Cybersecurity for your digital transformation

Services and solutions from Schneider Electric

SESA42372

Peter FUGLSANG
Product Application Engineer

Business Unit	Europe Operations
Function & Sub-Function	Sales | Product Application Engineering
Company I Work For	SCHNEIDER ELECTRIC DANMARK A/S
Location	Ballerup, Ballerup, DENMARK +1 more
	+Edit/Remove Alternative Work Address

SESA625752

Graham RENNIE
Director, Technology and Standards

Business Unit	Industrial Automation
Function & Sub-Function	Sales | System & Architecture Engineering
Company I Work For	Schneider Electric Systems UK Limited
Location	UK Home based, Telford, UNITED KINGDOM

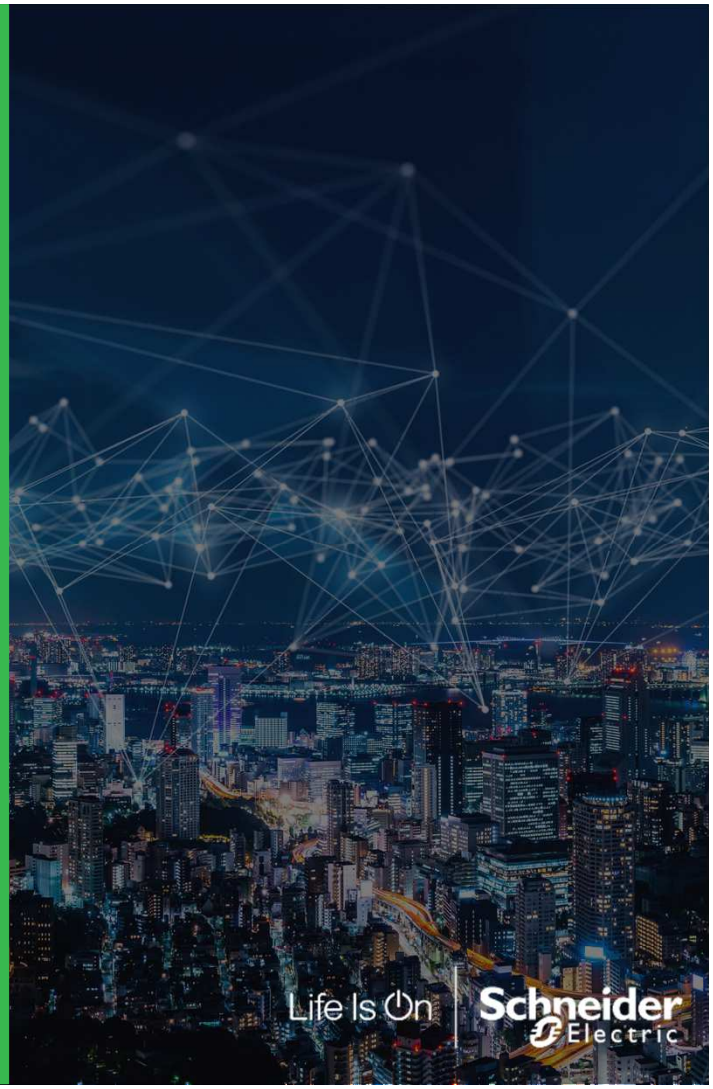
Life Is On Schneider Electric

Confidential Property of Schneider Electric

Internal

Contents

- The value of cybersecurity
- End-to-end cybersecurity
- Secure communication
- Global partners, success stories and presence



Internal

The value of cybersecurity

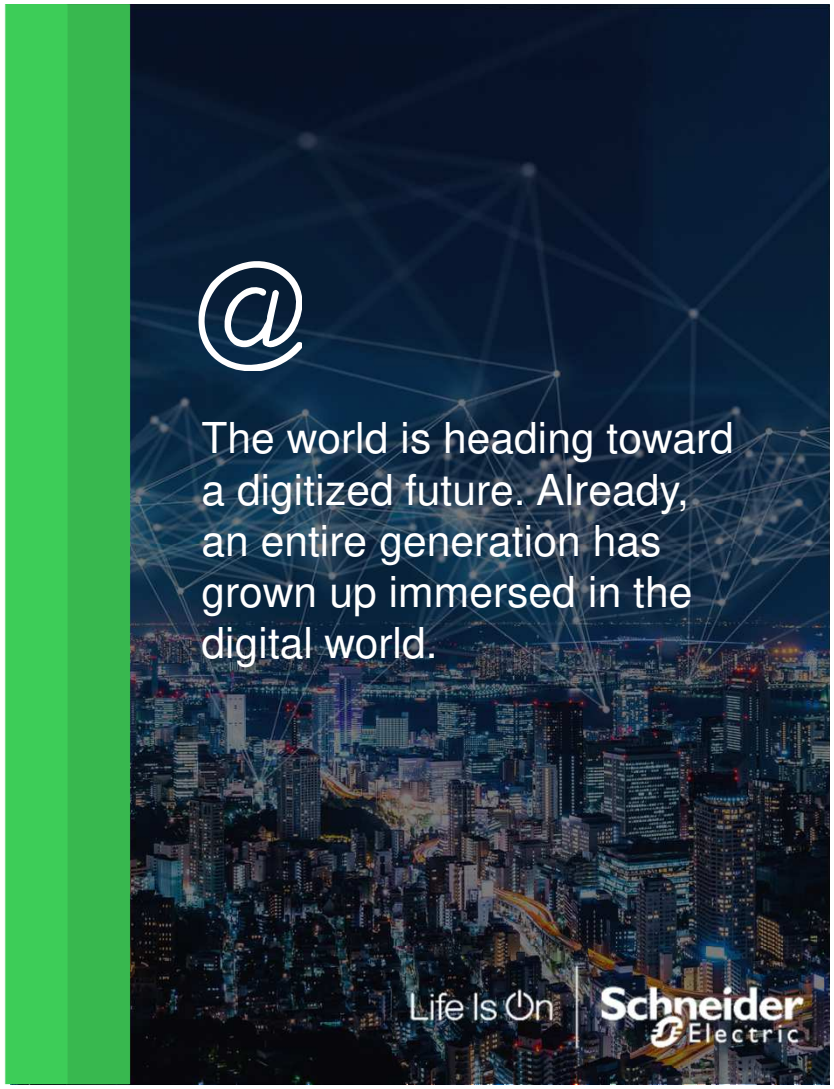
Life Is On Schneider Electric

Your digital transformation journey

Digital transformation - or the widespread adoption of digital technologies to:

Securely harnessing the benefits of the IoT to deliver real time business value

Internal



The Internet of Things (IoT)

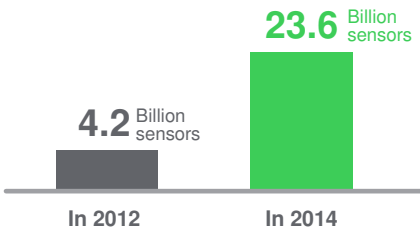
Enterprises across all industries are already making big bets on a connected future.

4.5 billion people have access to the internet.

People are connected on every type of device, globally spending an average of **6.4 hours** online daily.

The Internet of Things (IoT) market is expected to grow to **75.44 billion** connected devices by 2025.

Sensors shipped for industrial use has skyrocketed!



But is data being leveraged well for analytics?

On average, **60-73%** of all data within an enterprise goes unused for analytics

Source:
Accenture

Internal

Life Is On Schneider Electric

IoT business value

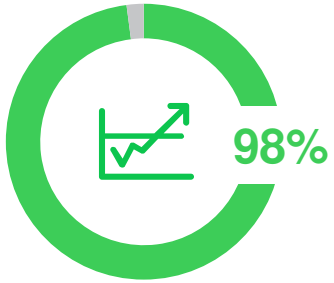
~10%
Reduction in maintenance costs - of industrial equipment with predictive maintenance.

10-20%
Workforce optimization

Up to **12%**
Savings on operating expenses

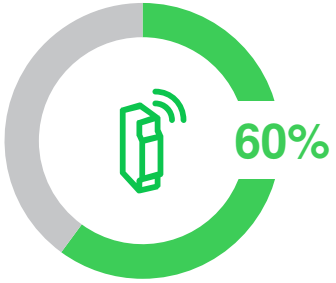
Up to **25%**
Savings on energy bills

Source:
Schneider Electric



98%

Industrial companies expect to increase efficiency by 2020 with digital technologies, including predictive maintenance and augmented reality.



60%

Manufacturers will have empowered shop floor workers with AR / VR, intelligent apps by 2021

Life Is On Schneider Electric

Internal

Digital transformation

The truth

Digital transformation is:
The exploitation of emerging technologies to create a smart, orchestrated and adaptive customer experience.

The myths

Digital transformation is not:
- Meant to disrupt your business.
- About headcount reduction.
- A business cure-all.
- All about trendy tech.
- A new thing.

The trends

Digital transformation will:
- Focus increasingly on customer data.
- Continue to follow emerging tech.
- **Requires a secure development lifecycle at every level across the business.**

Internal

Life Is On Schneider Electric

What's driving digitization in industry?

By its definition, the Internet of Things (IoT) is simply the inter-networking of physical devices to collect and exchange data via internet protocol (IP).

