Who is Schneider Electric?

Schneider Electric provides energy and automation digital solutions for efficiency and sustainability

SQUARE D by Schneider Electric

APC by Schneider Electric

AVEVA

Key figures for 2022

5% of revenues devoted to R&D

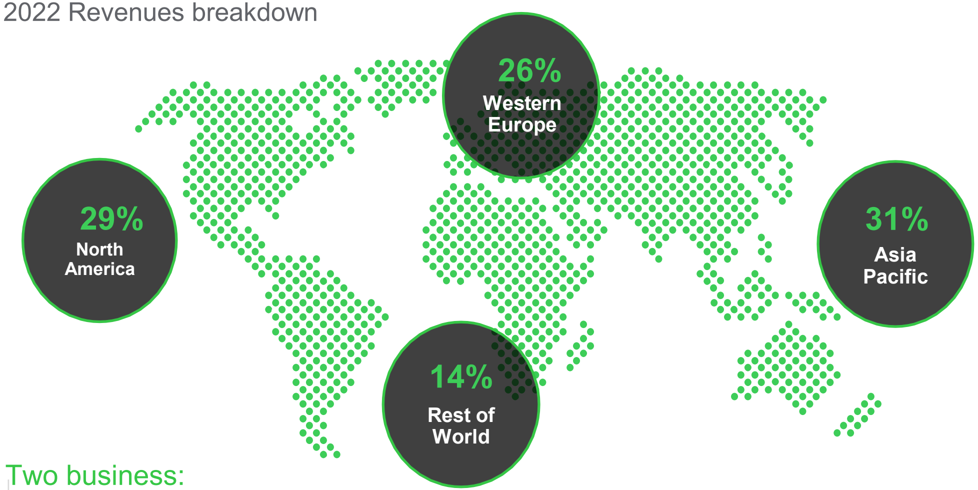
€34 billion
2022 revenues

43%
of revenues in new economies

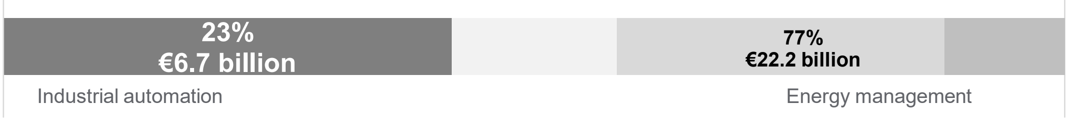
128,000+
Employees in over 100 countries

A well-balanced global presence

2022 Revenues breakdown



Two business:



Life Is On Schneider Electric

We partner in everything we do

650k service providers & partners

42k+ system integrators & developers

52k+ unique suppliers

Overview: ISA/IEC 62443 Standards

The world’s only consensus-based automation and control systems security standards

The ISA99 committee was **formed in 2002** and works closely with IEC Technical Committee 65

ISA/IEC 62443 standards contain **over 500 normative requirements** that address all phases of the system life cycle

Over 1,500 volunteer members represent a wide range of industry sectors and constituencies from all areas of the world

ISA/IEC 62443 standards address OT in 16 CI sectors, non-telecom & finance

ISA/IEC 62443 are the **most referenced** standard in the NIST Cybersecurity Framework

Formal and informal liaison relationships with IEC, OPAF, NAMUR, WIB, NIST, DHS, INL, ISASecure, and ISAGCA

Value: ISA/IEC 62443 Standards

Structured Approach to Operational Technology (OT) Security: ISA/IEC 62443 protects against cyber threats and ensure the reliability, safety and integrity of industrial operations.

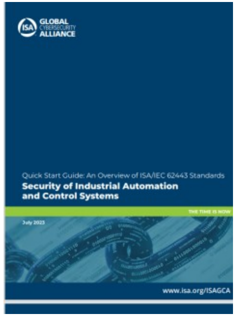
Global Consistency: ISA/IEC 62443 is an international standard, which is a common framework that can be adopted by organizations worldwide. Both supplier organizations and asset-owner organizations operate globally and benefit from conformance to a single international standard.

Risk Mitigation: ISA/IEC 62443 standards help organizations assess and mitigate the risks associated with cyber attacks on their industrial control systems. They provide a structured approach to identifying vulnerabilities and implementing measures to protect against threats.

