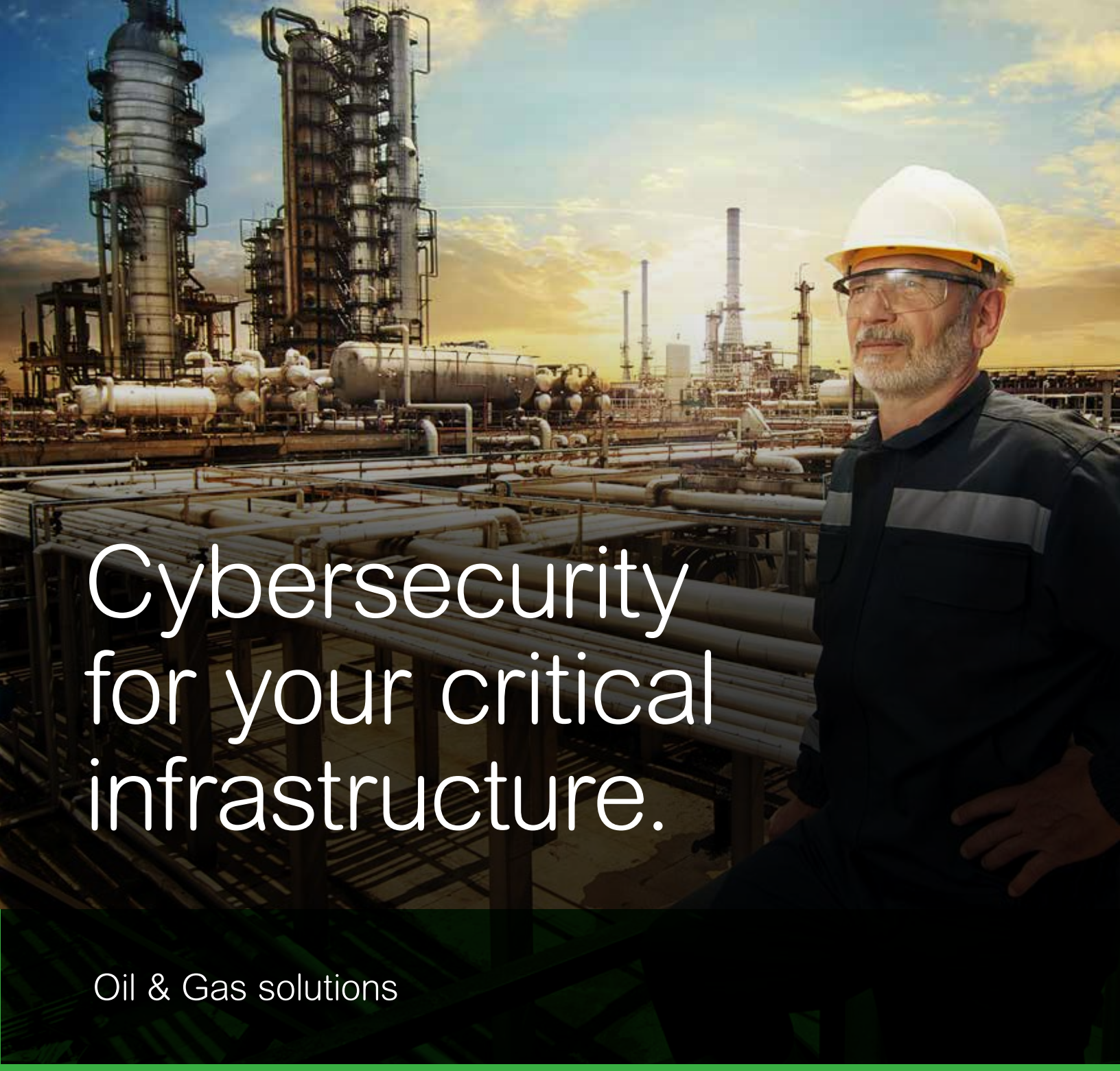
Life Is On | Schneider Electric

For more information, visit
schneider-electric.com/oilgas

Schneider Electric
Head Office
35 rue Joseph Monier
92500 Rueil Malmaison Cedex- France
Tel.: +33 (0)1 41 29 70 00
www.schneider-electric.com/oilgas



Cybersecurity for your critical infrastructure.