The true power and applicable value of IoT emerges when it is connected with five major technology transformations — ones that are accelerating our capacity to converge OT and IT systems:

CONNECTIVITY

- Smart connected devices (products)
- Standards-driven connectivity
- Lower cost of measurement

MOBILITY

- Pervasive and affordable communication
- Remote access
- User-driven interfaces

CLOUD

- Massive aggregation of data
- Data access by specialists
- Industrial application developer ecosystem

ANALYTICS

- Cognitive applications
- Artificial intelligence optimizing performance at all levels

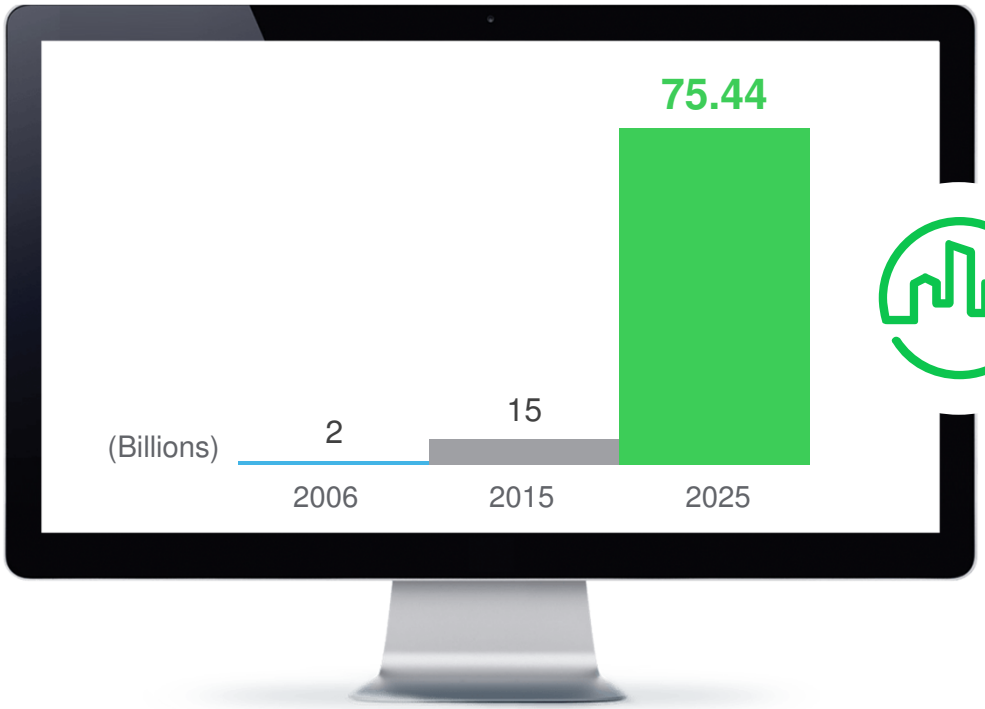
SENSING

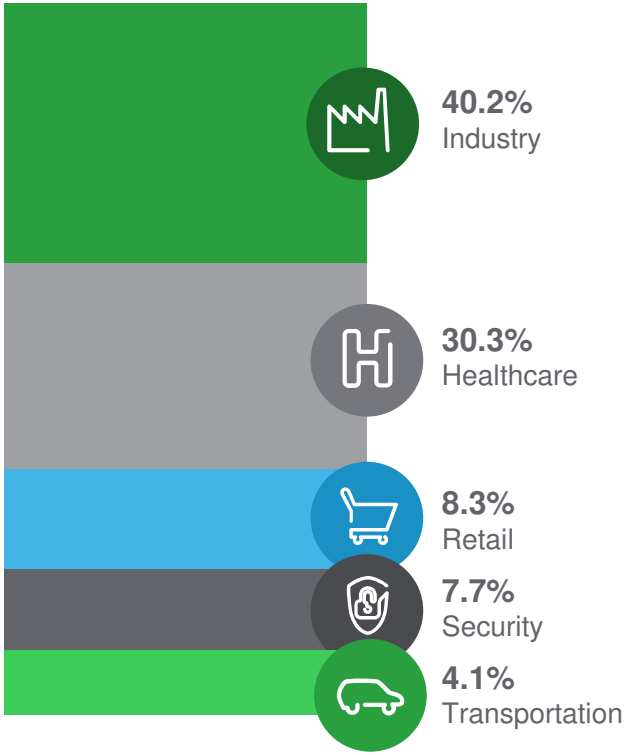
- Control from the field
- Astounding level of granularity to real-time data

Life Is On Schneider Electric

Internal

Growth in IIoT connected devices



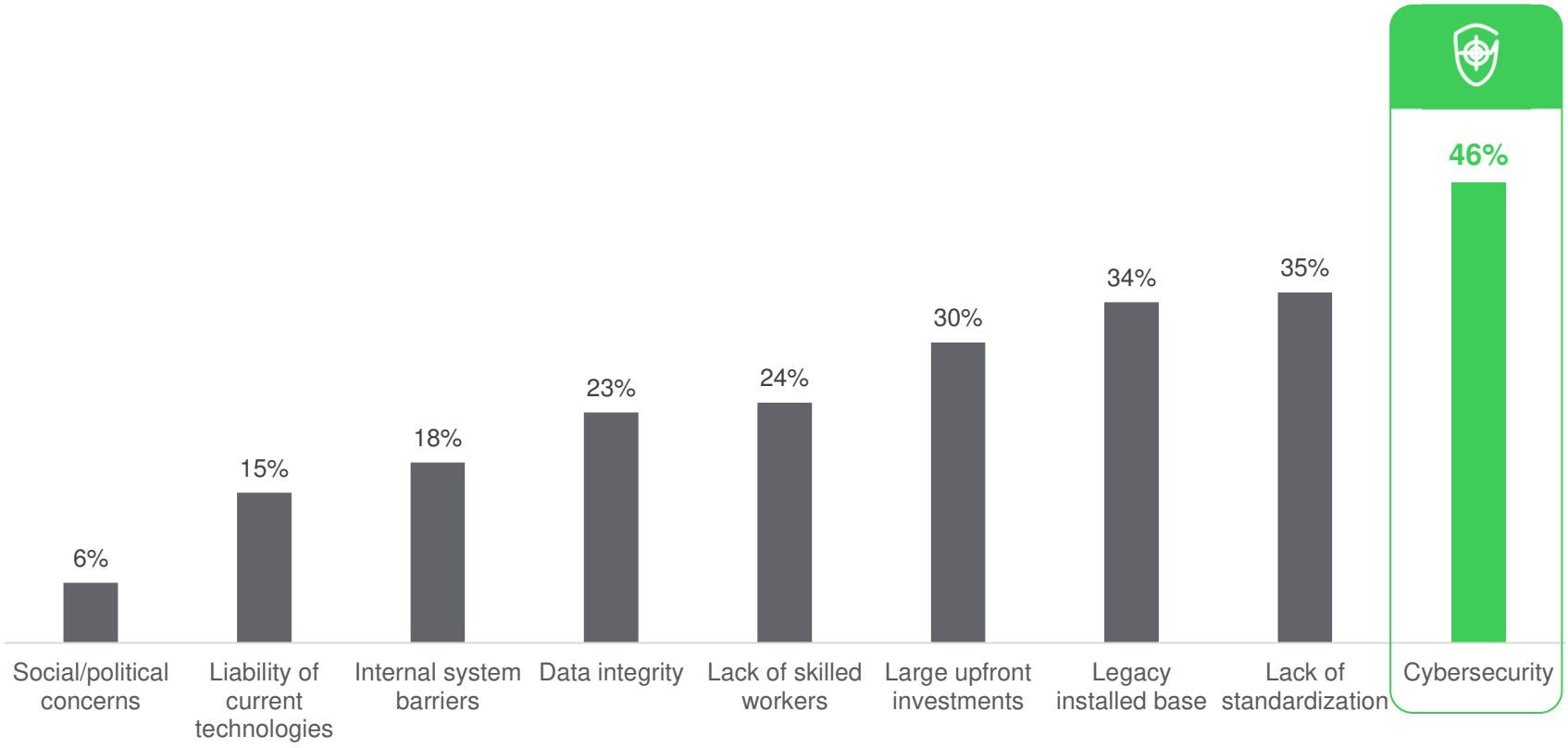


Source:
Intel

Internal

Life Is On Schneider Electric

Challenges to IIoT adoption



Source:
Morgan Stanley

Source: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

Internal

Life Is On Schneider Electric

Some statistics

Every **14** sec	a ransomware attack occurs
$3.8	million USD - average cost of a breach
Within **5** min	the average time it takes for an IoT device to be attacked after going online
67%	is the increase in security breaches over the last 5 years
49.6 days	typically pass between breach discovery and reporting dates
70%	of employees don't understand cybersecurity
Only **2**%	of IT budget is used for security
92%	of malware is spread by email
22%	of security issues stem from outdated and unpatched software
95%	of HTTPS servers are vulnerable to man-in-the-middle attacks

Source:
Hashed Out

Internal

The time for complacency is past

Cybersecurity defense requires a strong offense.