Vendors and Supply Chain: These standards provide guidance on cybersecurity when procuring and integrating control systems from different vendors. This helps ensure security is built into the supply chain.

Compliance and Certification: Requiring compliance to ISA/IEC 62443 demonstrates cyber readiness. Conformity assessment programs like ISASecure have been available for 13 years, providing transparency for asset-owner procurement activities and operational security status.

Free Resource available: Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control



ISA GLOBAL CYBERSECURITY ALLIANCE

Quick Start Guide: An Overview of ISA/IEC 62443 Standards

Security of Industrial Automation and Control Systems

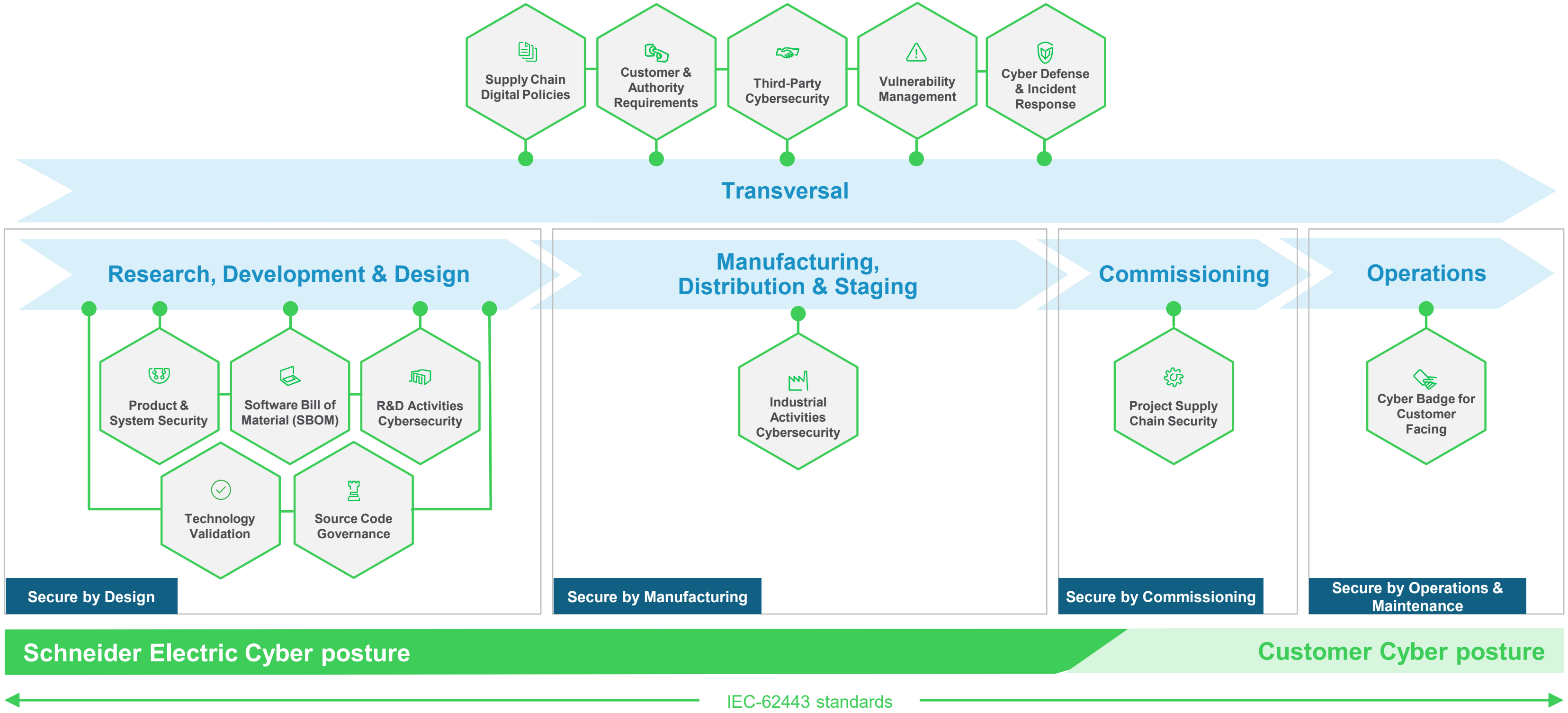
THE TIME IS NOW

July 2023

www.isa.org/ISAGCA

Schneider Electric’s Supply Chain Security

We seek to embrace the whole value chain from security by design to secure operations with a comprehensive set of programs…


