Securing CPG for the future

Cybersecurity solutions and services
Table of contents

Challenges & solutions

1. How Schneider Electric secures CPG

2. Digitization priorities

3. Our cybersecurity approach
Challenges & solutions

- Challenges & solutions
- Digitization priorities
- How Schneider Electric secures CPG
- Our cybersecurity approach
Dedicated to help facing the challenges of the CPG industry

- **Changing consumer demands**: Need to manage an important number of SKUs.
- **CapEx and OpEx constraints**: Need to extend life of aging equipment.
- **Climate change and resource scarcity**: Need to optimize the use of raw materials, energy, and water.
- **Consumer trust and regulation**: Need more product information, and traceability.
- **Changing workforce demographics**: More difficult to attract and retain talent.

**Challenges & solutions**

**Digitization priorities**

**How Schneider Electric secures CPG**

**Our cybersecurity approach**
Improving flexibility, traceability and sustainability of your operations from farm to fork

**Improve operations**
Transform your operations to improve efficiency and yield, while increasing flexibility to boost your competitiveness.

**Maximize asset value**
Reduce time to market and maximize asset’s reliability, performance and lifetime, leveraging the power of digital twins, IoT & analytics.

**Protect environment**
Meet your energy and sustainability goals and reduce costs with smart energy, water and waste management for your facilities.

**Manage quality and compliance**
Ease food safety compliance and increase traceability to preserve brand equity and shareholder value.

**Empower workforce**
Provide workers with mobility, guidance and collaboration for improved decision support in complex CPG environment.

---

**Challenges & solutions**

- **Digitization priorities**
- **How Schneider Electric secures CPG**
- **Our cybersecurity approach**

---

**Improvements**

- **40%** Flexibility increase
- **30%** CapEx savings
- **20%** Energy cost reduction
- **99%** Data collection time reduction
- **2x** Faster incident reduction
Increase efficiency, traceability and sustainability across the whole CPG value chain...

Leveraging digital transformation with Schneider Electric solutions

Digital engineering
Cut time, cost, and minimize risk of capital project engineering.

Asset performance
Maximize return on asset investment.

Workforce empowerment
Improve knowledge, performance & efficiency of plant workers.

Food safety & traceability
Ensure quality & compliance while increasing trust across the product life cycle.

Energy & sustainability
Meet your company sustainability goals.

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach

- Digital Twin Creation
- 3D Design
- Building Information Modelling
- Electrical CAD
- Machine Simulation

- APM Assessment
- Asset Information & Analysis
- Asset Maintenance
- Advanced Process Control
- Artificial Intelligence
- Modernization Services

- Operator Training Simulator
- Operator of the Future
- Workflow Management
- Knowledge & Continuous Improvement
- Management of Staff Scheduling

- Food Defense
- Cybersecurity
- Plant Traceability
- Label Assurance
- Track & Trace
- Digital Calibration
- Food Safety Management

- Strategic Energy Sourcing
- Sustainability & Energy Consulting
- Sustainable Access to Energy
- Energy as a Service
We help on every step of the value chain

Efficient facilities
Safer, more available, and greener resources

Resilient supply chain
Manage complexity and improve visibility

Agile manufacturing
Boost manufacturing flexibility & efficiency

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
... enabled by transversal digital transformation capabilities

- **Food safety & traceability**
  - Ensure compliance and increase trust across the whole value chain

- **Energy & sustainability**
  - Reduce environmental footprint and meet sustainability goals

- **Asset performance**
  - Maximize return on asset investment

- **Digital engineering**
  - Cut time, cost and risks of capital project engineering

- **Workforce empowerment**
  - Take teams’ efficiency to the next level

---

Challenges & solutions

- Digitization priorities
- How Schneider Electric secures CPG
- Our cybersecurity approach
Food safety & traceability
Ensure compliance and trust across the product life cycle

Manage your suppliers
Get visibility into your entire suppliers’s network, check their compliance and identify your risks

Digitize your compliance
Automatically document evidence of proper operation using digital tools and workflows

Reinforce your CPG defense
Protect your facilities from any unauthorized physical or cyber access

Monitor downstream logistics
Track and trace products and critical control points to guarantee product safety and protect your brand image.

Achieve end to end traceability
Increase visibility across your entire Value Chain, from raw materials to finished goods to improve transparency and trust for your end-consumers.