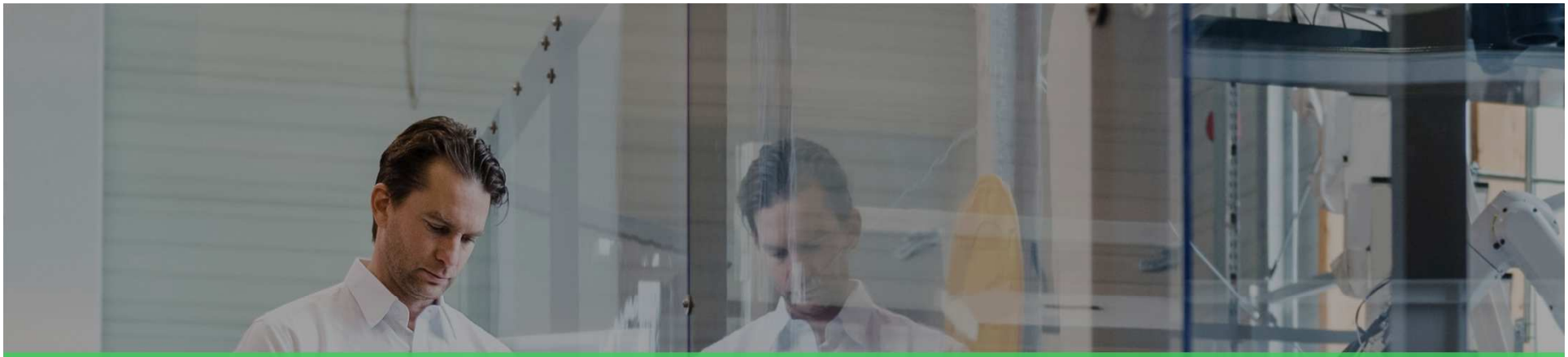
It is no longer a question of competitive advantage, or even minimizing damage.

It is a fundamental requirement for doing business today.

Life Is On Schneider Electric

Cybersecurity value proposition

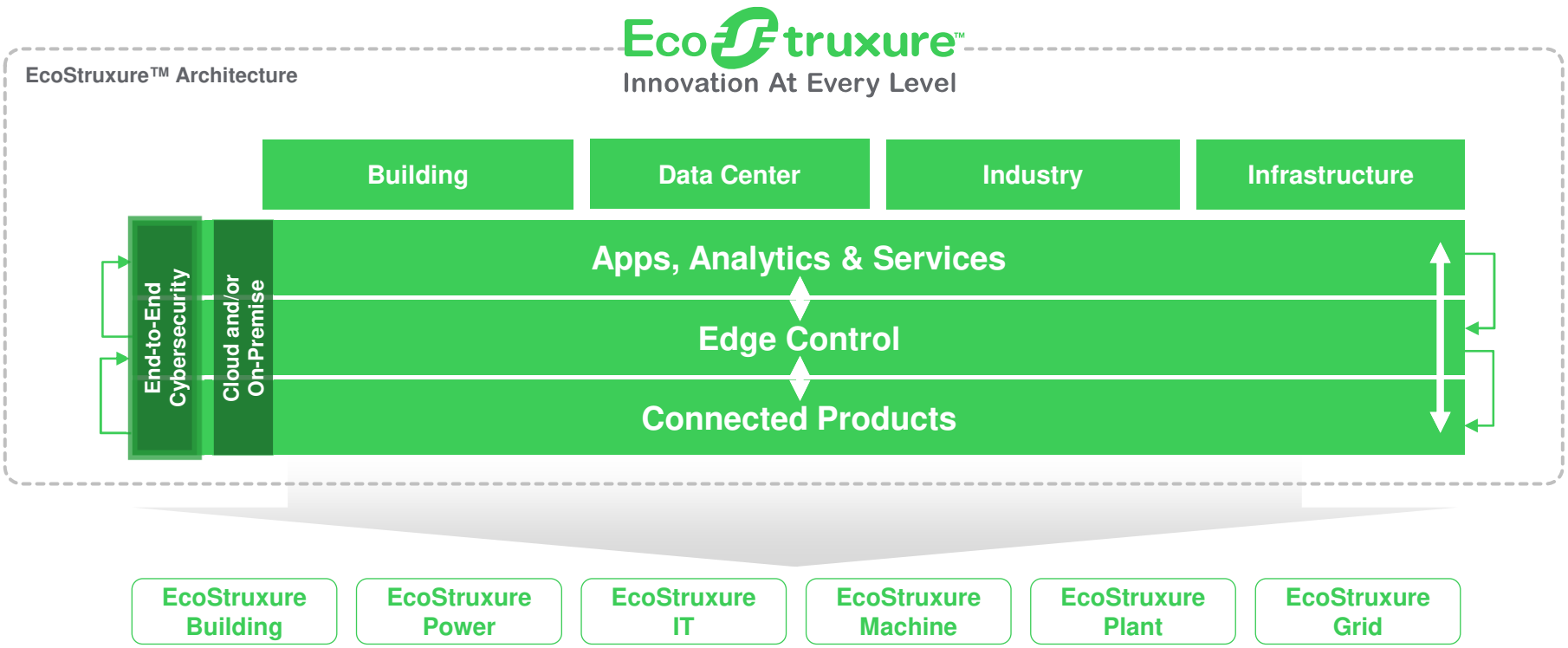
Internal



Services and solutions for all industries

Life Is On | Schneider Electric

End-to-end cybersecurity is an essential part of EcoStruxure



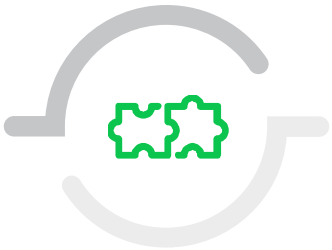
Internal

EcoStruxure architecture delivers cybersecurity across the connected offer lifecycle

Schneider Electric produces rules and policies to secure our connected offers from the device sensors to cloud

How we develop

Secure development lifecycle process



How we connect

Securing endpoints and IoT communications

How we secure the cloud applications

Leverage IT security best practices

How we protect data

Protect data privacy and confidentiality

Internal

Life Is On Schneider Electric

How we design and develop

Schneider Electric employs secure development lifecycle practices in its R&D and product lifecycle processes

- Corporate policy dictates all R&D projects must comply with SDL practices
- SDL practices apply to internal development actions and all along the supply chain.
- Project release requires final security review

Ensuring our offers comply with Schneider Electric policies and standards

Enforcement model for connected offers to validate compliance

- **By policy, all connected offers must comply**
  - Pre-requisite to “Go Live” for new Connected Offers
  - Risk-based approach
- **Standards-based and regulatory-compliant:**
  - IEC 62443-4-1, -4-2, -3-3, -2-4
  - ISO 27001
  - GDPR and other Data Privacy Regulations

