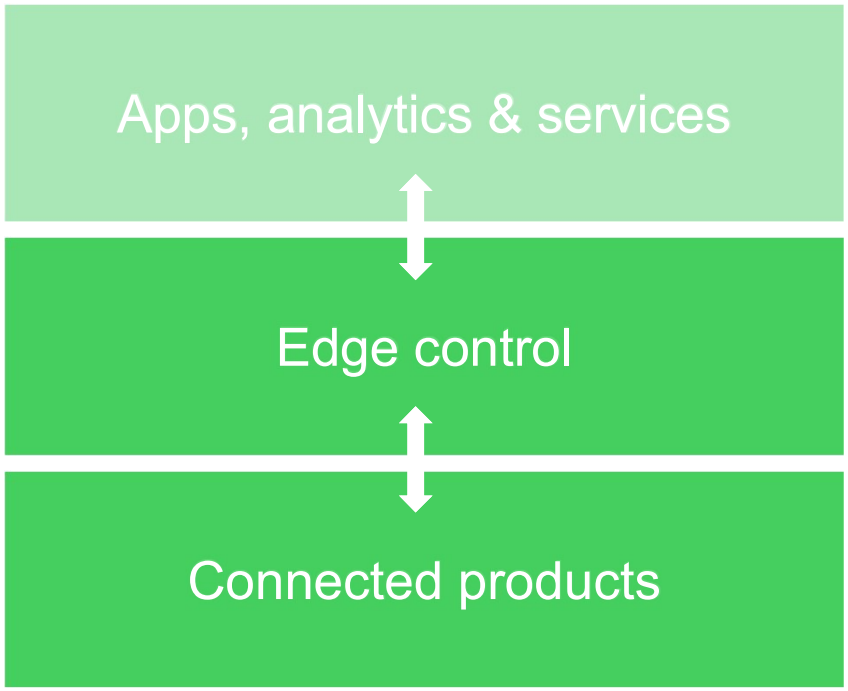
- The **OBJECTIVE**
  - Supports duty holder capability.
  - Delivered through Defence in Depth philosophy (IEC-62443)
- The **EFFECT**
  - Establish Content
  - Make Detection Easier
  - Make Compromise Difficult
  - Make Disruption Difficult
  - Reduce Impact

Life Is On | Schneider Electric

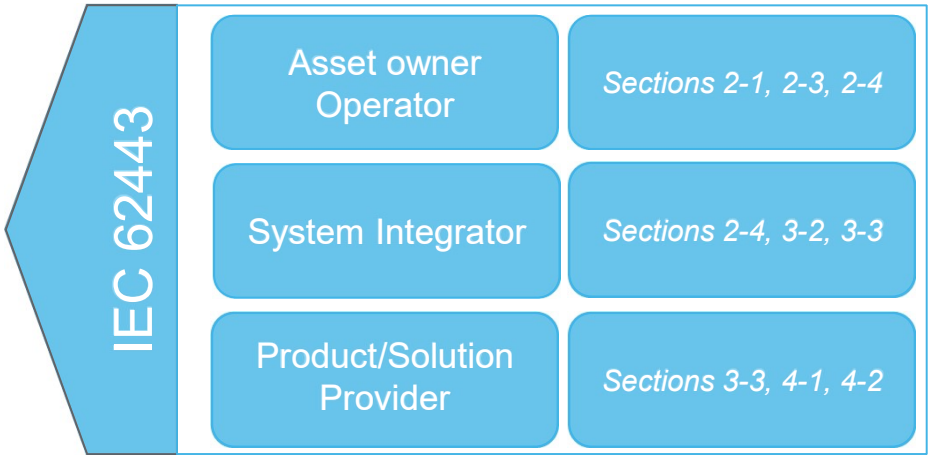
Standards for Products and Networked Solutions

