Life Is On | Schneider Electric

Securing Operational Technology (OT): Addressing digital risks in business-critical infrastructures

by Schneider Electric

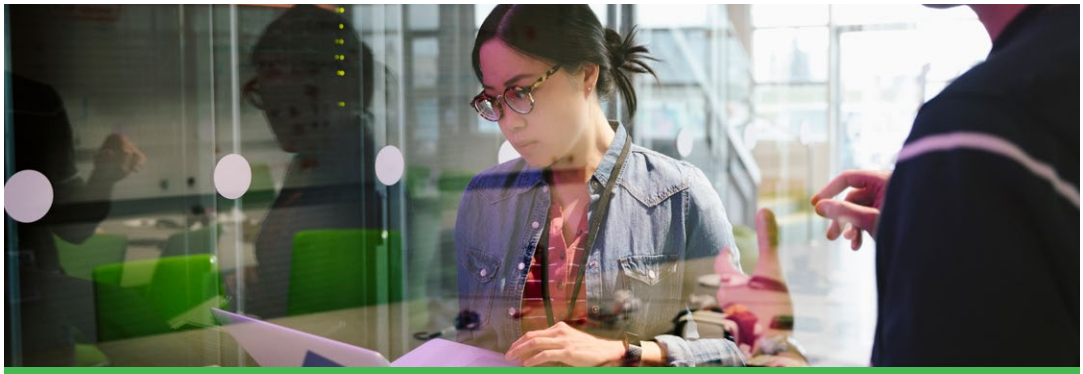
Executive summary

Digital transformation enables industry to improve operational and business performance in ways never imagined before. To take advantage of the Industrial Internet of Things (IIoT), companies must expand connectivity across their people, assets, and systems, and make full use of extracted data to improve their operations and processes. All this connectivity closes the gap between IT and OT, meaning a company's operations are in sync with their business, enabling greater performance. However, it also widens the attack surface for would-be cybercriminals.

This white paper examines risks to Operational Technology (OT) as industrial facilities implement IoT devices across the environment. In the age of the IIoT, cybersecurity can no longer be an afterthought. There is too much at stake, financially and operationally.

Global industry faces a new reality: today's bad actors frequently have unlimited time, resources, and funding to carry out their cyberattacks. In the face of new, ever more dangerous threats, forward-thinking companies will quickly implement best practices for securing their mission- and business-critical environments. By making security part of the operations lifecycle, companies are more likely to succeed in the digital economy.

Contents



Thriving in the digital economy

"Any skilled engineer can take control remotely of any connected 'thing'. Society has not yet realized the incredible scenarios this capability creates."

André Kudelski, Chairman and CEO of Kudelski Group[2]

Without question, the hyper-connected economy is here. About 20 billion objects are connected to the internet at present,[1] with objects and machines becoming increasingly interconnected to each other. As global industry integrates technology at the heart of its facilities and operations, the question everyone should have in mind is: how can we secure this fast-proliferating digital landscape in industrial environments?

Indeed, while having hundreds of devices connected to the same network eases processes and improves efficiency, it also opens a wider window to security threats.

An attack in the Information Technology (IT) world can result in significant theft, loss, or misuse of data, which can be a blow to a company's reputation. In many cases, industrial stakeholders can look to IT security as good practice. IT security at large is widespread across markets. By contrast, the practice of securing the Operational Technology (OT) environment is in its infancy, and it is even more critical. That is because an attack in the OT space can have direct repercussions on physical surroundings, such as a full grid outage or, in the most extreme cases, the loss of human life.

Revealing the impact

"Popular movies have frequently exploited the idea that the infrastructure of modern life is vulnerable to well-staged cyberattacks. But the real-world Stuxnet virus succeeded better than anything out of Hollywood in proving that power plants and other nuclear assets can indeed be sabotaged."

McKinsey & Company[4]

Industry's first wake-up call was the Stuxnet case, which surfaced in 2010. This malicious computer code wormed its way into the middle of an Iranian nuclear plant, ultimately affecting about 100,000 computers worldwide (mostly in Iran), including uranium centrifuges.[3] More recently, an industrial facility in the Middle East was the target of a highly sophisticated and prolonged cyberattack, dubbed Trisis or Triton. When attackers attempted to infiltrate the facility's safety integrated system, the system detected an anomaly and took the plant to a safe state via a shutdown. Unfortunately, such cybercrimes are no longer relegated to the world of science fiction.