Supply Chain Digital Policies
Customer & Authority Requirements
Third-Party Cybersecurity
Vulnerability Management
Cyber Defense & Incident Response
Transversal
Research, Development & Design
Product & System Security
Software Bill of Material (SBOM)
R&D Activities Cybersecurity
Technology Validation
Source Code Governance
Secure by Design
Manufacturing, Distribution & Staging
Industrial Activities Cybersecurity
Secure by Manufacturing
Commissioning
Project Supply Chain Security
Secure by Commissioning
Operations
Cyber Badge for Customer Facing
Secure by Operations & Maintenance
Schneider Electric Cyber posture
Customer Cyber posture
IEC-62443 standards

… with main components and owners for each pillar

1 Supply Chain Digital Policies

- Inventory of policies and regulation
- Impact analysis through key offers
- Change plan and timelines

2 Customer & Authority Requirements

- Accurate and standard security info made available on key offers
- Customer & authorities' requirements satisfied accurately/timely

3 Technology Validation

- Reviewed by U.S. Department of Energy's CyTRICS program
- Closed any findings from CyTRICS program
- Static Code Analysis
- GSL Pen Test Completed

4 Cyber Badge for Customer Facing

- Securing the endpoints of front-line people
- Training & Awareness (role-based)
- Secure commissioning and hardening guidance

5 Industrial Activities Cybersecurity

- Each industrial site is certified with IEC62443
- Cybersecurity leader is appointed
- Site Cyber performance indicator is at the highest level

6 Project Supply Chain Security

- IEC 62443 Site certification
- PaSCoS part of project governance
- Cybersecurity site leader appointed

7 Product & System Security

- Compliant to Secure Development Lifecycle
- Compliant to final cybersecurity reviews and Digital Offer certification

8 Vulnerability Management

- Incorporated into CPCERT
- Producing SBOMs with every release

9 Software Bill of Material (SBOM)

- SBOM is made available for key offers

10 Third-Party Cybersecurity

- Key direct and indirect procurement suppliers are assessed
- Key suppliers' contract are augmented with Cyber T&C

11 Source Code Governance

- Offer is compliant with Source Code Security Policy
- Alignment with Corporate development tooling