Oil & Gas solutions

schneider-electric.com/oilgas

Life Is On | Schneider Electric


ESD

The new digital age

Technology's constant evolution is producing significant changes in the way the Oil & Gas industry faces challenges.

Challenges

The Oil & Gas industry, like many in the energy sector, are facing cybersecurity challenges driven by internal requirements, industry standards, and government regulations.

- Interoperable open protocols
- Use of commercial off-the-shelf hardware/software
- IT/OT convergence
- Internet of Things
- Big Data and analytics

Schneider Electric™ Oil & Gas solutions address compliance and cybersecurity challenges from analysis through implementation and management. Our global consulting experts will assess your current compliance situation, then define an overall cybersecurity plan and remediation strategy encompassing processes, procedures, people, products, networks, and applications.

Our unique solution provides cybersecurity compliance for your critical infrastructure and integrates seamlessly between manufacturing operations and corporate Information technology networks.

The expanding cyber threat landscape

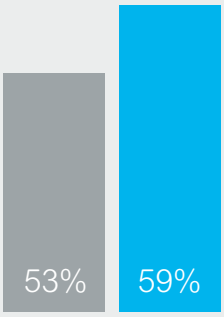
The increase in digital and online solutions, together with the growth of open platforms, is a growing cybersecurity threat. The SaaS model, whereby huge data warehouses store vast amounts of information in a cloud-based service, is of particular concern as more and more people turn to these solutions.

Attackers can exploit any vulnerability in the existing architecture or setup. It becomes imperative for the organization's team to ensure their system is designed with adequate protection and that periodic updates are made as a life cycle policy.

In the face of new technologies and changing scenarios, Schneider Electric takes a proactive role in protecting customers and our systems by investing in and developing the latest security capabilities. Market-specific and application-focused cybersecure development processes and validations, designed for your unique control system, ensure we securely accomplish the digitization and Internet of Things (IoT) journey while complying with the latest regulations and standards.

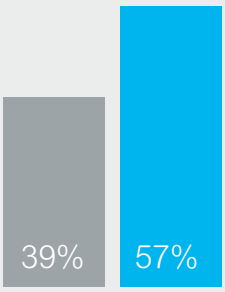
Schneider Electric addresses compliance and cybersecurity challenges from analysis to implementation and management.

Market minds — cybersecurity today



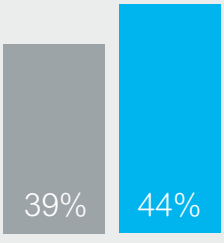
59%

of respondents see criminal syndicates as the most likely source of an attack today, compared with 53% in 2014.



57%

of respondents say the lack of skilled resources is challenging information security's contribution and value to the organization today, compared with 39% in 2014.



44%

of respondents see phishing as a top threat today, compared with 39% in 2014.

88%

of respondents do not believe their information security fully meets the organization's needs.

*Source: Global Security Survey 2015, Ernest & Young

Our comprehensive security offer

You can tackle today's challenges with the comprehensive Schneider Electric portfolio of secure products, solutions, and services.

Start building your defense against cyberattacks with a solid foundation from our selection of over 150 cybersecurity-certified products.