Similarly, everyone remembers WannaCry, the ransomware attack that affected more than 200,000 computers across more than 150 countries.[5] WannaCry caused damage to many users, from individuals to huge companies and industrial facilities. By encrypting computers and machines in factories and asking for payment, the ransomware was able to cause huge damage to the IT and OT organizations.

This last mass attack was eye-opening well beyond the incident, as it ultimately revealed that all industrial players needed to work together to ensure a path to safety in the OT world across the entire digital ecosystem.

Accelerating OT security

In the past, before the proliferation of the Industrial Internet of Things (IIoT), OT infrastructure was fairly safe from cyberattacks. This is because proprietary standards and hard-wired connectivity protected devices in a unique way. The widespread integration of embedded devices and OT networks with corporate or IT infrastructure has created a much greater attack surface over an increasing number of open networks. Every endpoint in a factory or facility is a possible path for hackers, and the impact on maliciously accessing industrial controls could be disastrous.

When it comes to cybersecurity, IT stakeholders typically look to secure data and protect data privacy. Industrial companies, by contrast, seek to protect safety, efficiency, and reliability as they race to seize the many benefits created by converging their IT and OT. These advantages include just-in-time inventory, faster production, improved energy use, and better safety, but the real benefit is a new-found ability to manage and control business performance.

What are common OT risks?

As industrial companies implement cybersecurity strategies as an inherent aspect of their digital transformations, it is important to recognize the differences between securing the IT and the OT environments. Companies can garner lessons learned from IT over decades and, in turn, create a holistic approach to ensure that cybersecurity in a hyper-connected world adopts strategies concerning known and emerging risks and threats. According to the State of Industrial Cybersecurity 2019 survey, about "70% of companies surveyed consider an attack on their OT/ICS infrastructure likely. Despite this, many have yet to define their own approach to implementing OT/ICS cybersecurity."[6]

So, what are the inherent risks in OT?

A wide attack surface

Today's cyberattacks are numerous, frequent, and more threatening than ever before. Attackers aim to infiltrate and manipulate not just an individual company, but the entire ecosystem to which it belongs. Needless to say, 20 billion connected objects create many endpoints. Each device can be an entry point for hackers to access the broader industrial ecosystem. Consider, for example, that in today's digital factory, there are hundreds —and even thousands — of connected sensors across the industrial environment. Each is a potential target for hackers.

Legacy infrastructure with aging assets

Many of the systems that control the world's most critical operations were installed and developed decades ago, before the advent of the IIoT and back when cybersecurity was not even a consideration. Additionally, these systems are built for the long haul: they have decades-long lifespans and, in many cases, will continue to operate until the plant is decommissioned. Securing these systems in the age of the IIoT is doubly challenging due to the technical limitations of the devices and the need to maintain compatibility with other legacy infrastructure. Here, as new integrations of current technology proliferate at lightning speed, digital risk increases if an end-to-end cybersecurity plan to address both current and legacy systems is not in place. According to an Accenture survey, 79% of CEOs questioned indicated that their organization is "adopting new and emerging technologies faster than they can address related security issues."[7]

Targeted attacks on unique weaknesses

In addition to managing aging assets, industrial companies are wrestling with the fact that OT cyberattacks often target unique weaknesses for a very precise impact. Instead of targeting a weakness that will affect the biggest number of users, as often seen in the IT space, recorded cases show that, industrial hackers generally focus more resources on attacking a specific weakness in a rare device to aim at a single target.

This particular type of modus operandi requires specific paths of protection. Typical defensive measures, such as antiviruses, are not commonly applicable due to the limitations of the devices; regular antiviruses would unacceptably slow or incapacitate them. What's more, it is expensive, complex, and inefficient to design specific protection programs for each device. To stop an attack once it is detected, the devices should be quickly disconnected from the system. Such a disconnection is very challenging in many factories. Though the installation of patches is a common remediation for IT systems, it is often more complicated to implement in industrial environments as patches should be installed during the limited maintenance periods and may require device recertifications, leaving the devices exposed during the gap.