Global Schneider Electric Cyber Security Program

Based on Standards

Developed using a Secure Development Lifecycle

Providing Stand Alone and System security features

Secured Schneider Core Offer

Security Products

Partnership Ecosystem to offer best of breed solutions

IT Technologies adopted to the OT world

HIRSCHMANN
A BELDEN BRAND

WATERFALL
Stronger Than Firewalls

McAfee

Recommended Practices

Security Information on products and vulnerabilities

Competency Centers and Information

Security Services

Lead by Cyber Security Experts

Support by OT security Experts

Schneider Electric

invensys

THALES

GSEC

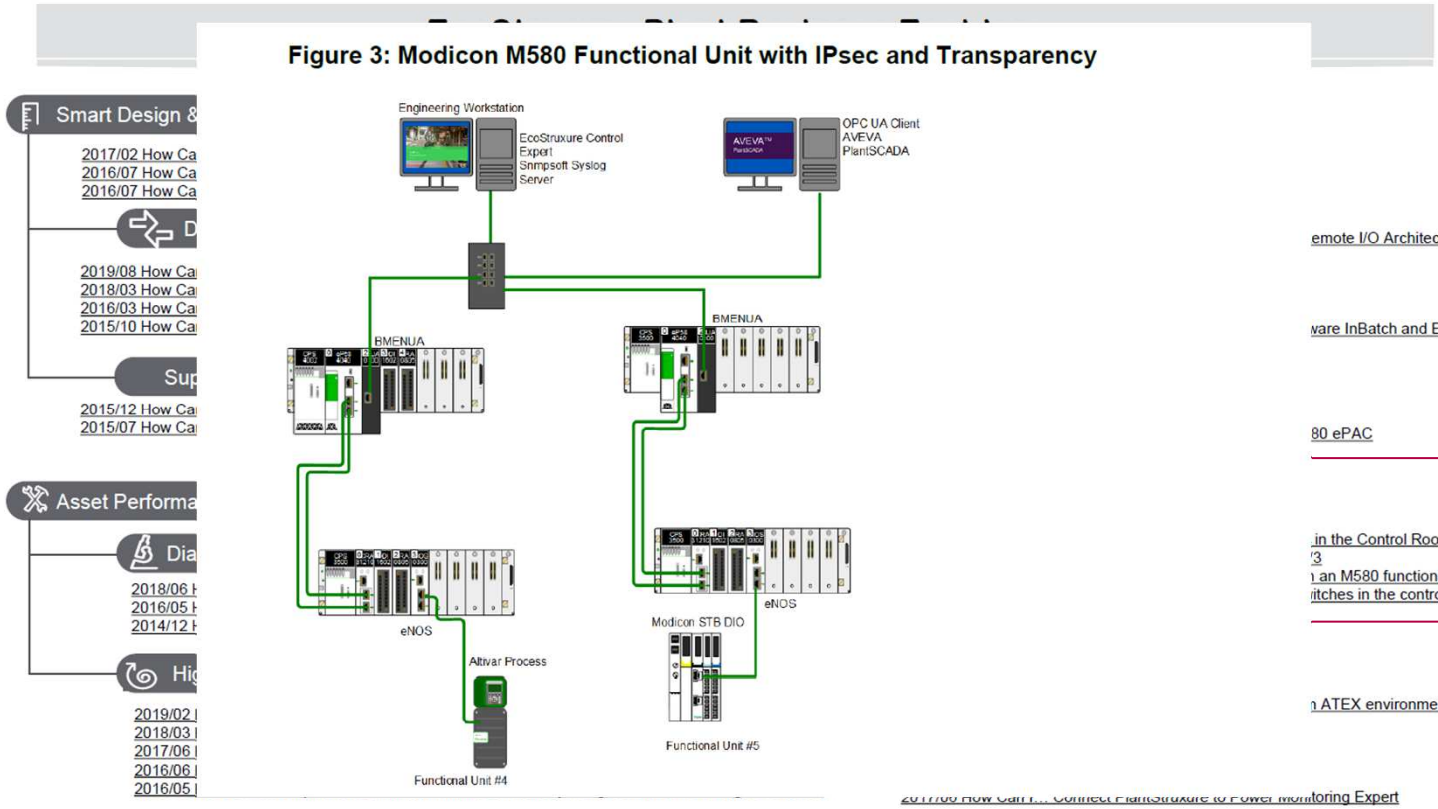
SIS Security Infrastructure Solutions

SECURICON
Information Security Solutions

Internal

Life Is On Schneider Electric

Cyber Security – TVDA documents



Smart Design &

2017/02 How Ca
2016/07 How Ca
2016/07 How Ca

D

2019/08 How Ca
2018/03 How Ca
2016/03 How Ca
2015/10 How Ca

Sup

2015/12 How Ca
2015/07 How Ca

Asset Performa

Dia

2018/06 H
2016/05 H
2014/12 H

Hig

2019/02 I
2018/03 I
2017/06 I
2016/06 I
2016/05 I

emote I/O Architecture to M580 e PAC

ware InBatch and Ecostruxure Hybrid DCS

80 ePAC

in the Control Room V2
3
an M580 functional unit
itches in the control network v1.0

ATEX environments V2

2017/06 How Can I... Connect PlantStruxure to Power Monitoring Expert

Internal

Cyber Security – Product Implementation Strategy

Standards Driven - IEC62443

Our guide line :

- **Robustness**
  - Robustness of Products according to high level certification
    - Any new product must be Achilles level 2 certified

- **Security Features in Products – Standards & Certifications**
  - Comply with local certifications required (US, Europe, China …)
  - Development according to the IEC62443-4-2

- **Security features at system level**
  - Turn the whole PlantStruxure architecture into a real Role Base Access Control

IEC 62443 – Security Levels Definition

IEC 62443 : The standard dedicated to industry devices Cover 3 areas

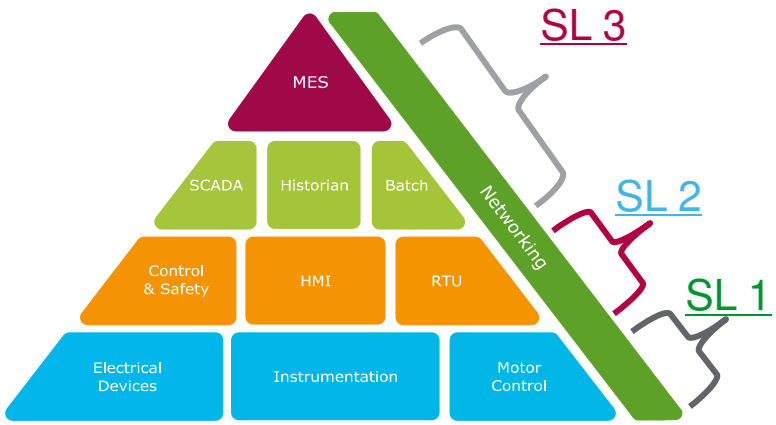
Robustness	CRT	Communication Robustness Testing
Functional	FSA	Functional Security Assessment
Development practices	SDSA	Software Development Security Assessment

IEC62443 defines security levels

PLCs target SL2
IOs target SL1

IEC 62443 Certification is delivered by independent 3rd party

Cover both CRT / FSA / SDSA



Internal

End-to-end cybersecurity

Life Is On Schneider Electric

The three pillars of cybersecurity

Any cybersecurity strategy is only as strong as its weakest link. That's why it is fundamental to identify and mitigate risks by applying standards and good practices throughout the whole line of defense which must integrate people, processes, and technology.

People

Strong cyber protection requires an educated and aware workforce. In many cases, your people are your first and last line of defense. A crucial element of this area is creating and communicating a company-wide security culture, advanced by ongoing training.

Processes

In order to identify and eliminate cyber risks, you need to establish and adhere to good processes, practices, and policies. Companies should begin with consistent, regular risk and threat assessments and gap analyses.

Technology

Your cyber defense is only as strong as the technology deployed to manage and control your operations. This aspect is all about protecting what your company develops and deploys, as well as ensuring that the technology coming from your supply chain vendors is secure.

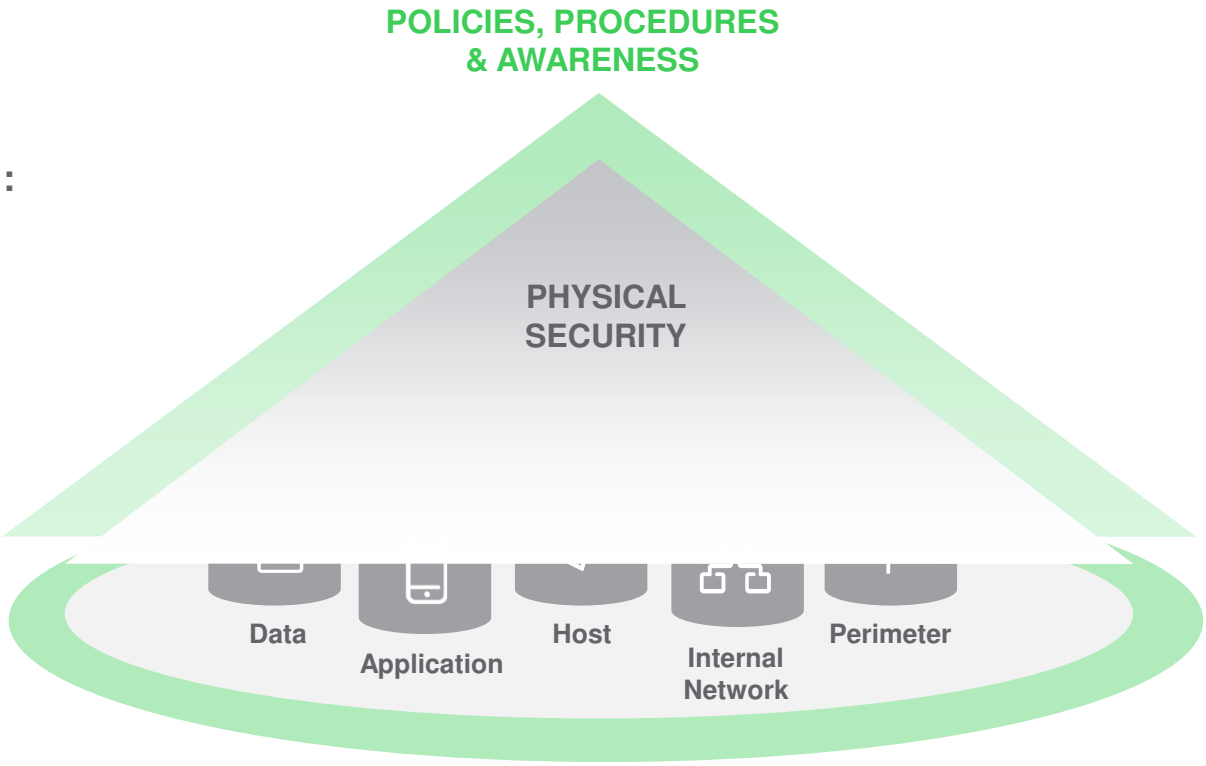
Schneider Electric cybersecurity solutions

Differentiation:

- Depth in IT
- Depth in OT
- Flexible
- Customized

Defense in depth:

- People
- Process
- Technology



Internal

Our differentiation

Ability to implement cybersecurity solutions across varying operating environments including energy management and industrial automation domains.