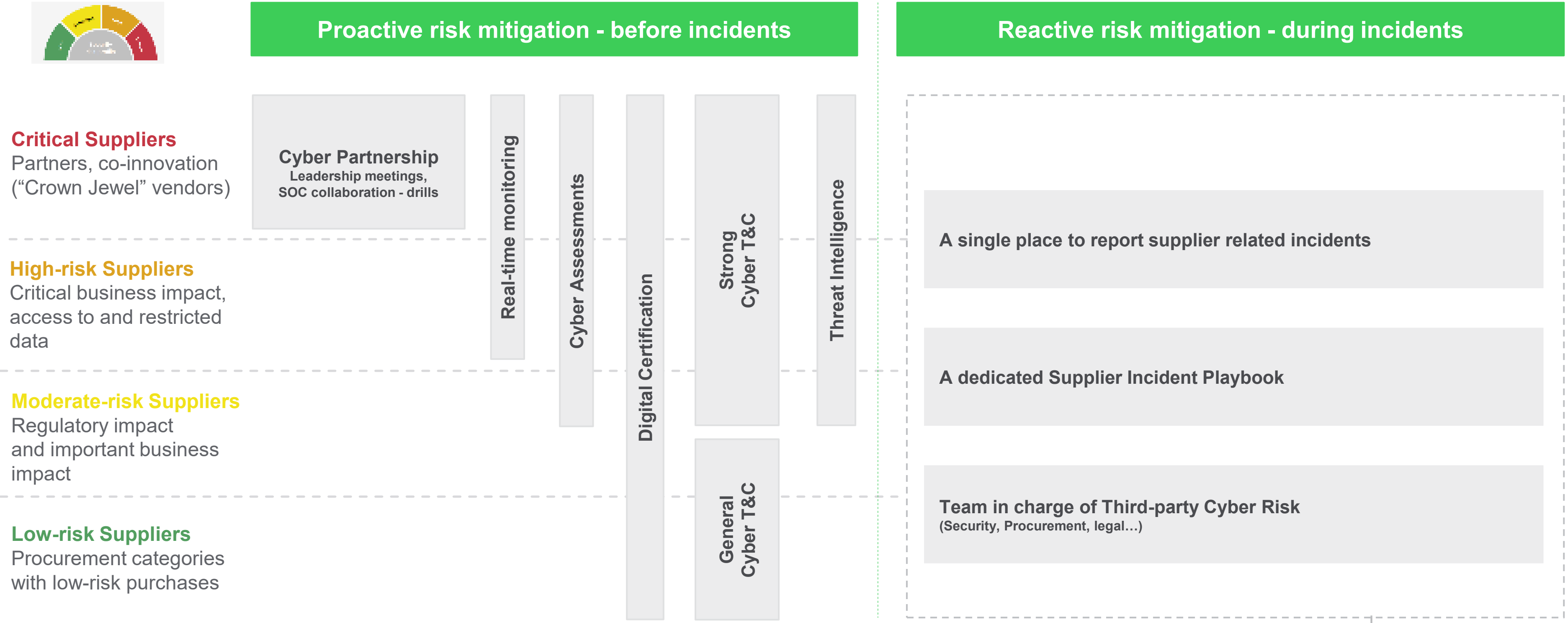
12 R&D activities Cybersecurity

- Site certification to the R&D Site Framework control set (based on IEC, NIST & ISO27K)
- Cybersecurity leader is appointed
- Site Cyber performance indicator is at the highest level

13 Cyber Defense & Incident Response

- Active monitoring for threats is in place
- Detection of IP and Source Code leakage
- Detection of key data leak is in place

Our 80 commodities and €14B spent are governed through a tiered approach, based on risk profiles



Proactive risk mitigation - before incidents

Reactive risk mitigation - during incidents

Critical Suppliers
Partners, co-innovation
(“Crown Jewel” vendors)

High-risk Suppliers
Critical business impact, access to and restricted data

Moderate-risk Suppliers
Regulatory impact and important business impact

Low-risk Suppliers
Procurement categories with low-risk purchases

Cyber Partnership
Leadership meetings, SOC collaboration - drills

Real-time monitoring

Cyber Assessments

Digital Certification

Strong Cyber T&C

General Cyber T&C

Threat Intelligence

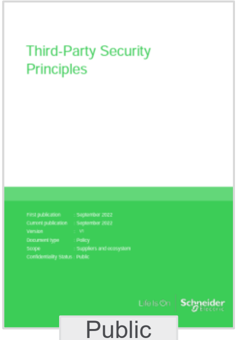
A single place to report supplier related incidents

A dedicated Supplier Incident Playbook

Team in charge of Third-party Cyber Risk
(Security, Procurement, legal…)

We rely on a set of policies and agencies to make it happen

Set of guidelines



Third-Party Security Principles

First publication : September 2022
Current publication : September 2022
Version : V1
Document type : Policy
Scope : Suppliers and ecosystem
Confidentiality Status : Public

Life Is On | Schneider Electric

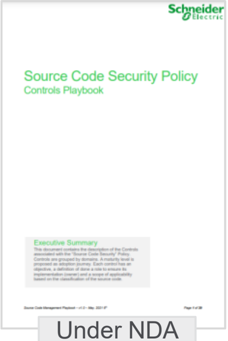
Public

Technical security requirements for Third Parties

First publication : December 2022
Current publication : December 2022
Version : 2.0
Document type : Standard
Scope : Global
Confidentiality Status : Restricted

Life Is On | Schneider Electric

Under NDA



Schneider Electric

Source Code Security Policy
Controls Playbook

Executive Summary
This document contains the description of the Controls associated with the "Source Code Security" Policy. Controls are grouped by domains. A maturity level is proposed as adoption journey. Each control has an objective, a definition of done a role to ensure its implementation (owner) and a scope of applicability based on the classification of the source code.