IEC - 62443 : *Security for industrial automation and control systems*

EcoStruxure layers

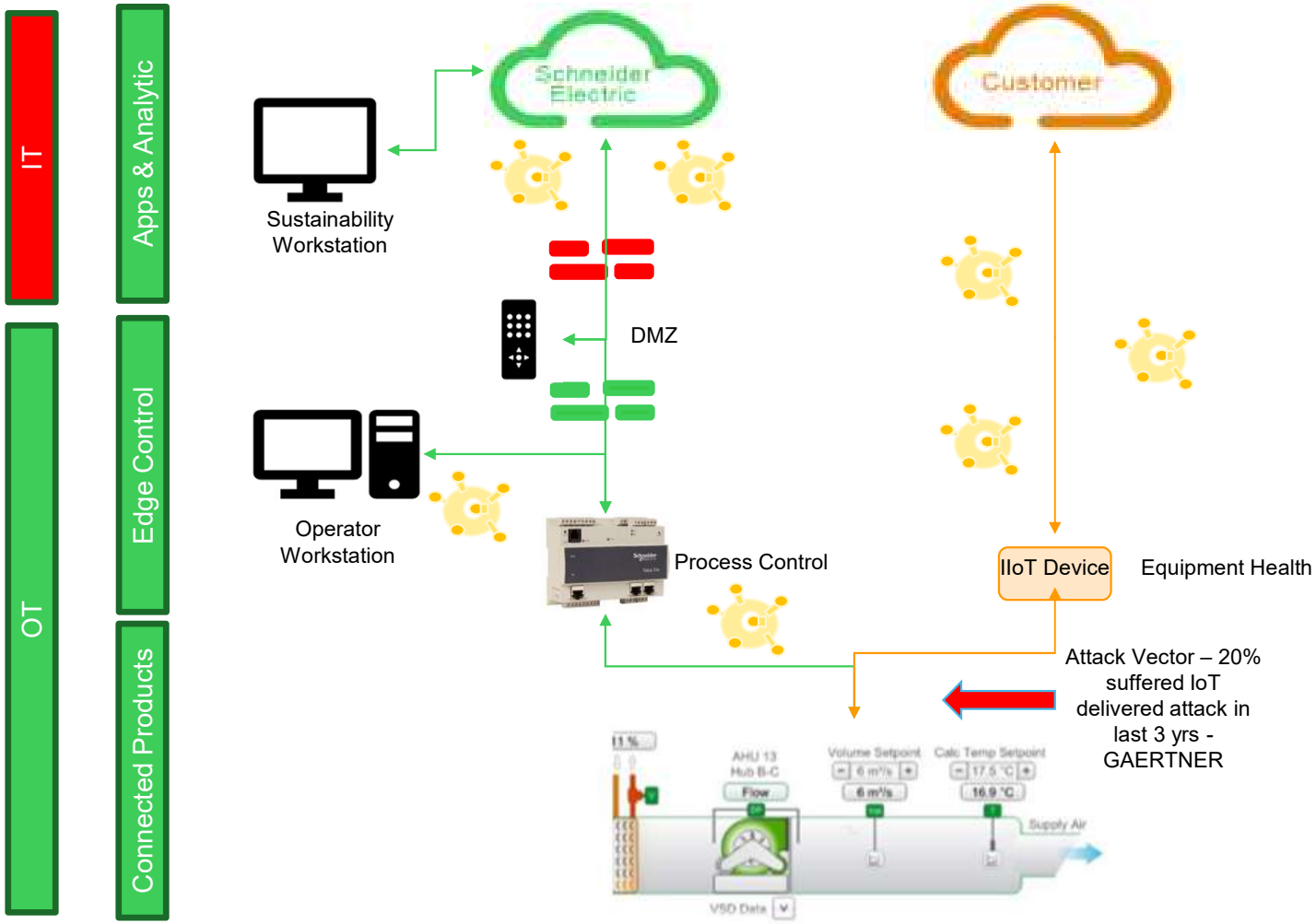


Schneider Electric selected the IEC 62443 as its core cybersecurity standard at **OT System and Product level**