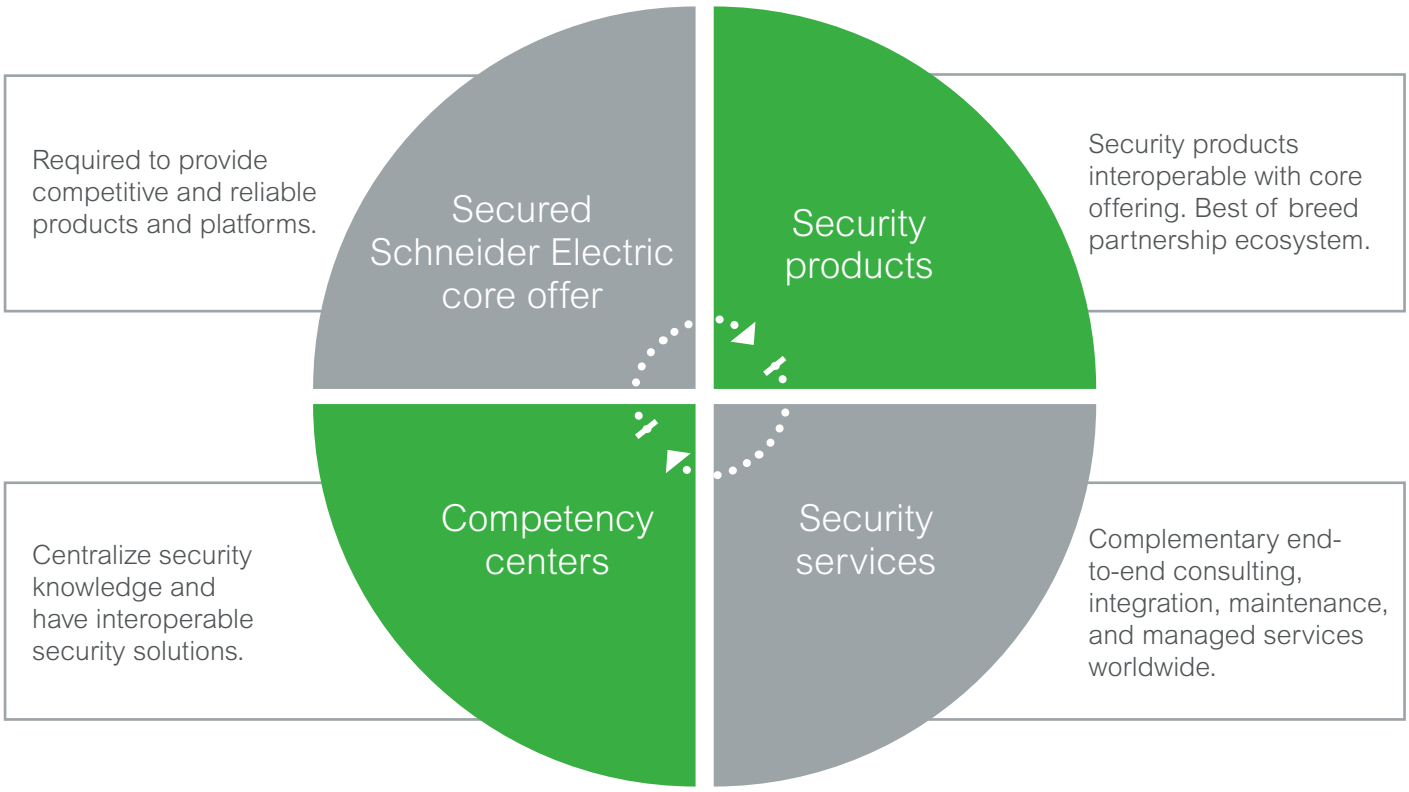
We'll help you implement systems for your critical infrastructure that meet the current cybersecurity standards and regulations.

If you have any system installed, our global cybersecurity experts can help you assess your threat level and suggest actions to be taken. Schneider Electric offers you more than 5,000 Oil & Gas specialists worldwide — we're where you are.

Security goes beyond the technologies to prevent incidents; it also incorporates people, processes, training, and continual assessment through policies, procedures, and awareness. It must include the end operator and any partners responsible for system design and implementation.

Schneider Electric cybersecurity experts can train your team on-site or at our well-equipped facilities.