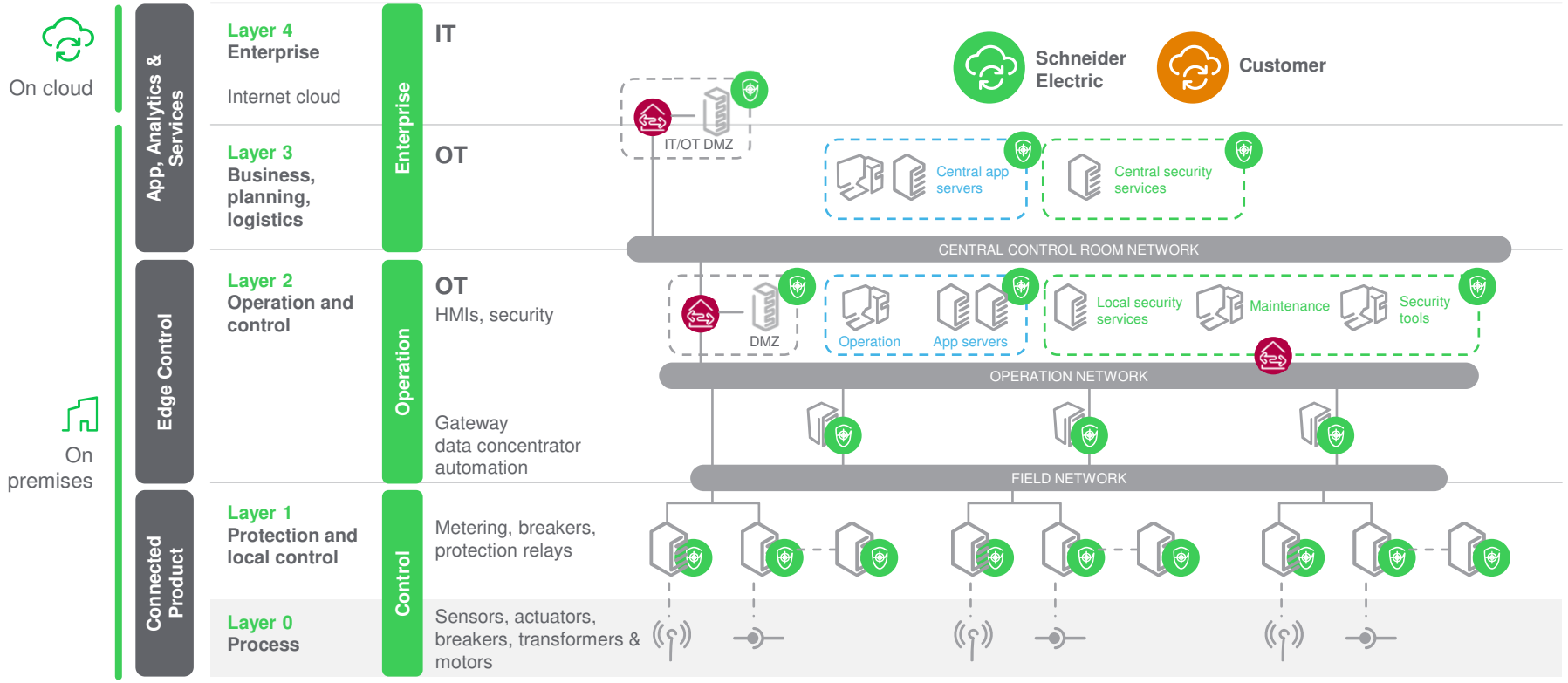
- Vendor-agnostic solution capabilities.
- Understand & apply IT cybersecurity solutions within OT context and perspective.
- Flexible security solutions to ensure maximum value and efficiency.
- Customized controls based on customers' requirements.
- Deep understanding of OT priorities and concerns.

End-to-end cybersecurity with Innovation at Every Level

Internal

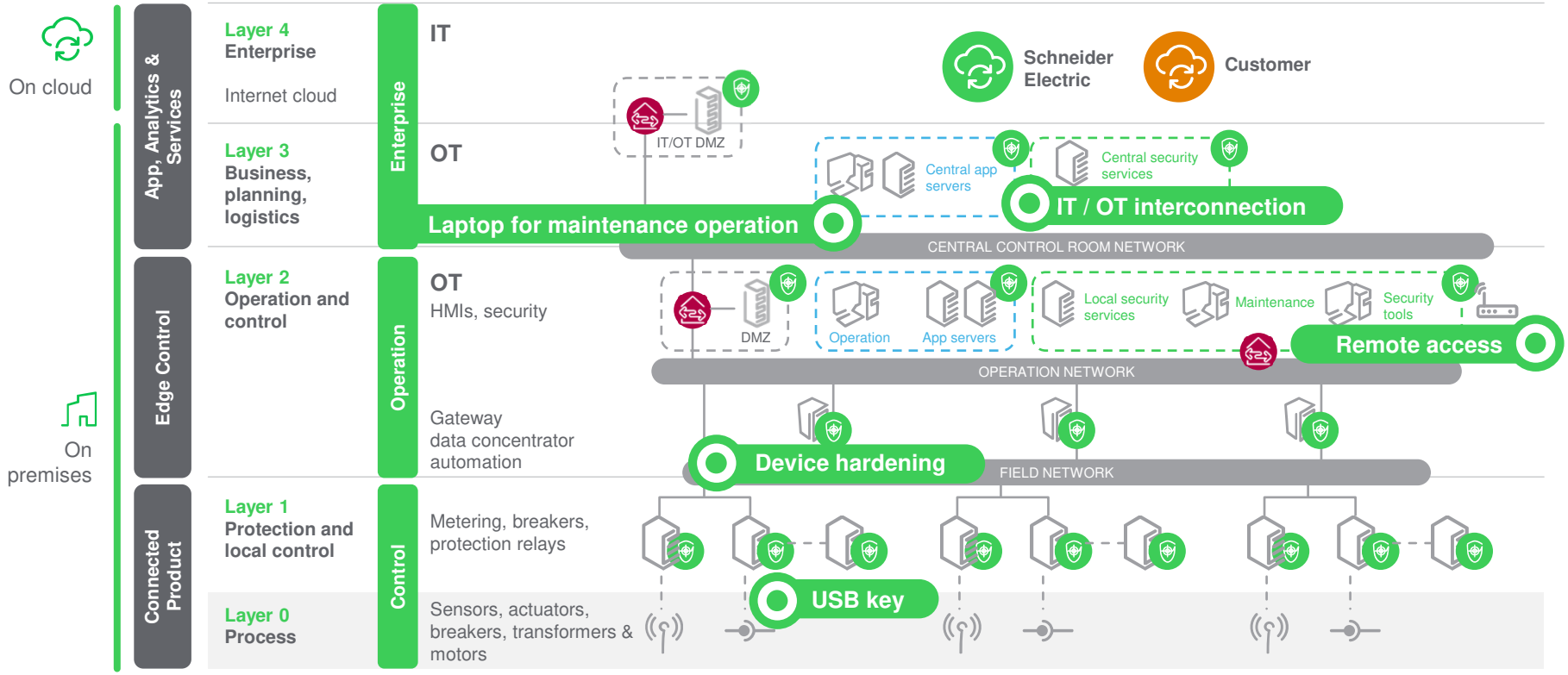
Life Is On Schneider Electric

OT cybersecurity scope



Internal

Major intrusion vectors with OT (risk points)



Internal

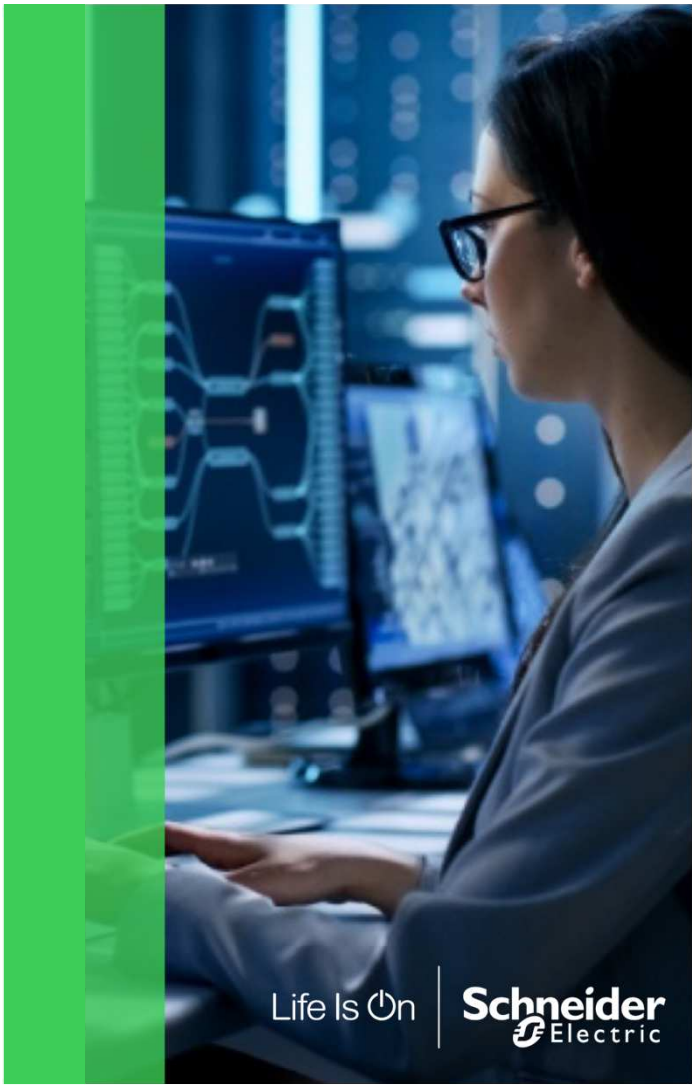
The IACS Stakeholders

The IACS stakeholders span a wide range of people, from suppliers to integrators and asset owners. To establish a robust and effective IACS cybersecurity, all stakeholders share responsibility during all phases of the IACS cybersecurity life cycle.