Regular exposure to third-party access

In addition, the OT environment is particularly exposed to third-party risks. Compared to IT, OT environments are more likely to rely on vendors for ongoing support but less likely to formally manage the associated external risks. These vendors are often granted privileged access through their own laptops and USB devices, the internet, or fully hosted environments with little control. Even with no malicious intent, this broader access poses a huge risk in terms of cybersecurity despite the dangers of infection. Several heavy industrials have reported that third parties frequently connect laptops and external storage devices directly into OT networks without any prior cybersecurity checks.

Addressing these OT risks

As the IIoT promises to advance the world with significantly more cost-effective deployments, advanced analytics, and immense scalability, it also introduces cybersecurity threats previously relegated to the IT department. Now, many devices can connect to the internet, share information, and receive control signals or configuration updates. These new devices present security risks that historically have been unfamiliar to operational teams. Connecting these devices exposes them to the outside world, which means malevolent actors with high skills can intercept, modify, or disable these devices. Their motivational interests can range anywhere from criminal to national security or societal change.

With such complex OT risks, it is essential to protect industrial assets and processes and move from reaction to proactive prevention. Some practices that might seem simple are essential. For example, having stricter password policies, giving basic training to employees, or including cybersecurity terms within suppliers' contracts are fundamental steps that can have a big impact on securing an ecosystem. Here are some recommended steps for securing the OT environment:

Network segmentation

Intelligence is migrating upward through the automation hierarchy and into the IT architecture. The data from the factory devices is fed upward into the control layer, and onward so business and operations managers have real-time insight into the performance of the plant. With that data, they can make better real-time decisions on what actions to take for better business outcomes.

For the factories producing more advanced technologies with higher risks, high-level security solutions can be implemented, the most secure of which is the networking segmentation (conduits and zones systems).

In this case, the factory is divided into zones, with each being isolated from one another. In order to allow the information to circulate, channels (conduits) are created between the different zones. These conduits allow only specific information to circulate, enabling the user to monitor it while blocking the rest of the incoming or outgoing information. Attackers or malware that have breached one zone will find it difficult to pivot to another zone if controls such as a properly configured data diode, firewall, IPS, or IDS are in place.

These ensure that only authorized traffic is allowed to traverse zone boundaries.

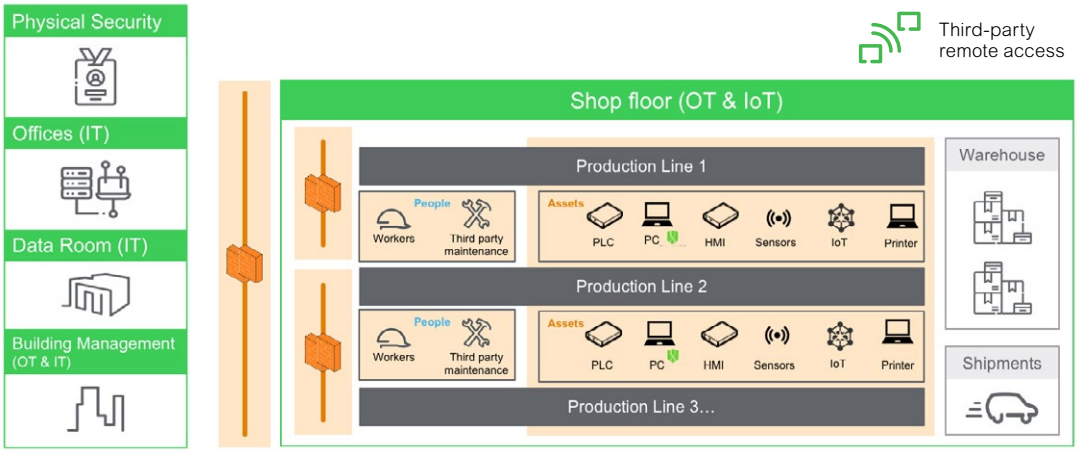


Figure 1: Network segmentation to separate IT and OT environments

People and operating models

Though most of the risk management solutions and mitigations involve technological methods, the human factor in cybersecurity should not be neglected. It is a huge part of the risk landscape. In the realm of industrial control systems, human error and unintentional actions are responsible for more than a fourth (27%) of network incidents.[8] That is why it Is essential to implement mandatory, ongoing training that is consistently and continually adapted depending on the expected cybersecurity involvement of the worker. Policies should be created and enforced to help formalize standards and guidelines. These policies might focus on numerous aspects of the network management and facility organization, and can include measures such as password regulations, incident management actions, and user access controls. In addition, in case of a crisis, playbooks should be available to help the worker to focus on essential specific actions while being possibly overwhelmed by a stressful situation.