Build a credible value chain
75% time reduction in compliance

Achieve best-in-class defence in depth
100%

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach

Ensure consumer trust
Ensure compliance and trust across the product life cycle

**CPG safety & traceability**

- **End to end traceability**
  - Increase visibility across your entire supply chain to build a sustainable value chain
  - Raw Materials
  - Products

- **Digitize your compliance**
  - Automatically document evidence of proper operation using digital tools and workflows

**Fields & Farm**
- Suppliers’ information management
  - Get visibility into your entire suppliers’ network, check their compliance and identify your risks

**Cooperative**
- **CPG & cybersecurity**
  - Protect your facilities from any unauthorized access and ensure the right in-depth defense for your IT and OT systems

**Manufacturing**
- **Monitor downstream logistics**
  - Manage efficiently your assets tracking, performance and maintenance to optimize your supply chain logistics

**Distribution**
- **Digitization priorities**
  - How Schneider Electric secures CPG

**Retailer**
- **Challenges & solutions**

**Consumers**
- **Our cybersecurity approach**
Digitization priorities

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
Growth in IIoT connected devices

2015
2 (Billions)

2020
15

2025
75.44 (Billions)

Source: Intel

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Challenges to digitization

Source: Intel

- Social/political concerns: 6%
- Liability of current technologies: 15%
- Internal system barriers: 18%
- Data integrity: 23%
- Lack of skilled workers: 24%
- Large upfront investments: 30%
- Legacy installed base: 34%
- Lack of standardization: 35%
- Cybersecurity: 46%

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

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
IT vs. OT - cybersecurity priorities

**IT**

- Enterprise system and networks used to manage IT process and data that support banking systems, personal devices (laptops, cell phones, etc.)
- Focus areas - confidentiality, integrity and availability.
- Data confidentiality, data integrity and operational continuity are the priorities.

**OT**

- Operational networks that support and control physical processes such as washing of produce, pasteurizing, chopping, cooking, freezing, labelling and packing, etc.
- Focus areas - availability, integrity and confidentiality.
- Operational continuity and safety of humans and environment are the priorities.

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
A collection of measures (technologies, processes, and people) employed to **protect operational CPG processes and management systems**, along with **their associated assets** (products, equipment, networks, computers, programs and data) from **cyber threats** to maintain the safety, resilience and confidentiality of the system and data.
Cybersecurity in CPG: Cyber risks and did you know?

Cyber risks:

- Cyber-attacks are becoming more sophisticated and targeted.
- Mega breaches now cost an average of $42 million.
- In March 2021, the second-largest brewer in the United States was forced to halt its beer production due to a significant “cybersecurity incident”.
- It caused a delay to parts of the company’s business, including its brewery operations, production, and shipments.

Did you know?

CPG operations and the complex CPG supply chain are a clear target.

Many different suppliers

Interconnected suppliers & manufacturers

Long & complex supply chain to the end consumer

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
How Schneider Electric secures CPG

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Cybersecurity best practices for CPG

RECOMMENDATIONS

Cybersecurity risk should be viewed as a key business risk

Networks should be monitored and maintained through continuous vulnerability and risk assessments

Regular training and awareness for all employees

Sources: Kaspersky Labs, 2015; Trustware, 2016; Allianz Risk Barometer 2021
• CPG programs should be developed to reduce the risks from both internal and external threats in order to protect your customers. CPG defence assessment is based on 3 basic types:
  - **Threat assessment** (TACCP) of critical areas in the CPG supply chain. This includes also reviewing cybersecurity risks.
  - **Vulnerability assessment** (VACCP).
  - Likelihood of the threat assessment and its impact.

Sources: FSIS, 2021; FSCC22000, 2021, FDA, 2021
Reinforce your CPG defenses

Protect your facilities from any unauthorized physical or cyber access

Enhance facilities security

Protect your facility’s occupants and assets with an integrated, role-based physical access control and intrusion detection solution that unifies your building’s security infrastructure and building management systems.

Ensure the right defense in-depth for your IT/OT systems

Identify and mitigate risks by applying standards and good practices throughout the whole line of defense which must integrate people, processes, and technology.
Smart facilities
Safer, more available and greener resources

Power safety & availability
Standardization, site assessment, and predictive maintenance for safe and available power

Power quality & efficiency
Detect and mitigate power quality issues to increase equipment efficiency and life time

Renewable energies & microgrid
Manage complex energy mix to optimize cost and carbon footprint

Efficient utilities
Assess utilities performance and implement tools supporting continuous improvement measures

IT / OT infrastructure management and cybersecurity services
Provide self contained and secure computing environment for your on-premise applications

Smart building
Provide the best conditions for your manufacturing operations

Sustainability & energy management
Increase corporate transparency to meet your energy and sustainability goals

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
How to make sure your plant is protected against cyber-attacks.

Maintain CPG safety compliance and traceability to preserve brand equity and shareholder value.