Schneider Electric 360° cybersecurity approach



Defense in depth

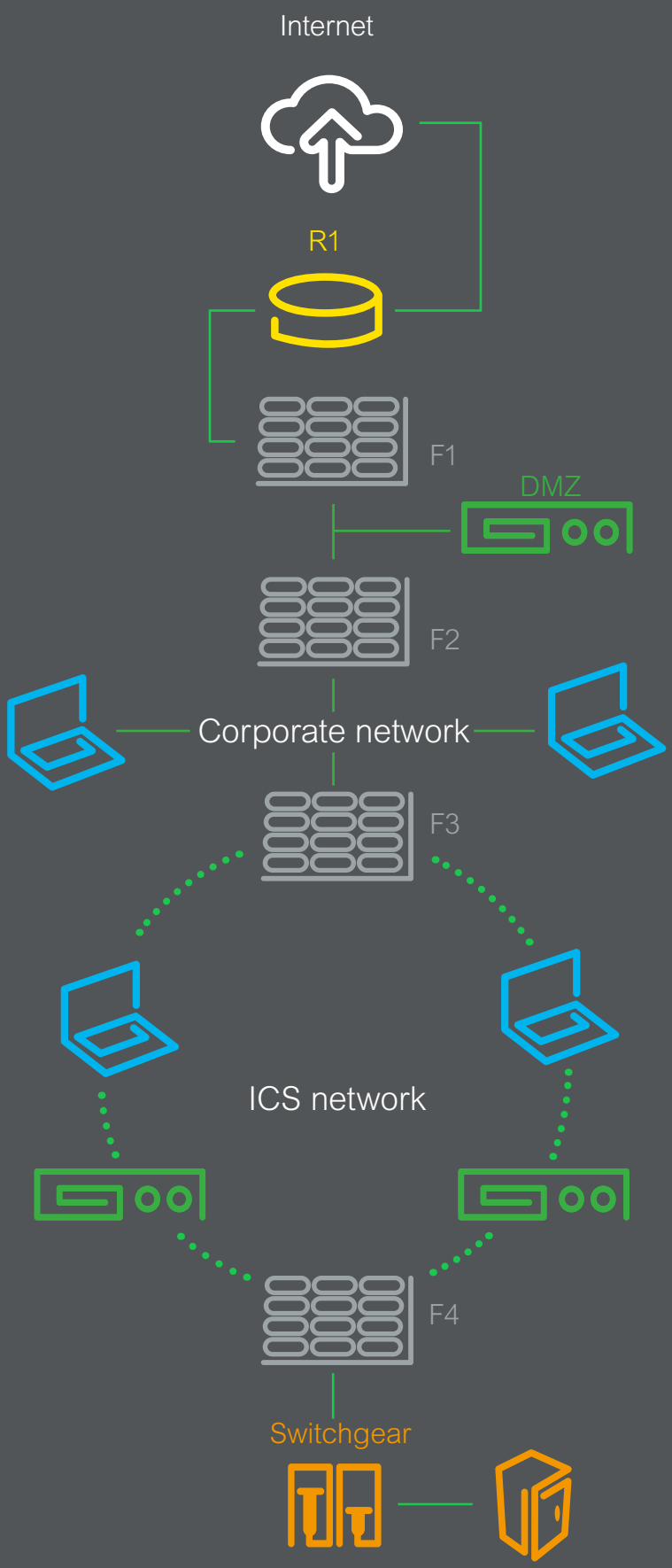
Security has historically focused on keeping out potential attackers through a perimeter-based defense. Today, the standard thinking is to anticipate a successful attack and design networks with a defense in depth strategy to minimize and mitigate damage from all kinds of attackers. This approach involves a multilayered, multitechnology, and multiparty strategy to protect critical assets.

We design and provide secure systems that include our equipment and/or our partner solutions.

Following IEC 62433 standards, we have developed the recommended layered architecture within our control systems to make them inherently secure when installed and achieve the highest level of security in critical infrastructure.

Schneider Electric's expert consulting with a track record of global success helps assess an organization's current compliance situation and define an overall cybersecurity plan and remediation strategy encompassing processes, procedures, people, products, networks, and applications.