Life Is On Schneider Electric

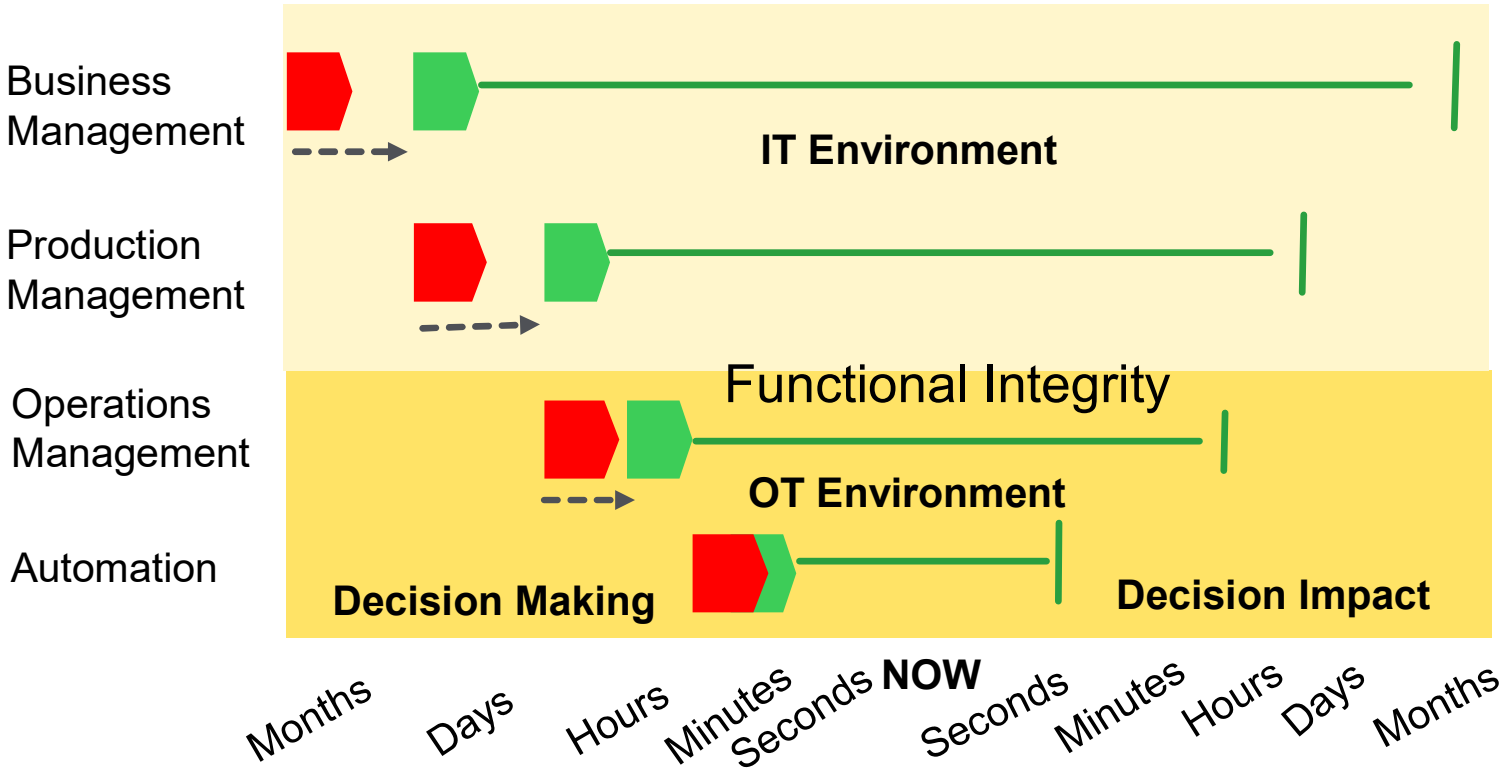
IIoT can bypass your Defence in Depth



IIoT Device has more processing power than a 750 Lb DEC VAX

Life Is On Schneider Electric

Why IIoT is a closed control loop safety concern ?