Avoiding the cascading effect

Recent malware attacks show that an OT infection can spread to the IT domain and vice versa, in a cascading effect. This was the case with the infamous ransomware WannaCry. Though it was initially aimed at PCs, it soon propagated to the OT environment, where devices were a lot harder to protect and to patch. For that specific pattern to happen, the ransomware was exploiting a weakness in the Server Message Block protocol, through four unprotected ports. By blocking the access to these ports, the zone was able to remain WannaCry-free. Thus, the network segmentation method discussed previously has proven an efficient way to avoid cascading the effect.

Securing legacy infrastructure

One of the major challenges for securing both IT and OT equipment is how to address the cybersecurity hurdles of legacy systems, especially infrastructure with a capital expenditure whose lifespan is 30 years or longer. Although the new generation of physical infrastructure products and solutions are far more cybersecure, it can be practical and economically feasible to apply a range of basic but effective security controls to legacy systems to improve their security posture.

Continually securing legacy operations and systems against new threats is a challenge, but it is not impossible. It is critical to strive to adhere to industry-recognized practices to further reduce threats to aging installations. Taking these precautions and speaking with security consultants and cybersecurity providers can significantly increase the layers of protection. These precautions, which may be more critical for legacy infrastructure lacking advanced cybersecurity controls due to their age, can include:

- Keeping all programming software locked in cabinets and not connecting them to any network other than the network that the devices are intended for.
- Locking all controllers in cabinets and not leave them in “program” mode.
- Implementing physical controls such that no unauthorized person has access to the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- Locating control and safety system networks and remote devices behind firewalls and physically and logically segmenting them from the business network.
- Banning laptops that have been or are connected to any other network, besides the intended network, from connecting to the safety or control networks without proper sanitization.
- Scanning all methods of mobile data exchange such as CDs or USB drives with an isolated endpoint running the latest antivirus signatures before allowing these media into the OT environment.
- Minimizing network exposure for all control system devices and systems, and ensuring that they are not accessible from the internet unless a risk assessment has been performed and the risk is within acceptable thresholds.
- Using secure methods, such as Virtual Private Networks (VPNs), when remote access is required. At the same time, it should be recognized that VPNs may have vulnerabilities and should be updated to the most current version available.
- Recognizing that a VPN is only as secure as the connected devices themselves.

Adopting shared responsibility

Cybersecurity is everyone’s responsibility, and each party has a role to play. Manufacturers and Original Equipment Manufacturers (OEMs) should endeavor to provide the safest, most up-to-date devices at the moment of production. Manufacturers and OEMs must also design safe protocols and interfaces for these devices, offer basic security training, and develop patches when needed. In parallel, end-users of the systems are obligated to train their workforce on safe practices and provide them with guidelines on what to do in the event of a cyber incident. Furthermore, end users must be responsible for keeping their devices up-to-date, as per the given instructions. By uniting manufacturers, OEMs, and utilities practices, the OT world will become inherently more secure.

What is Schneider Electric doing to secure its supply chain?

Schneider Electric's digital risk strategy recognizes that cybersecurity is not just a feature of hardware or software components. Since Schneider Electric's Smart Factory program was launched, there has been a greater focus on cybersecurity. This program is based on Schneider Electric's IoT-enabled EcoStruxure™ platform, which comprises connected products; edge control; and apps, analytics, and services. These solutions can greatly contribute to an increase in productivity and to more accurate and easier process controls. To be able to use the features of this new platform safely, cybersecurity must be included in risk management discussions.