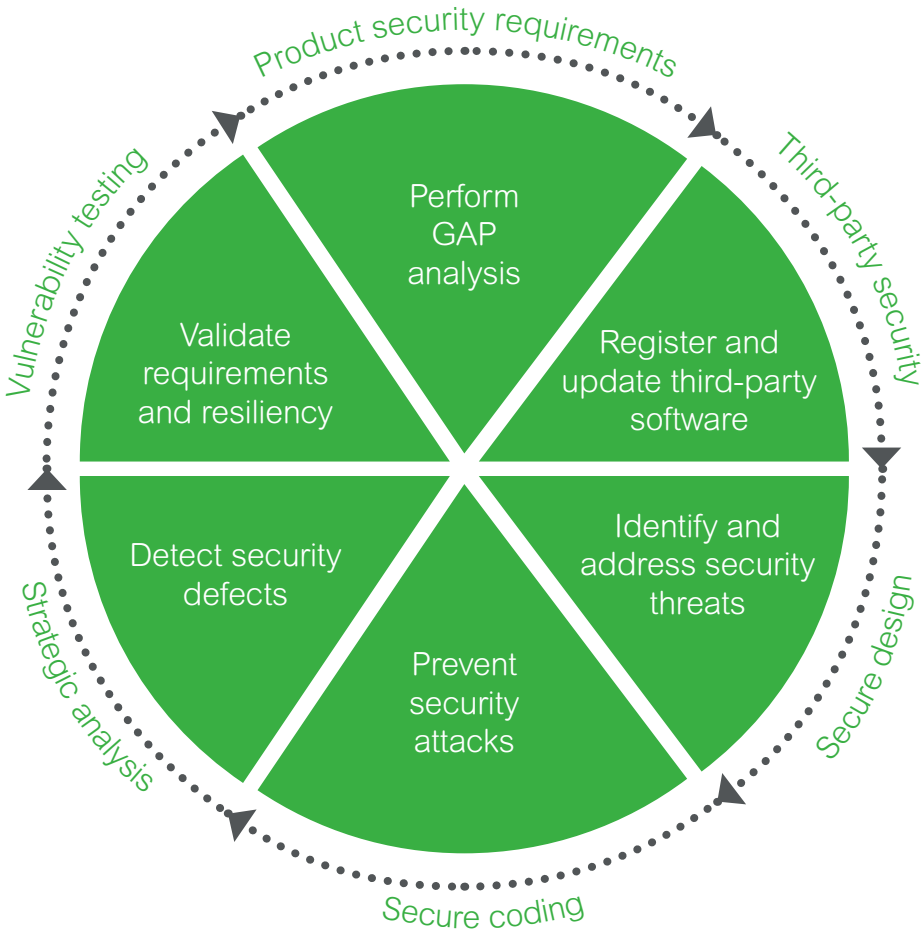
Defense in depth example



Secure Development Lifecycle

The Secure Development Lifecycle (SDL) is a repeatable and measurable process designed to increase the resiliency and trustworthiness of solutions. SDL is a process by which security is considered and evaluated throughout the development life cycle of products. The use of an SDL process to govern development, deployment, and operation of a monitoring platform is good evidence that the vendor is taking appropriate measures to ensure security and regulatory compliance. Schneider Electric has earned the industry's first ISA Secure Security Development Lifecycle Assurance conformance certificate from Exida LLC, an ISA Secure ISO 17065 accredited certification body.