* From PTQ Q3 2019, Digitalisation is transforming KPI Settings

IIoT can bypass your Defence in Depth

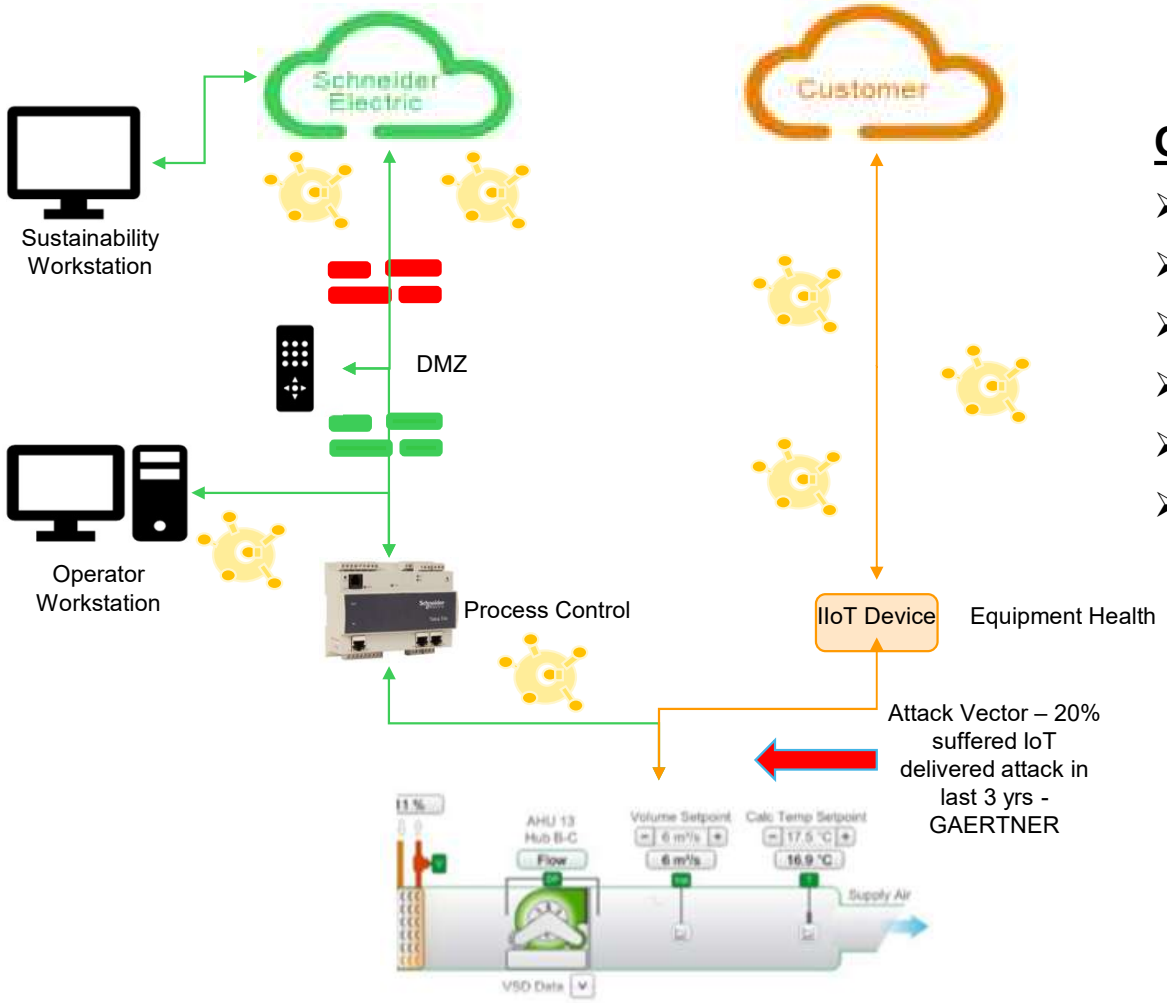
IT

OT

Apps & Analytic

Edge Control

Connected Products



OT IEC-62443 Standards

- Role based access control
- Patch Management
- Encryption of data in transit
- Encryption of data at rest
- Physical security
- Legacy Support