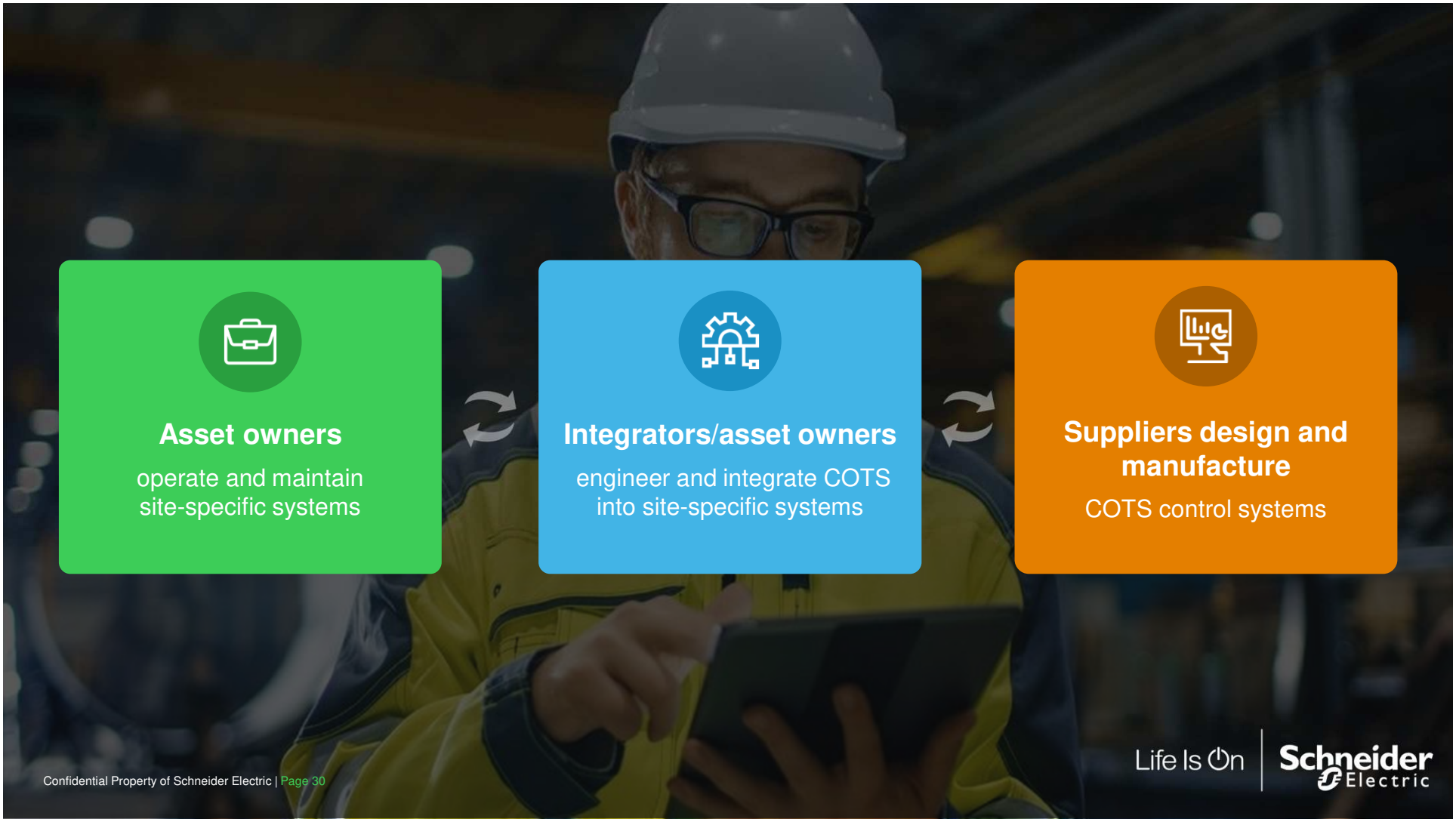
Product suppliers must develop secure-by-design components. These components should include security capabilities to support the use of the products in integrated solutions.

System integrators must use site-specific security best practices to support the cybersecurity requirements for the deployment of products at operational sites.

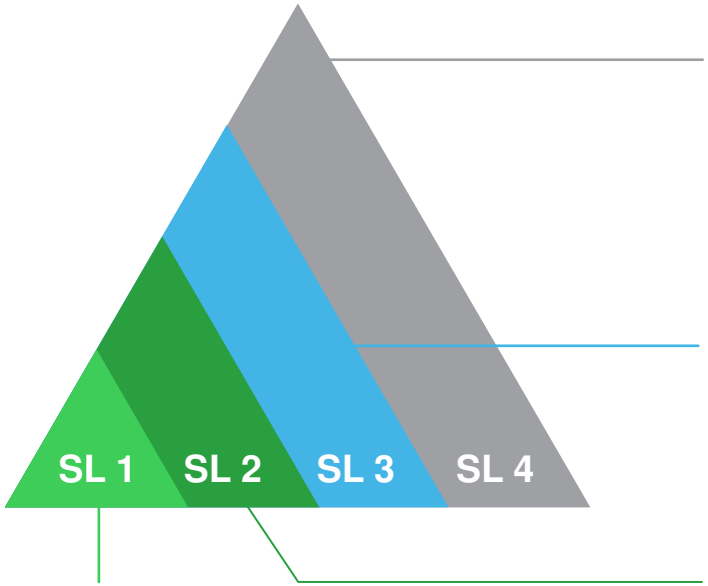
Asset owners must configure, deploy, operate, and maintain the solution in compliance with the approved cybersecurity guidelines.



Internal


Asset owners
operate and maintain site-specific systems
Integrators/asset owners
engineer and integrate COTS into site-specific systems
Suppliers design and manufacture
COTS control systems
Life Is On
Schneider Electric

Security levels within IEC62443



Protection against casual or coincidental violation.

Protection against intentional violation using simple means with low resources, generic skills and low motivation.

Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation.

Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation.

IEC62443-2-4

- Compliance
- requires 24/7 network
- monitoring

Internal

Life Is On Schneider Electric

IEC 62443-3-3 Security Levels Requirements

The foundational security requirements:

Foundational Requirements		Examples
FR1	Identification and Authentication Control (IAC)	IAM principles i.e. user id, authentication and authorization
FR2	Use Control (UC)	Roles and responsibilities enforcement/compliance
FR3	System Integrity (SI)	Change management
FR4	Data Confidentiality (DC)	Encryption
FR5	Restricted Data Flow (RDF)	Firewalls policies/segmentation
FR6	Timely Response to Events (TRE)	Logging, alarms, events
FR7	Resource Availability (RA)	Backup and restore

Life Is On Schneider Electric

Internal

Why ISA / IEC 62443

Information Source ISA GCA

Internal

Life Is On Schneider Electric

Cyber security roadmap

The existing features M580 ePAC

Confidential Property of Schneider Electric

Internal

Life Is On Schneider Electric

Modicon M580, the Most Advanced CyberSecured PAC

Inherent Cybersecure Design

- Firmware **encryption and integrity check**
- Cryptographic **secured communication**
- **Firewall** features – Access Control List
- **Secured** operation modes
- **Know-how** protection
- **Traceability**
- CyberSecurity **Certified**
  - Achilles L2, China, CSPN (France),

Major Benefits

Trusted and Secure Operations

- **Comply** with regulations
- **Reliable** operations
- **Easy** to configure

Life Is On Schneider Electric

Cyber security roadmap

Detailed architectures

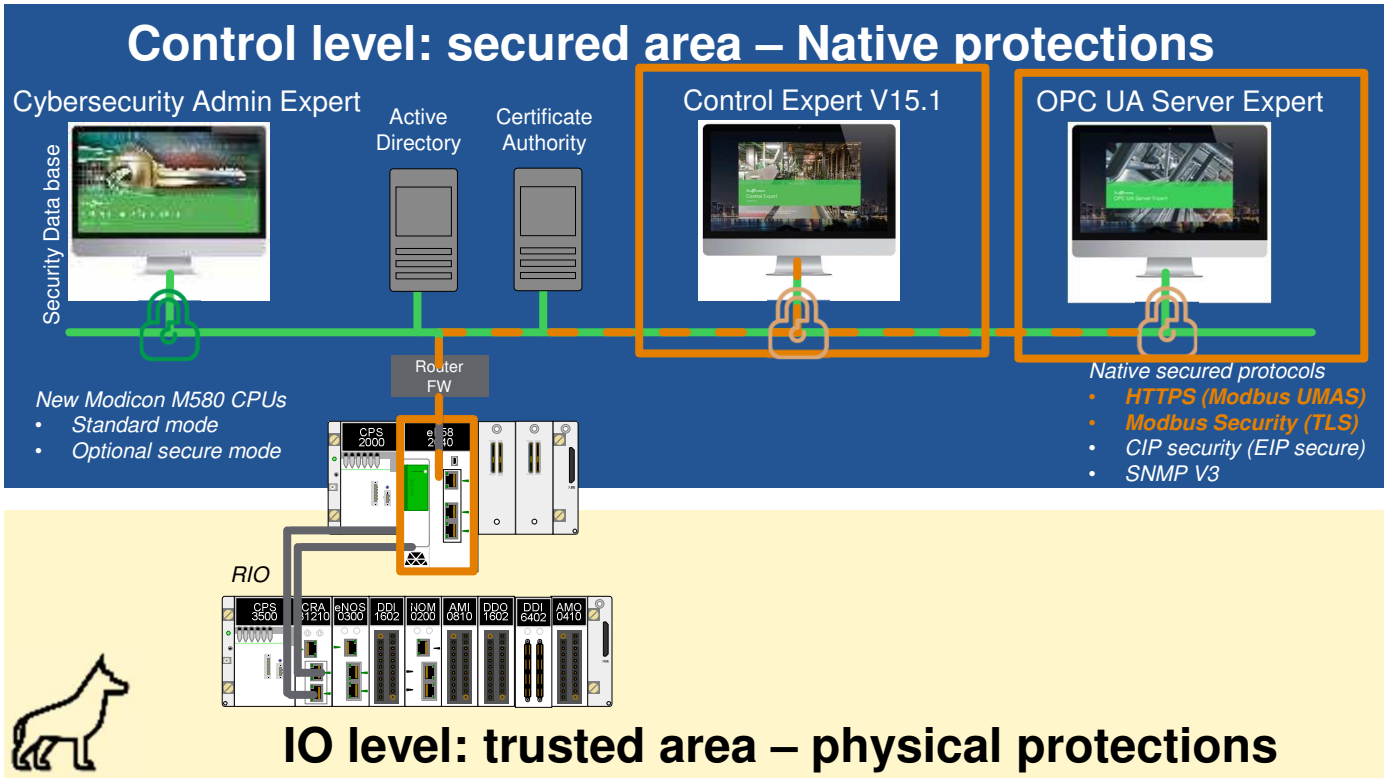
Confidential Property of Schneider Electric