Secure Development Lifecycle



Tested, validated, documented architecture

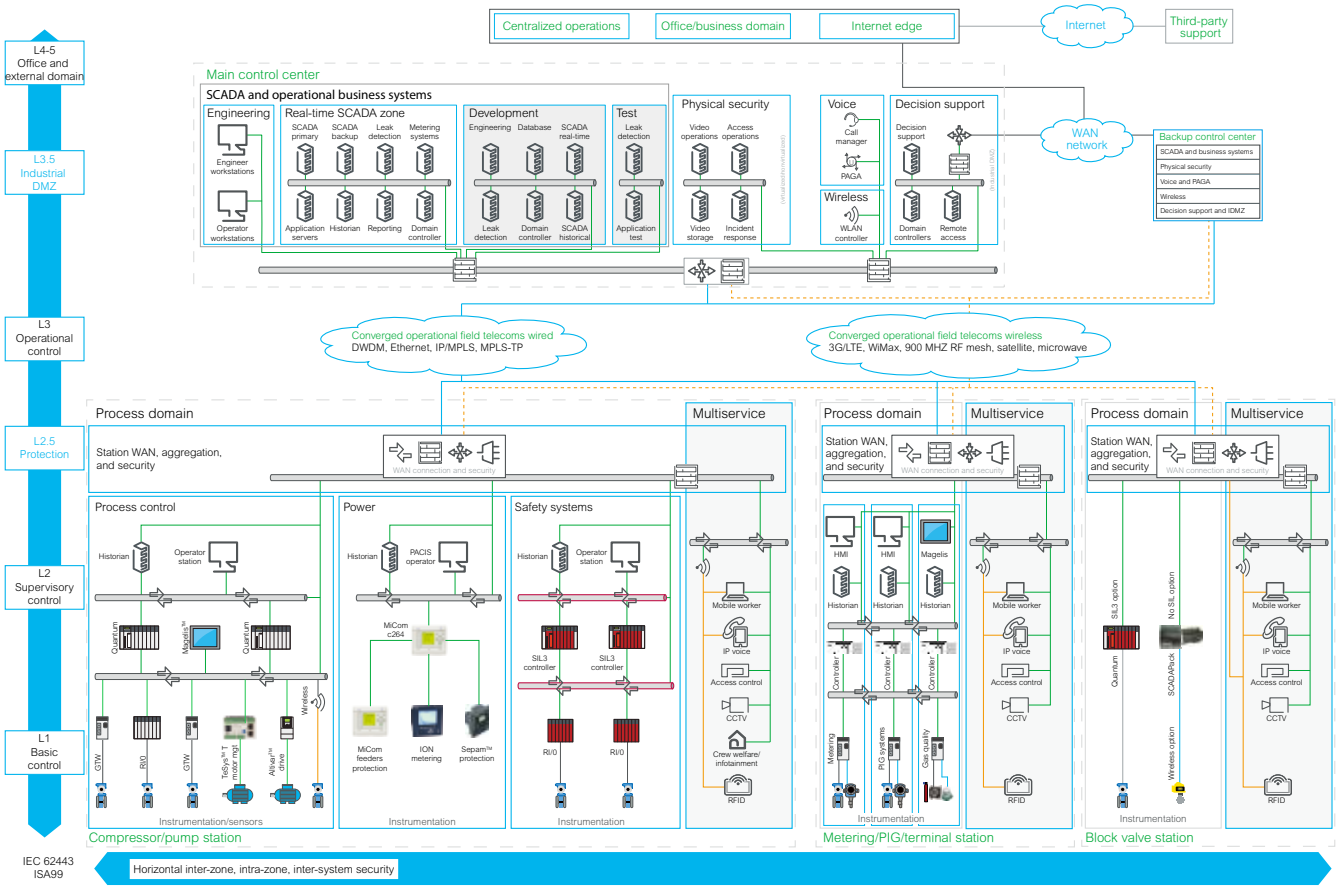
We want you to gain peace of mind with Schneider Electric solutions. We can help you effectively address customer security and compliance needs using common technologies and systems with the correct processes and procedures in place for safe operation and management. This does, however, require a much greater emphasis on IT and OT operations and convergence of people and philosophical levels in addition to architectural and solution areas. Merely securing the components is not enough to secure the architecture. The architecture must be tested, evaluated, and challenged as a global architecture to measure its performance and determine if the security level vector established by the reference standard IEC 62443 is met.

This architectural approach helps ensure a reliable solution.

To reduce the potential risks of technology deployment, our best practice is to build secure, validated designs that incorporate all components of cybersecurity.