Life Is On Schneider Electric

The IIoT platform for your Sustainability

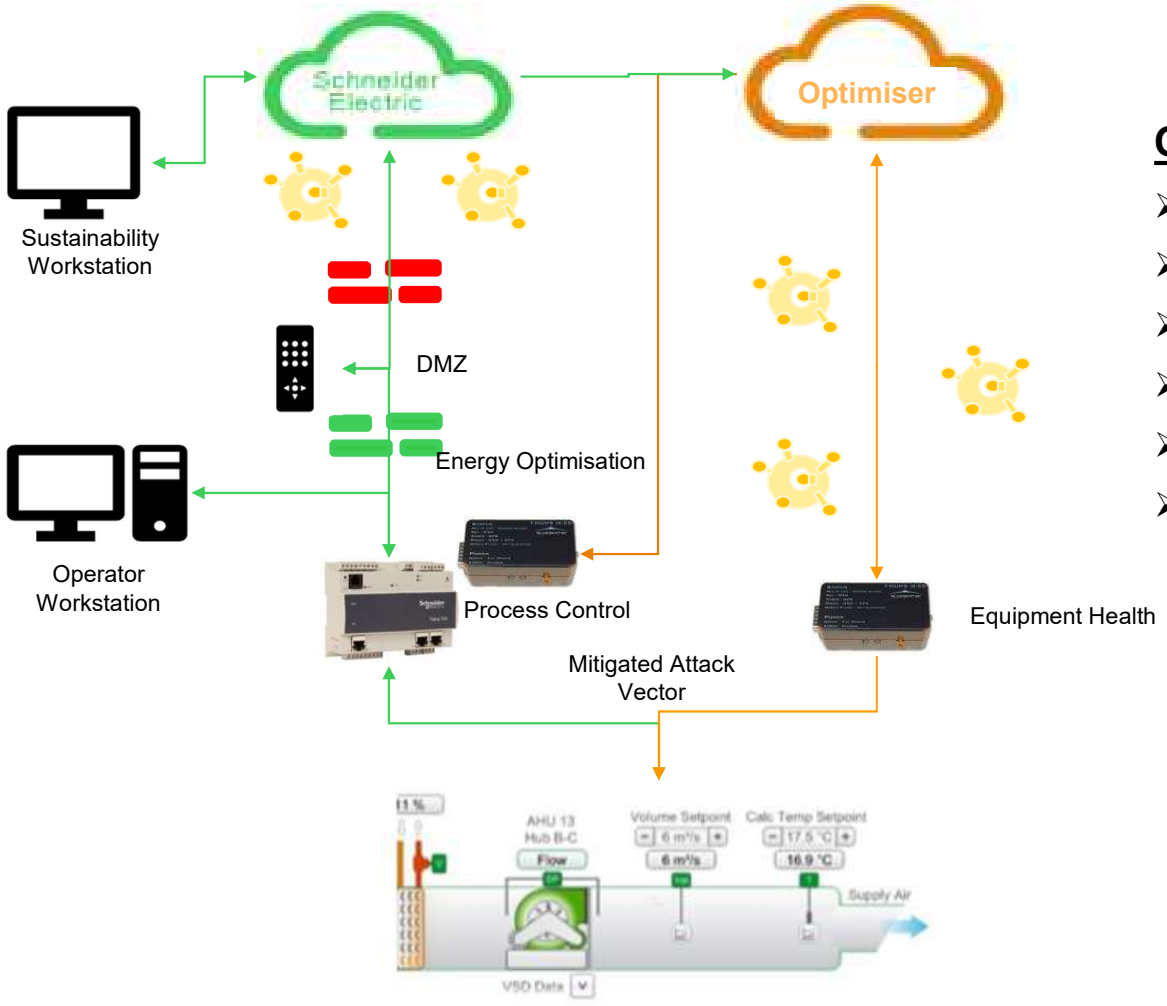
IT

OT

Apps & Analytic

Edge Control

Connected Products

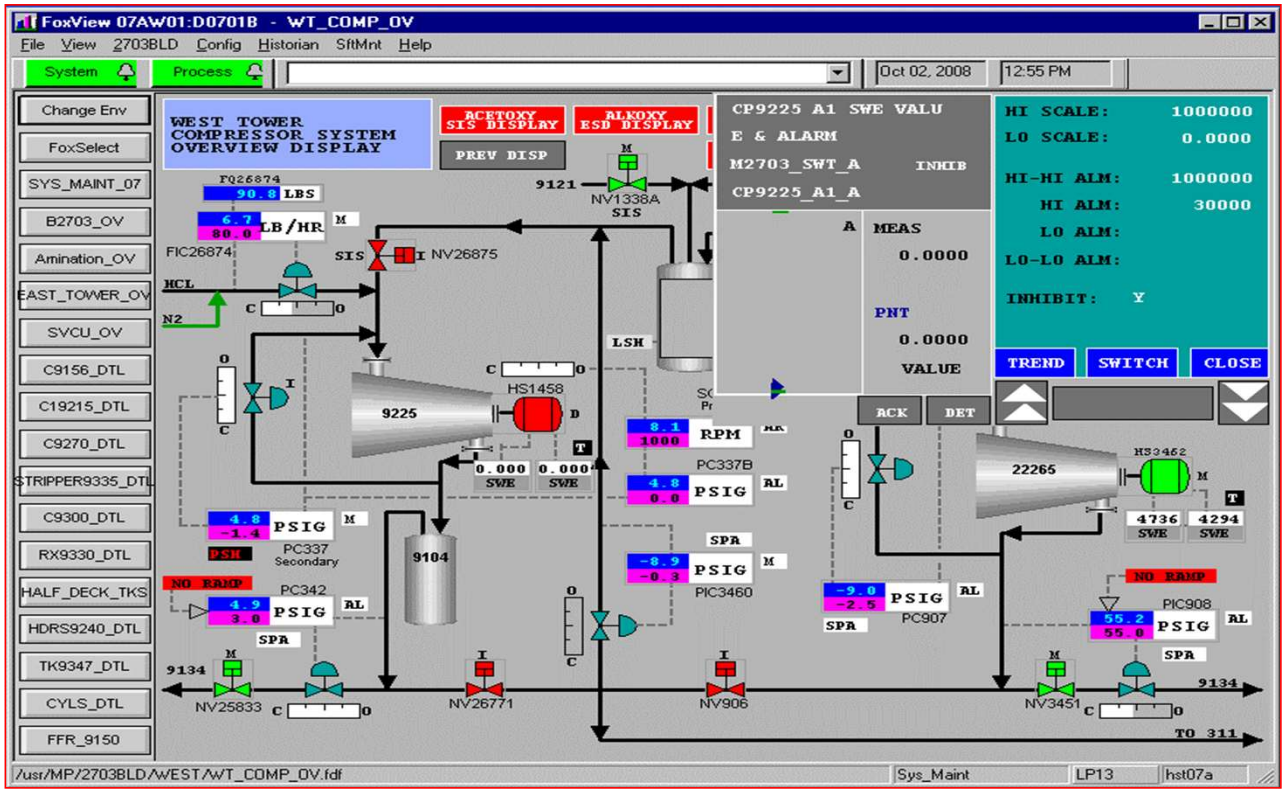


OT IEC-62443 Standards

- Role based access control ✓
- Patch Management ✓
- Encryption of data in transit ✓
- Encryption of data at rest ✓
- Physical security ✓
- Legacy Support ✓

Life Is On Schneider Electric

Sustainable Operations based on Condition



- Proactively ensures high value asset achieves design life.
- Helped Define the operational sweet spot for the compressor
- Alerts Operator on breach of limit so that they can ACT in real-time.
- Operator can click on HMI tag for more detailed analysis (Trend etc)

The reduction in compressor loading delivered a $7,500 /Month in energy savings.