Source Code Management Playbook – v1.0 – May. 2021 6" Page 1 of 38

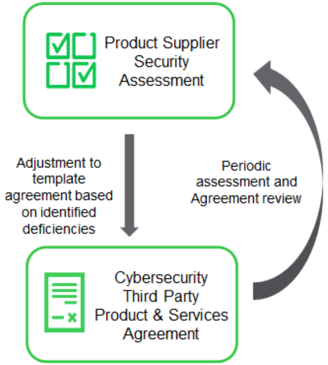
Under NDA

Assessments & Real-time monitoring

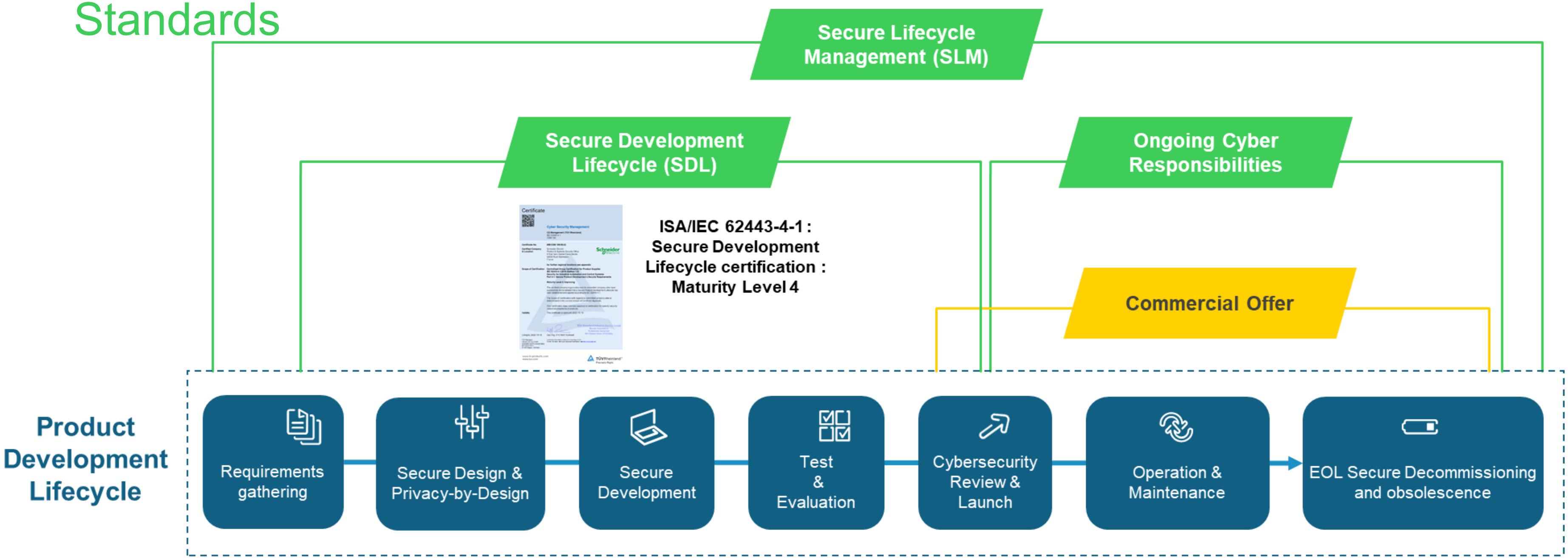
riskrecon

SecurityScorecard

BITSIGHT


Product Supplier Security Assessment
Adjustment to template agreement based on identified deficiencies
Periodic assessment and Agreement review
Cybersecurity Third Party Product & Services Agreement

Our Software Assurance Practices are designed from International Standards



Secure Lifecycle Management (SLM)

Secure Development Lifecycle (SDL)

Ongoing Cyber Responsibilities

Commercial Offer

ISA/IEC 62443-4-1 : Secure Development Lifecycle certification : Maturity Level 4

Product Development Lifecycle

Requirements gathering

Secure Design & Privacy-by-Design

Secure Development

Test & Evaluation

Cybersecurity Review & Launch

Operation & Maintenance

EOL Secure Decommissioning and obsolescence

Key

🟦 Lifecycle phase
🟨 Operational
🟩 Practices

CREST. PEN TEST

CREST pen-testing certification attests to Schneider Electric's skills and proficiency when testing resilience and security

ISO/IEC 29147 and ISO/IEC 30111 : Vulnerability Management and Disclosure processes certification

We start by scrutinizing the security of our R&D sites, with a global Cyber Framework that adapts to the sites' complexities