Schneider Electric worldwide tested, validated, documented architecture labs host systems for customer visits and presentations, and are good evidence of our philosophy of testing before implementing via demonstrated architectures.

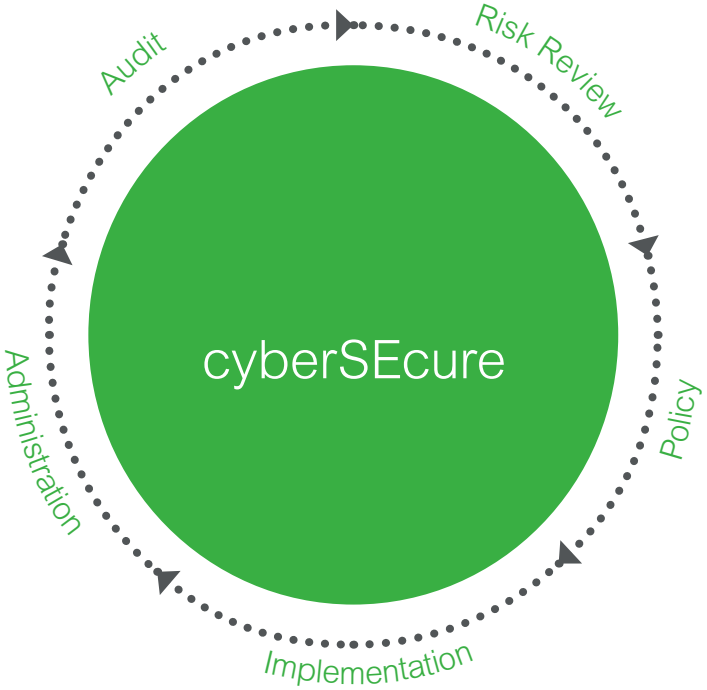
Example of TVDA hosted in our EcoStruxure lab in Houston



Cybersecurity services

Let us help you design, develop, deploy, and maintain your critical infrastructure.

- Tackle cyber threats with a control system that meets leading industry standards and the latest regulations.
- Bring your staff up to speed with current standards through Schneider Electric training.
- Get help from Schneider Electric consultants to design cybersecurity according to current regulations and requirements.
- Maintain your critical infrastructure to ensure uptime of your control system with help from the Schneider Electric services team.



Worldwide presence

Schneider Electric has over 100 cybersecurity experts around the world who bring their global collaborative knowledge to customers locally.

We have successfully delivered projects worldwide. Our team of experts regularly audits systems and recommends remedial actions, trains customers, and helps them maintain their systems.

Schneider Electric has partnered with external best-in-class cybersecurity leaders to deliver a comprehensive international security standards based cybersecurity program. Together we provide our customers with a complete solution so they can focus on the most important aspect of their business — increased returns.

OIL & GAS SOLUTIONS

Schneider Electric — your trusted partner

- A dynamic ecosystem of partnerships and platforms including governments, universities, and suppliers helps drive research, policy, and collaborative projects that produce a holistic security-conscious offering.
- We have earned the industry's first ISA Secure Security Development Lifecycle Assurance conformance certificate.
- ISO conformant vulnerability management process is activated upon external notification, vulnerability disclosure, or customer report.
- Our advanced Global Threat Intelligence Center actively monitors cyberspace for threats to our products and customers.
- 150+ products are cybersecurity standards-certified for electrical and process installations.
- Our cybersecurity team of experts understands your process requirements, enterprise needs, and business environment.