Life Is On Schneider Electric

Key Takeaways– Sustained Network Infrastructure

Tim Sowell Blog – March 31, 2014

1) Shorten deployment time with **secure reference designs**
2) Create efficiencies and reduce complexity in hybrid network with **standards**
3) Increase sustainability with **energy effective** solutions.
4) Security is a **benefit** not a burden

Schneider - Electric Cyber Security Services

Victor Lough

Business Lead

Victor.Lough@SE.com

Life Is On Schneider Electric

Mitigating against a Cyber Breach

Tristan Hall
Partner
CMS

Loretta Pugh
Partner
CMS

Cyber Team

CMS Law.Tax

Mitigating against a Cyber Breach

Tristan Hall | Partner, Insurance | CMS
Loretta Pugh | Partner, Data Protection | CMS

Your speakers today

Tristan Hall

CMS Partner
Insurance

tristan.hall@cms-cmno.com

Loretta Pugh

CMS Partner
Data Protection

loretta.pugh@cms-cmno.com

Today’s agenda

Overview

Incident Response Plan

Other Mitigants

Security

Insurance

Conclusions

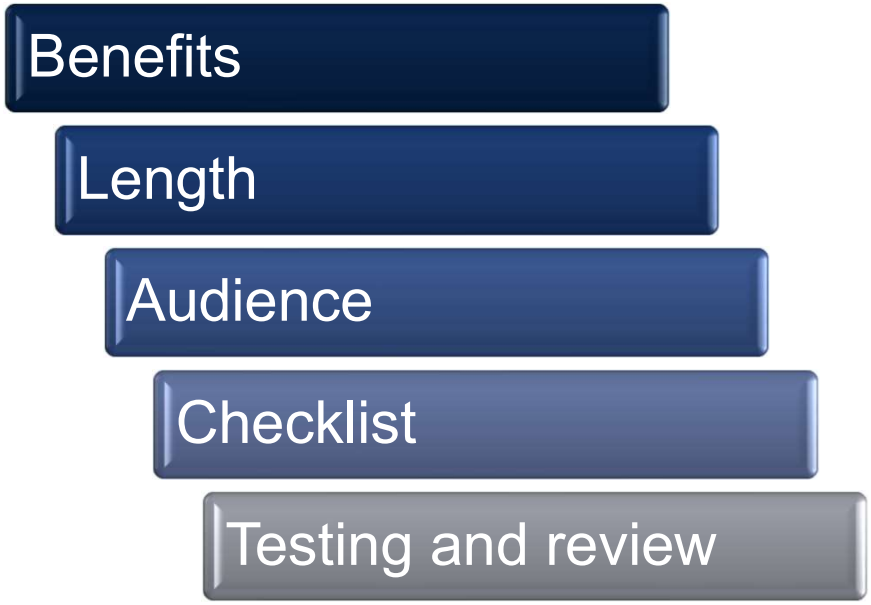
Cyber Team

Overview

– Why is this important?