Internal

Life Is On Schneider Electric

Modicon M580 End-to-end security architecture

End-to-end cybersecure control system according to **IEC62443-4-2 Security Level 2**

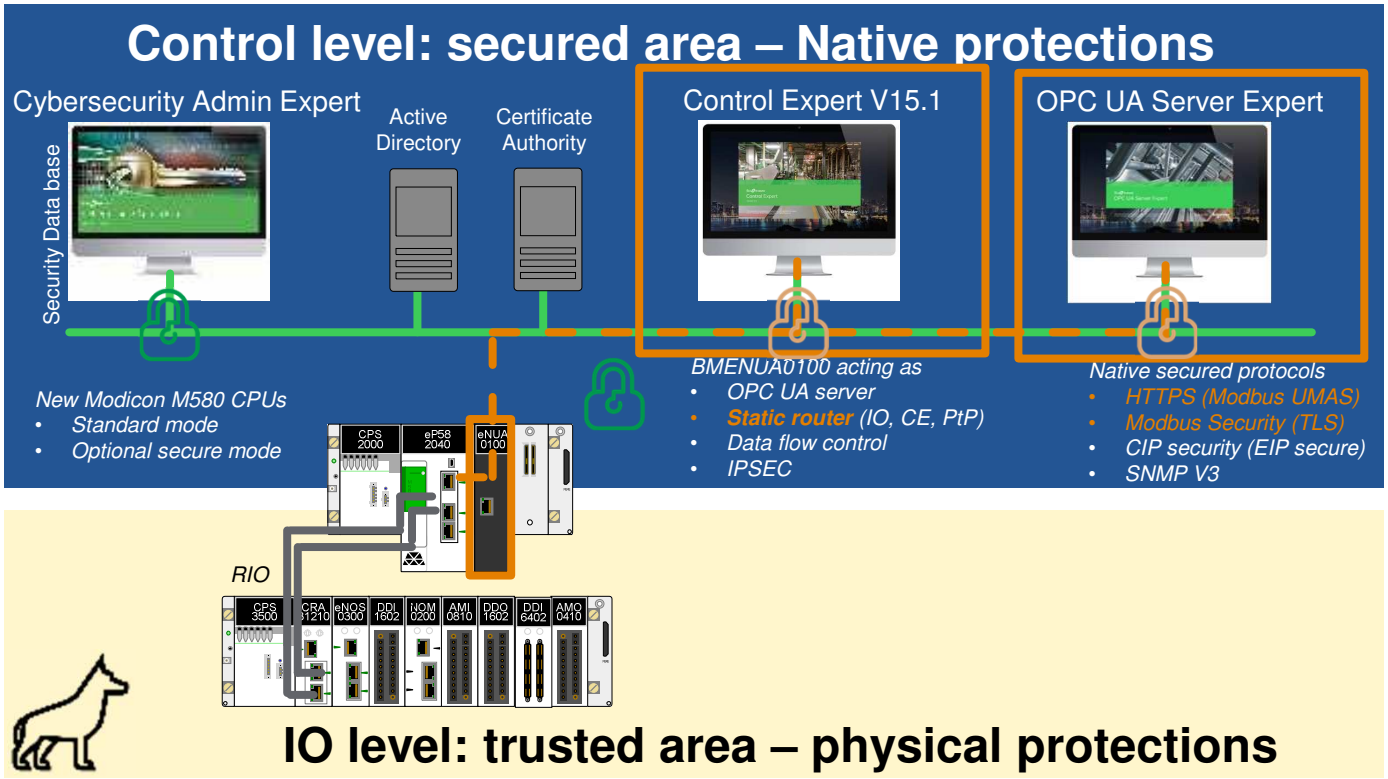


- **End-to-end** cybersecurity at **control level** relying on natively **secured protocols**
- **Any action** (user/machine) authenticated(Certificates) and **authorized** (RBAC) on **PLC**
- **Centralized cybersec configuration** by unique tool (CAE)
- **Hierarchical architecture** via NUA or external router/fw

Internal

Modicon M580 End-to-end security architecture

End-to-end cybersecure control system according to **IEC62443-4-2 Security Level 2**



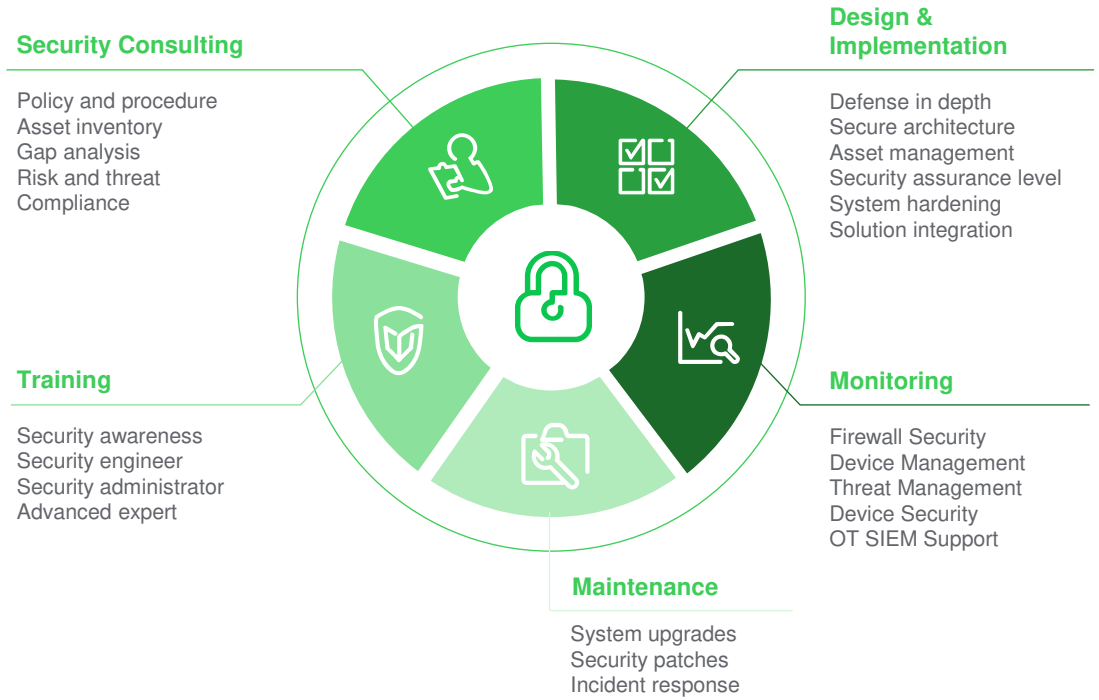
- **End-to-end** cybersecurity at **control level** relying on natively **secured protocols**
- **Any action** (user/machine) authenticated(Certificates) and **authorized** (RBAC) on **PLC**
- **Centralized cybersec configuration** by unique tool (CAE)
- **Hierarchical architecture** via NUA or external router/fw

Internal

Our approach for your operational life cycle

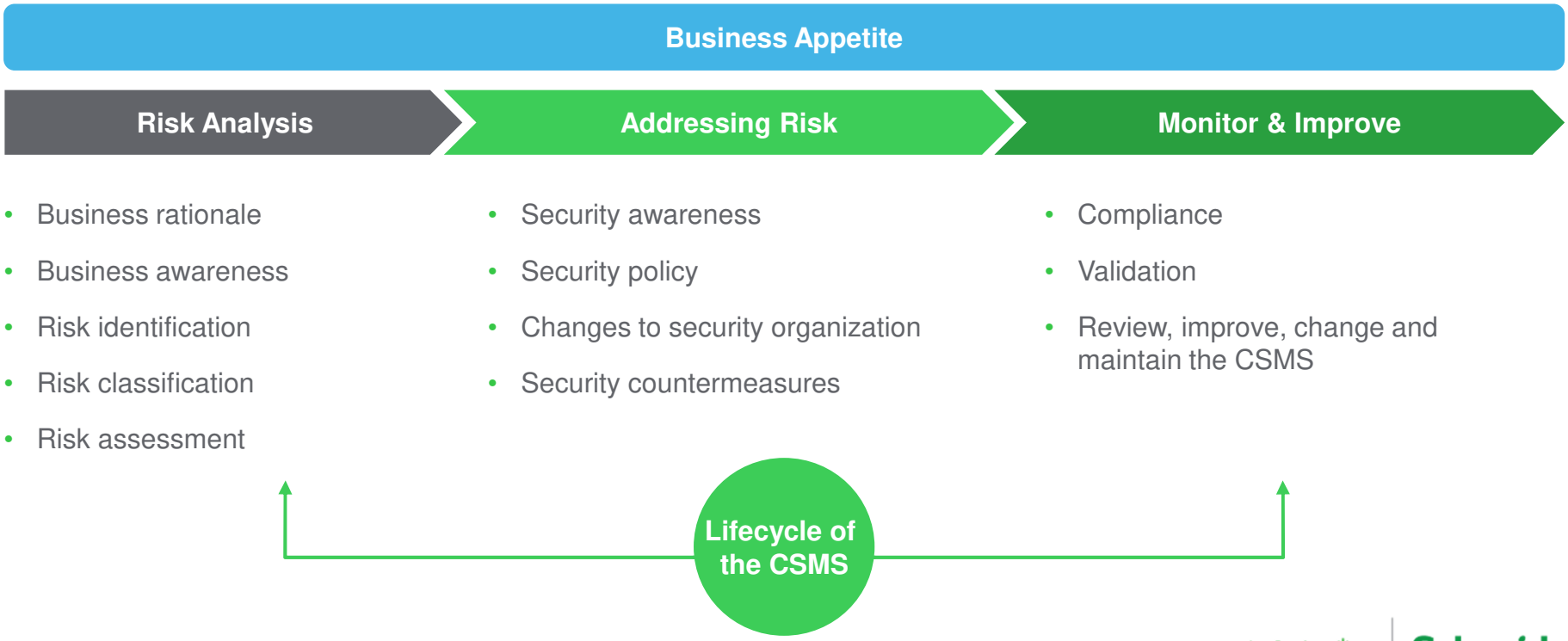
Schneider Electric is committed to providing solutions that support your needs for cybersecurity protection across all business types and industries. We apply a rigorous mindset, policies, and methodologies in the development of our products and the implementation of our solutions.