Vision

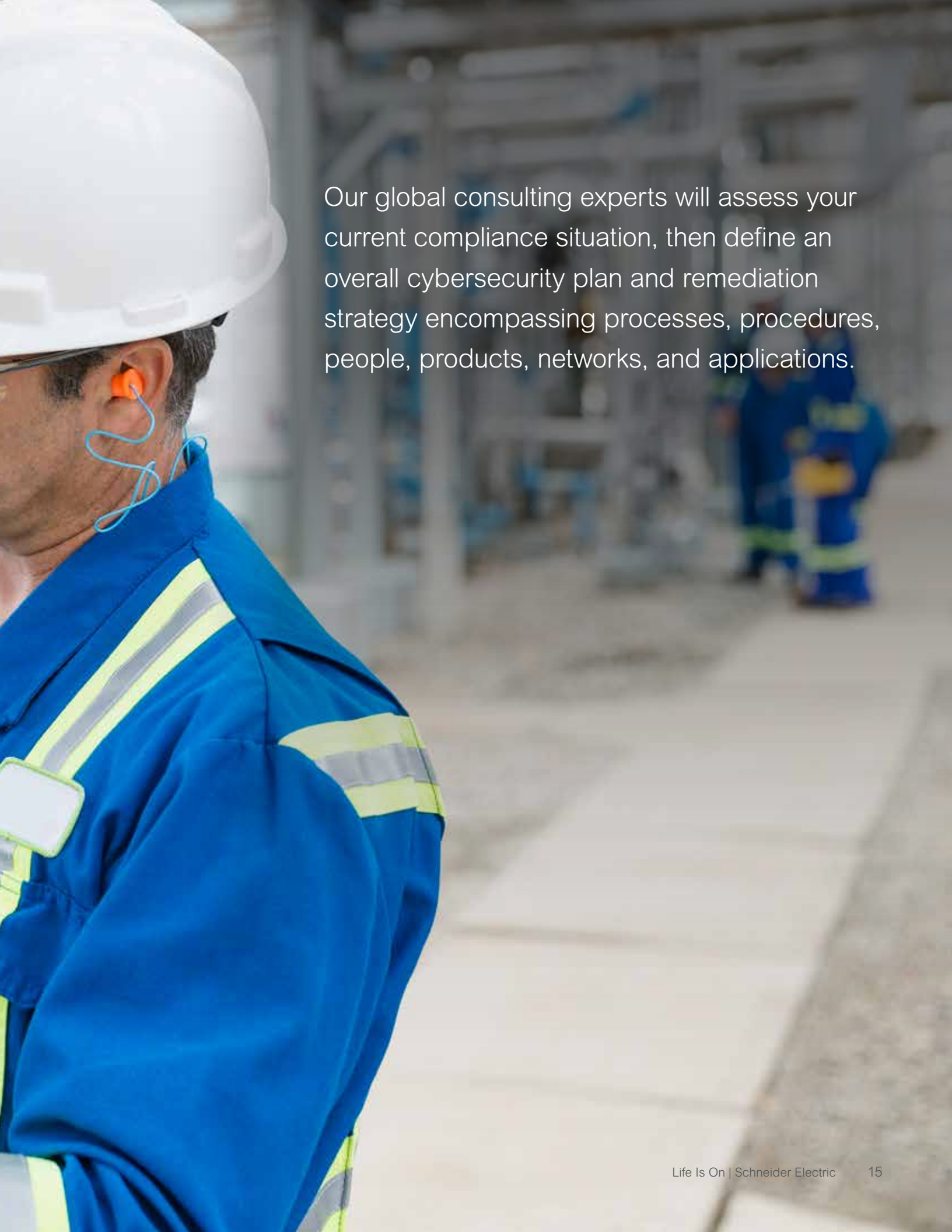
To live in a world where all Schneider Electric offerings are secure, customers are satisfied with our security, and we can leverage our security as a competitive advantage.

“Qatargas recently used the services of the Schneider Electric EMEA Cybersecurity Team for three projects.

They were knowledgeable in this field and willing to discuss and come up with new or custom solutions to benefit the end user (Qatargas). The solutions have already been implemented and are working well.

Overall, Qatargas is satisfied with the services provided by the EMEA Cybersecurity Team of Schneider Electric.”

Ahmed Hassan Al-Sulaiti
Head of project execution “On-plot & Off plot”



Our global consulting experts will assess your current compliance situation, then define an overall cybersecurity plan and remediation strategy encompassing processes, procedures, people, products, networks, and applications.