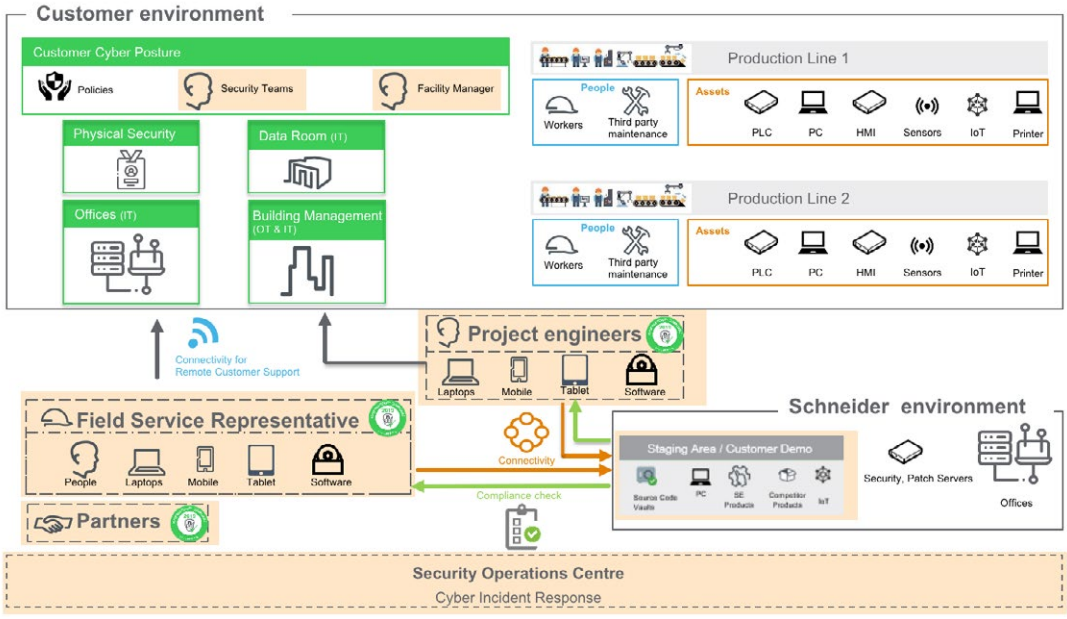


Figure 2: Securing the end-to-end digital ecosystem from supply chain factories and customer-facing activities beyond field services

Cybersecurity is a fundamental, ongoing business practice that strives to identify, mitigate, and reduce risks by applying standards and good practices to people, processes, and technology across the end-to-end digital landscape. Relevant challenges are identified for high-value assets, the at-risk population, and IT/OT segmentation. Then, the cybersecurity framework is designed with a mix of policies and best-in-class solutions. This strategy is communicated with providers and suppliers to ensure their understanding and compliance with Schneider Electric's security policy, which creates a holistic strategy from the supply chain to deploying solutions to customer sites.

To secure its own factories across the global supply chain, Schneider Electric adopts a cybersecurity strategy that uses the ISA/IEC 62443 set of cybersecurity standards as a baseline. The ISA/IEC 62443 approach comprises four levels that Schneider Electric has condensed into basic, intermediate, and advanced. The basic level has been mandated for all Schneider Electric factories. One of the requirements to reach this level is the designation of a Cybersecurity Site Leader. Skilled and trained accordingly, this person must be appointed in each plant to ensure that these actions are properly implemented and that 100% of shopfloor employees have completed a cybersecurity training.

According to the required level of security, intermediate and advanced levels are also deployed in Schneider Electric plants. For instance, at OT factories producing advanced technologies, remote access controls must be implemented for subcontractors, and firewalls must be installed to separate the networks. The plant is divided into several zones that are isolated from each other by conduits and zones. By doing so, Schneider Electric takes care that if an installation is compromised by a virus, access to this installation can be controlled to protect each zone.

Figure 3: Scalability of the deployment strategy for cybersecurity on industrial sites

In order to ensure optimal protection and reaction in case of alerts, Schneider Electric cybersecurity stakeholders often organize penetration tests and incident response simulations. This testing means that some facilities are assessed on their reaction to a possible cyberattack. Through these operations, new measures and trainings are implemented to confirm up-to-date safety.