Skilled and certified professionals provide vendor-agnostic services to help you assess your risk, implement cyber specific solutions, and maintain your defenses over time at your location.



Internal

IEC 62443 Cyber Security Management System (CSMS)



Internal

Cybersecurity solutions portfolio

The solutions we design and implement are flexible and customized to meet your specific needs and requirements. The most critical cybersecurity solution elements are defined in four categories.

Permit - manage access to operations systems and information through network and physical controls.

Protect - implement specific controls as part of the operations systems for ongoing protection.

Detect - monitor the operating environment to detect and communicate threats.

Respond - develop procedures and systems to support rapid response to cyber incidents to contain and mitigate attacks.

Permit	Protect	Detect	Respond
• Authentication, Authorization, Accounting • Multi-Factor Authentication • Network Segmentation • Secure Remote Access • Physical Security	• Endpoint Protection, Anti-malware • DLP, HIPS, Whitelisting • Removeable Media Control • Patch Management	• Security Information & Event Management (SIEM) • Network Performance Monitoring • Asset Identification • Anomaly Detection • Intrusion Detection	• Backup / Disaster • Recovery • Forensics • Incident Response

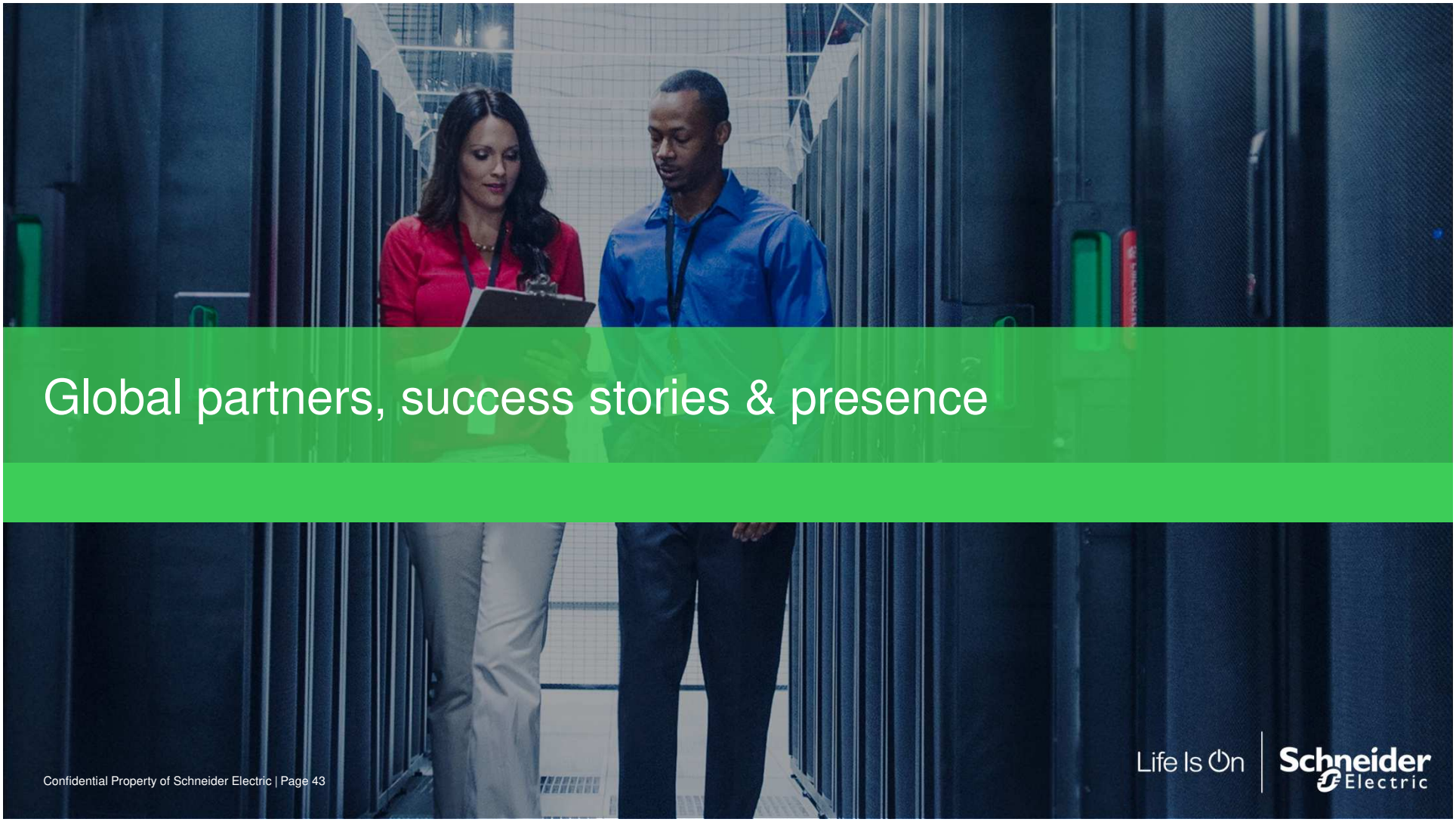
Internal

Life Is On Schneider Electric

Contact information

Name : Peter Fuglsang
Title : Product Application Engineer
Country : Denmark
Email : peter.fuglsang@se.com
Mobile phone : +4520205511

Name : Graham Rennie
Title : System & Architecture Engineering
Country : United Kingdom
Email : graham.rennie@se.com



Global partners, success stories & presence

Life Is On Schneider Electric

Drawing on our ecosystem of partners

Internal

Life Is On Schneider Electric

Cybersecurity success stories

Site #1

France

Leading food production company

Cyber offering:

- IT / OT integration.
- DMZ implementation.
- Design and deploy secured architecture.
- Global user management system, network monitoring.
- Secure remote access, device control.

Success factor:

- Customized solution meeting customer's global operation demands.
- French team customer relationship management.
- Centralized host and network solutions meeting industry and national standards.

Why Schneider:

- Regional security expertise supported by global organization.
- Strong IT / OT solutions providing a flexible offer.
- Significant process level security capabilities complemented by network and host-based security solutions.

Internal

Cybersecurity success stories

Site **#2**

UK

Industry #1 beverage company

Cyber offering:

- Remote access cybersecurity solution.
- 141 global manufacturing sites.
- Remote desktop solution offering full IT/OT separation with military grade hardware.
- Multi-factor authentication.
- Configuration and user management.
- Threat analysis and patch management.

Success factor:

- Customized solution meeting customer's global operation demands.
- UK team customer relationship management.
- Local installation and site support offer.

Why Schneider:

- Regional security expertise supported by global organization.
- Fully compliant with ISA/IEC62443.
- Ongoing comprehensive service offer.
- OT provider with IT expertise.

Internal

Cybersecurity success stories

Site **#3**

Qatar

LNG leader within the Middle East

Cyber offering:

- Cybersecurity Demilitarized Zone (DMZ) implementation.
- Modernization of CS controls in OT network.
- 3rd party IT / OT integration for ICS.

Success factor:

- ICS vendor agnostic (independent) approach.
- Customized systems offered for ICS, OT Network, + IT interface
- Fast track opportunity / rapid response, customer relationship management.

Why Schneider:

- Strong regional and global cybersecurity expertise & presence.
- Customization of security controls and integration with 3rd party solutions.
- Expertise in a large spectrum covering enterprise IT & ICS within OT.

Internal

International standards compliance

Internal

Life Is On Schneider Electric

Global reach

Schneider Electric has a rapidly growing global team focused on cybersecurity. We leverage a strong IT experience and deep knowledge of the OT world to help customers understand what they have today and where the biggest gaps are in managing cybersecurity.

Our quick reaction team is ready to help our customers act quickly in case of a cyber attack – to assess potential damages and recover.

Schneider Electric is a proud member of:

- ISA Global Cybersecurity Alliance
- Cybersecurity Coalition
- Cybersecurity Tech Accord

Team certifications

Internal

Cybersecurity Virtual Academy

The earlier you start with a security mindset, the better. Investing in awareness and training is much less expensive than the cost of remediation, a damaged reputation, and downtime.

At Schneider, we share information externally through our Cybersecurity Virtual Academy. This virtual academy provides:

- Value-added content
- Engages customers, prospects, and other interested groups in an ongoing dialogue about cybersecurity topics

Internal

Strengthening your cybersecurity

Strong cybersecurity is a business requirement.

Secure data collection and transmission is critical when harnessing the benefits of IoT.

Schneider Electric is committed to supporting your digital transformation.