  - Legal obligations
  - Disruption
  - Reputation

Incident Response Plan

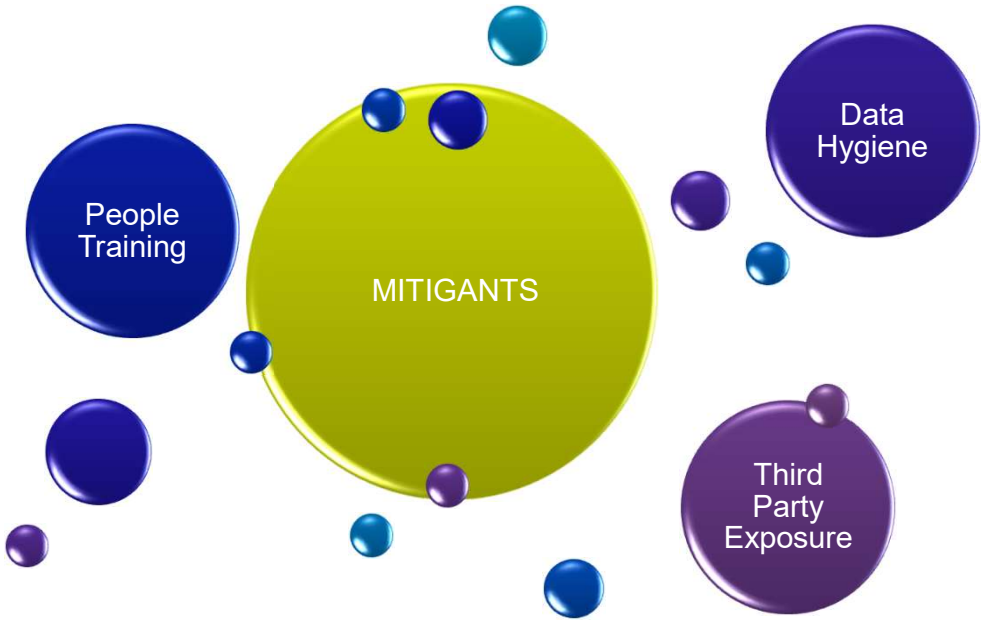


Cyber Team

Incident Response Plan Contents

Cyber Team

Other Mitigants



Cyber Team

Security

- Expert advice
- Investment
- Quick wins:
  - Passwords
  - MFA
  - Offline backups

Cyber Team

Insurance

- Pre-breach services
- Incident response solution
- Business interruption
- Civil claims

Conclusions

C/M/S/ Law-Now™

Law.Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

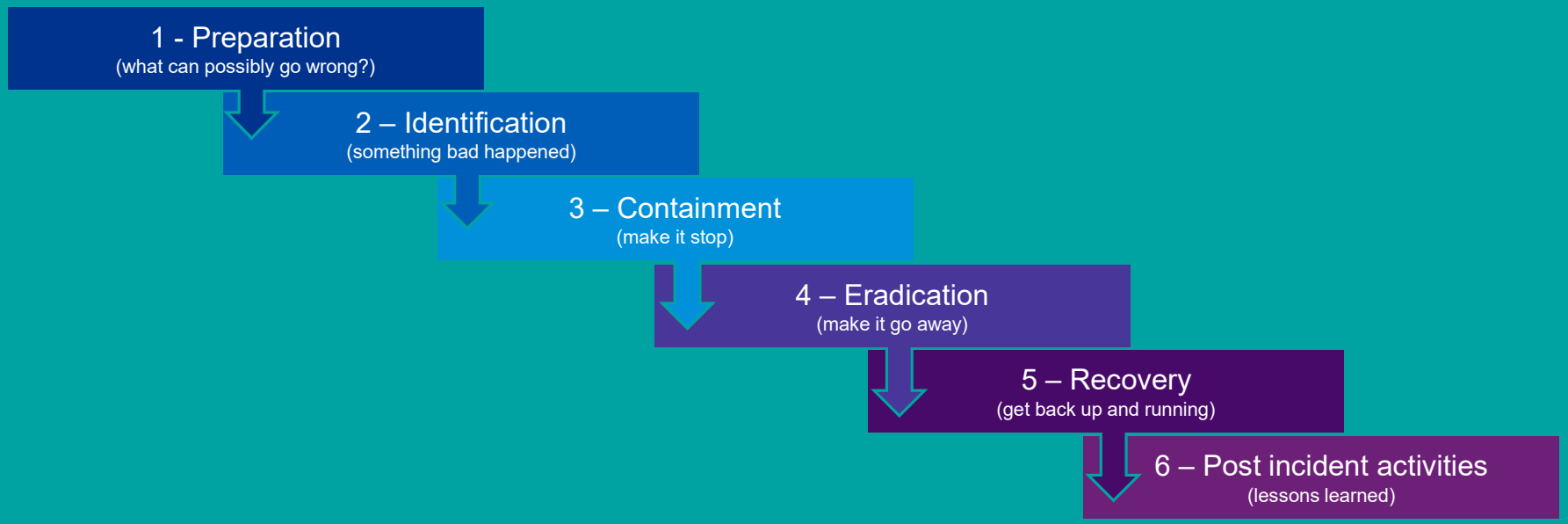
cms.law

Cyber Team

Cyber breach lifecycle

Martijn Verbree
Partner and Lead of KPMG UK's Corporates Cyber Security business
KPMG

Cyber breach lifecycle



Panel Discussion and Q&A

food & drink federation
passionate about food & drink

Thank you for attending our event!

@foodanddrinkfed
#FDFCyberSecurity


Join us for our next event…
AUTOMATION & DIGITALISATION
IN THE FOOD & DRINK INDUSTRY
24 – 25 MARCH 2021
fdf
food & drink federation
passionate about food & drink