BASIC → INTERMEDIATE → ADVANCED

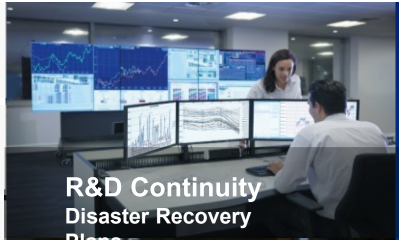
Cyber Leaders
Site security control compliance

Awareness
Training, assets

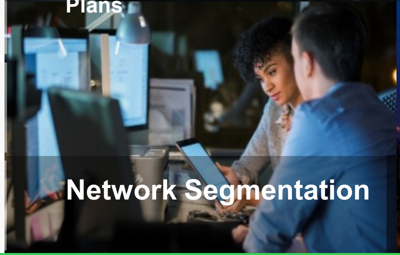
Asset Inventory
Ownership & Accountability

R&D Site Maps
Topography

Protection
Vulnerabilities, Malware and Remediation



R&D Continuity
Disaster Recovery Plans



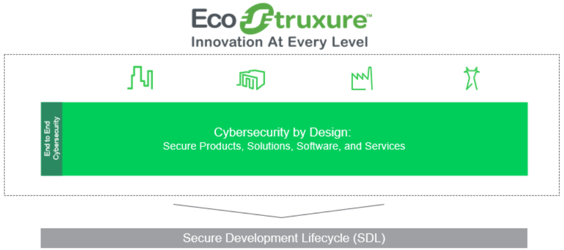
Network Segmentation

Red/Blue Team Site Penetration Tests for Validation of Security Posture and Incident

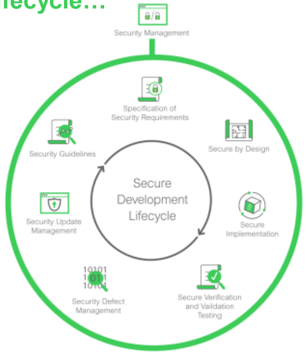
Continuous Threat Detection & Incident Response

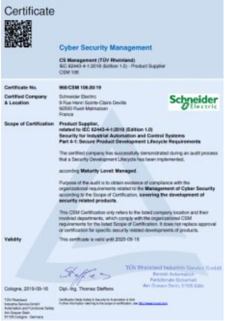
We then ensure that when we deploy Product, Software & Systems, security is there "by design"

Security is embedded by design…


EcoStruxure
Innovation At Every Level
End to End Cybersecurity
Cybersecurity by Design:
Secure Products, Solutions, Software, and Services
Secure Development Lifecycle (SDL)

…it follows the Secure Development Lifecycle…


Security Management
Specification of Security Requirements
Secure by Design
Secure Implementation
Secure Verification and Validation Testing
Security Defect Management
Security Update Management
Security Guidelines
Secure Development Lifecycle



Certificate

Cyber Security Management

CS Management (TÜV Rheinland)
IEC 62443-4-1:2018 (Edition 1.0) - Product Supplier
CSM 106

Certificate No. **968/CSM 106.00/19**

Certified Company & Location
Schneider Electric
9 Rue Henri Sainte-Claire Deville
92500 Rueil-Malmaison
France

Scope of Certification
Product Supplier,
related to IEC 62443-4-1:2018 (Edition 1.0)
Security for Industrial Automation and Control Systems
Part 4-1: Secure Product Development Lifecycle Requirements

The certified company has successfully demonstrated during an audit process that a Security Development Lifecycle has been implemented.

according **Maturity Level: Managed**.

Purpose of the audit is to obtain evidence of compliance with the organizational requirements related to the **Management of Cyber Security** according to the Scope of Certification, **covering the development of security related products**.

This CSM Certification only refers to the listed company location and their involved departments, which comply with the organizational CSM requirements for the listed Scope of Certification. It does not replace approval or certification for specific security related developments of products.

Validity This certificate is valid until 2020-09-16

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2019-09-16 Dipl.-Ing. Thomas Steffens

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see [illegible]

Our Secure Development Lifecycle (SDLv2) process is officially certified against IEC 62443-4-1 standard.

…R&D teams use secure infrastructure and code analysis tools….

…Products, Software, and Systems are penetration tested in the CREST-accredited Schneider Electric Global Security Labs…

…all driven through education and maturity….