- **Plant traceability**: Track your entire operations to reduce company exposure in case of quality issue.
- **Raw Materials**: Track & trace to protect your brands from counterfeiting.
- **Manufacturing defence**: Protect your facilities from any unauthorized access.
- **Cybersecurity**: Ensure the right in-depth defense for your IT and OT systems.
- **Label assurance**: Provide consumers with the right information.
- **CPG safety management**: Ensure fast and accurate product recall at the right granularity level.
- **Regulatory compliance**: Implement systems natively supporting CPG safety regulation compliance.
- **Cybersecurity solutions & services**: Our cybersecurity approach.
Achieve end-to-end traceability
Connecting the entire value chain: end-to-end

Applications

- Farm data
- Collect data
- Manufacturing data
- Distribution data
- Consumer data

Upstream
- Fields
- Farms
- Cooperative

Plant
- Manufacturing

Downstream
- Warehouse
- Retail
- Consumers

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Our approach – defense in depth

1. Security plan
   - Define and apply security policies and procedures (roles and responsibilities, physical access control, asset management, procurement policy).

2. Network preparation
   - Define and apply security policies and procedures (roles and responsibilities, physical access control, asset management, procurement policy).

3. Perimeter protection
   - Activate/apply security functions (access control, media policy, unused services deactivation, patch management, HIPS…).
   - Note: antivirus and virus database updates may cause compatibility issues. It is highly recommended to test proper functioning of the system (new install and updates) before deployment.

4. Network segmentation
   - Segment areas of network according to location, function, security needs.
   - Note: firewall can impact system; it must be chosen and placed with care.

5. Device hardening
   - Activate/apply security functions (access control, media policy, unused services deactivation, patch management, HIPS…).

6. Monitoring and updates
   - Continuous monitor, manage, and protect. Patch with new software revisions, reporting for audit compliance.

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach

Security plan

Network preparation

Perimeter protection

Network segmentation

Device hardening

Monitoring and updates
CPG cybersecurity success story

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.
Industry #1 beverage company architecture

Layer 5: Enterprise
- DATA CENTERS

Layer 4: Corporate
- SINGLE OR MULTIPLE SITES AND LOCATIONS

Layer 3.5: DMZ
- SRA CENTRAL MANAGEMENT SERVER (VM SUPPLIED BY CUSTOMER)

Layer 3: Operations Process Control Network
- SRA SITE SERVER (VM SUPPLIED BY CUSTOMER)
- ePO AV/PATCH SERVER (VM SUPPLIED BY CUSTOMER)

Layer 2.5: Cybersecurity Management
- SWITCH

Layer 2: Supervisory Control
- OWS
- PROGRAM TERMINAL
- HYBRID DCS SCADA
- SWITCH

Layer 1: Basic Control Field Devices
- MS80
- MS80
- MS80
- MS80

Layer 0: Physical Proc.
- MOVED HISTORIAN

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Our cybersecurity approach

Challenges & solutions

Digitization priorities

How Schneider Electric secures CPG

Our cybersecurity approach
Addressing cybersecurity challenges on multiple levels

Cybersecurity solutions for operational life cycle
Consulting, integration and managed security services

Technology partnerships
Situational awareness, compliance, change management, big data security

System deployment
Secure delivery of project and services during product or system deployment

Cybersecurity by design
Secure products, solutions, software

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Our approach & differentiation for your operational life cycle

Vendor-agnostic solutions.
Understand OT and IT perspective (for handling plant and corporate).
Scaled solutions to match every customer’s budget and maturity.
Vast experience in even the most heavily regulated industries.
Huge engineering and support team to help you close the deal successfully.
Cybersecurity design & implementation 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.
- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security

**Protect**
Implement specific controls as part of the operations systems for ongoing protection.
- Endpoint Protection, Anti-malware
- DLP, HIPS, Whitelisting
- Removeable Media Control
- Patch Management

**Detect**
Monitor the operating environment to detect and communicate threats.
- Security Information & Event Management (SIEM)
- Network Performance Monitoring
- Asset Identification
- Anomaly Detection
- Intrusion Detection

**Respond**
Develop procedures and systems to support rapid response to cyber incidents to contain and mitigate attacks.
- Backup / Disaster
- Recovery
- Forensics
- Incident Response

Challenges & solutions
Digitization priorities
How Schneider Electric secures CPG
Our cybersecurity approach
Visit our website to learn more about how to protect your business from cybersecurity threats.

Contact our cybersecurity team: se.com/cybersecurity-services

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0) 1 41 29 70 00

© 2021 Schneider Electric. All Rights Reserved. Life Is On Schneider Electric and EcoStruxure are trademarks and the property of Schneider Electric SE, its subsidiaries and affiliated companies.