Raising the bar of OT security via collaboration and partnerships

In isolation, it is possible for a company to have good cyber posture. However, unity around cybersecurity is essential to ensure security for all. In order to contribute to global efforts, Schneider Electric gives precedence in contributing to organizations such as the following:

ISA Global Cybersecurity Alliance

"As industry confronts escalating, innovative, and dangerous cyberattacks, every organization interested in securing our global infrastructure should collaborate to improve how end users defend themselves"

Mary Ramsey, executive director of ISA[10]

Led by its members, including Schneider Electric as a founding member, the International Society of Automation (ISA) Global Cybersecurity Alliance advances the development of new standard-based defensive strategies that contribute to improving cybersecurity in the OT space.[9]

To do so, cybersecurity knowledge and information must be shared in an open environment. This knowledge and information sharing helps facilitate the awareness and response to threats. Also, as no initiative can be complete without collaboration of governments and regulatory agencies, the ISA Global Alliance takes the initiative to encourage the advocacy of new measures and accelerate the development and adoption of standards in accordance with the prevailing, globally recognized ISA/IEC 62443 set of cybersecurity standards.

Cybersecurity Coalition

"Joining the Cybersecurity Coalition demonstrates that Schneider Electric takes cybersecurity challenges seriously and that we are committed to playing a foremost role in developing solutions. Our membership ensures we have a focused seat at the table to initiate open, transparent, and collaborative conversations that advance the adoption of cybersecurity policies and laws for the benefit of our customers, partners, and all stakeholders across our extended enterprise, including the communities and environments we mutually serve"

Hervé Coureil, Chief Digital Officer, Schneider Electric.[11]

Schneider Electric affirms its role in strengthening digital trust as a member of the Cybersecurity Coalition. The Coalition addresses the intersection between governments, researchers, and vendors. Here, the Coalition is focused on several critical policy issues that require close alignment and coordination to protect the vital interests of cybersecurity products and services industry, including:

- Promoting responsible vulnerability research and disclosure
- Promoting effective privacy processes within cybersecurity policy
- Establishing cybersecurity procurement requirements for government systems
- Increasing information sharing and threat intelligence
- Promoting sound cybersecurity practices in government at all levels

A cybersecurity partner ecosystem

Schneider Electric places a high priority on strengthening cybersecure digital innovation through an extended enterprise approach that includes strategic partnerships with best-in-breed technology providers, customers, startups, universities, and developers. The resulting ecosystem advances co-innovation and the development of more secure EcoStruxure solutions while also providing an open community to developers.

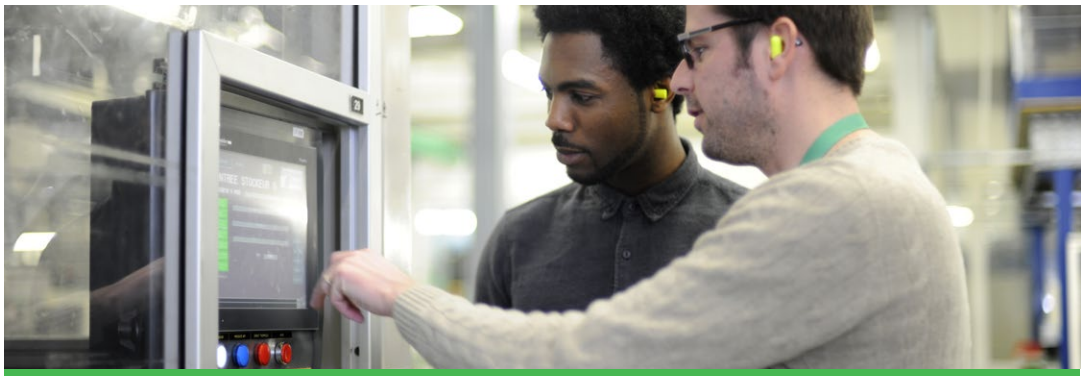
Examples of this digital ecosystem approach include collaborative development and management of a Security Operations Center (SOC) with IBM. This has led to the creation of incident response teams that strengthen resilience and responsiveness capabilities. Another example of a partnership is the one between Schneider Electric and Claroty, a specialist in providing visibility and greater security to OT networks.

Partnership with Claroty

To secure the network and assets inside the 300 factories and facilities across Schneider Electric's global supply chain, a partnership was leveraged with Claroty, an OT security specialist firm. Claroty's smart solution monitors network flows transiting between devices, in turn informing the SOC as soon as any abnormality is detected. Claroty also knows in real time which device is connected to the intranet or internet, as well as the specifications of each of these devices. This real-time monitoring allows live tracking of devices from initial deployment to when to patch, to obsolescence.