People

- Leadership
- Security Officers
- Cybersecurity Advisors
- R&D teams
- Edisons

Training/awareness

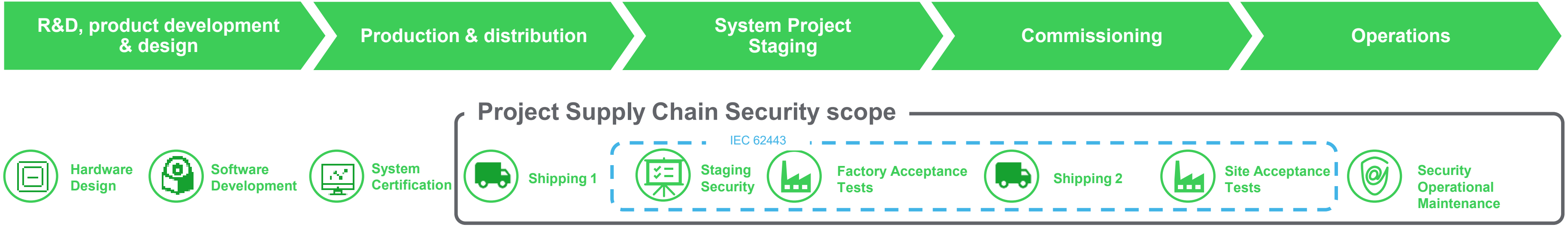
- Technical Expert Material
- Extensive training & webinars
- White papers
- Vulnerabilities & Incidents

… while collaborating & influencing industry, governments, and regulators

ISO IEC enisa ANSSI ISA U.S. DEPARTMENT OF ENERGY

Life Is On Schneider Electric

We also apply this metholodology to our Project Supply Chain



Project Supply Chain Security controls cover 6 key milestones of the customer “project supply chain”

1. Shipping 1

Sanity Check / Integrity / Protection of shipment.

Reception of the elements to be **assembled**, they come from Schneider production sites or from subcontractors.

2. Staging Security

Adequate secure testing environment.

Warehouse **storage, inventory and separation** of different projects.

3. Factory Acceptance Tests

Secure assembly / Hardening of systems.

Testing in a simulated environment of the equipment to be delivered to the customer.

4. Shipping 2

Sanity Check / Integrity / Protection of shipment.

Shipping of ordered items to the customer.

5. Site Acceptance Tests

Secure integration of systems in customer environment.

Reception and installation of the **new system on the customer site.** Connection with pre-existing equipment.

6. Security Operational Maintenance

Antivirus update / System update.

Maintenance phase to **ensure the continued operability** of the newly installed system.

We finally ensure Customer-Facing Populations is individually certified before meeting customer or accessing customer site

To go even further in the building of a trust relationship with our customers, Schneider Electric has launched an initiative to ensure a consistent level of security when interacting with customers: **The Cyber Badge**.

Cybersecurity measures

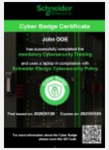
Use of secure endpoints compliant with security requirements, up-to-date and monitored

Cybersecurity trainings enforcing cyber discipline at customer sites and remotely

Regular controls by a dedicated central team to enforce Cyber Badge across Customer Facing Populations

Cyber incident prevention, detection and reporting leveraging Schneider Electric Security Operations Center

Visible on customer side



Schneider Electric

Cyber Badge Certificate

John DOE

has successfully completed the mandatory Cybersecurity Training

and uses a laptop in compliance with Schneider Electric Cybersecurity Policy

First issued on: 2020/07/28 Expires on: 2021/07/28

For more information about the Cyber Badge please scan this QR Code

Customer Facing Populations are issued a **virtual badge** delivered for a 3-month validity period as a proof of compliance

Restrictions enforced over non-compliant staff to avoid interactions with customers until compliance is achieved

The Cyber Badge policy is published online on the *Cyber Badge Principles*

Policy Considerations

- Very few states speak to a best practice like ISA/IEC 62443 or equivalent standard in their plans, rules or laws.

- In energy sector unclear which chapter of law for cybersecurity standards with building codes, consumer protection and utility regulations all nipping at edges of DERs in homes and buildings.

- Cybersecurity Advisory Team for State Solar (CATSS) Tool Kit is available to you – use it. NASEO & NARUC ran excellent stakeholder process with many options to address cybersecurity within state “retail” authority.

For More Information--

Jeff Morris
Senior Director, State Government Relations
Schneider Electric North America
jeff.morris@se.com