Public partnerships

Schneider Electric also engages in numerous public partnerships to help make both legacy and new products more cybersecure. For example, Schneider Electric is an active member of the Cybersecurity at MIT Sloan (CAMS, formerly IC^3), an interdisciplinary forum that brings together MIT faculty / researchers and C-level cybersecurity experts on cyberspace, cybercrime, and cybersecurity as applied to critical infrastructure.



Improving the security of industry with cybersecurity training and services

Schneider Electric also leads its own initiatives and collaborative resources for customers and partners. For example, Schneider Electric offers a Cybersecurity Virtual Academy which provides a thought leadership platform for the company and cybersecurity services for partners and customers who would like to reinforce their cybersecurity posture.

Cybersecurity Virtual Academy

Investing in awareness and training is much less expensive than the cost of remediation, a damaged reputation, or downtime. At Schneider Electric, sharing information with customers and partners is essential. That is why Schneider Electric created the Cybersecurity Virtual Academy to provide value-added content and engage customers, prospects, and other interested groups in an ongoing dialogue about cybersecurity topics.

Cybersecurity Services

Cybersecurity defenses are only as strong as the weakest link – if they are implemented improperly or left accessible, the system is not secure. Cybersecurity is a journey, not a destination.

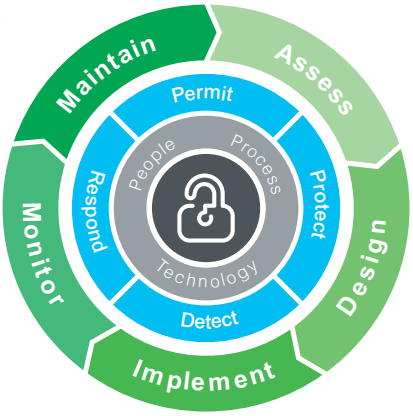
Schneider Electric's cybersecurity solutions are applied from the operations perspective while integrating the appropriate policies and requirements. Schneider Electric has deep knowledge and experience in cybersecurity, allowing it to provide customized and flexible experiences to customers independent of system vendors.

For the customers who would like to go even further, their maturity can be assessed, such as in the diagram below. With comprehensive services, Schneider Electric can help to progress from the initial stages with the potential to reach the optimizing level depending on the requirements.

Initial 1.0	Developing 2.0	Defining 3.0	Managing 4.0	Optimizing 5.0
People: No dedicated staff for security activities but risks broadly accepted.	**People**: Leadership structure formalized & management roles assigned.	**People**: Roles & Responsibilities established and formalized.	**People**: All RACI roles filled with dedicated resources and/ or responsibilities assigned.	**People**: Ongoing development & training, continuous improvement.
Process: No governance or management system in place.	**Process**: Basic governance framework and policy created.	**Process**: Comprehensive Cyber management system established.	**Process**: Formalized governance group, reviewing performance & metrics.	**Process**: Cybersecurity management system fully implemented.
Technology: No emphasis on formalized security controls.	**Technology**: Some technology implemented in an ad-hoc fashion.	**Technology**: Formalized technical controls.	**Technology**: Control measures in place & monitored for compliance.	**Technology**: High level of automation for monitoring, compliance & performance.

Figure 4: A cybersecurity assessment can determine an organization's level of maturing in protecting the digital ecosystem

One of the main focuses at Schneider Electric is to enha safety and security at every stage of a component's life. To do so, a global team with strong IT experience and deep knowledge of the OT world can help customers assess their needs and detect gaps in their cybersecurity management. This means secure, tailored solutions can be recommended and implemented. More importantly, Schneider Electric has the skills and experience to monitor and maintain existing and deployed installations more securely and independent of system vendors. Furthermore, it is essential to share knowledge and experience to develop the cybersecurity mindset that is critical today and in the future.



Schneider Electric solutions revolve around four essential factors:

- **Permit**: The access to the network is subject to safety measures such as authentication, authorization, and physical identification.
- **Protect**: The network is protected from malware and viruses and can have some advanced protection tools installed.
- **Detect**: Issues in performance, anomalies, and intrusions should be detected as soon as possible to allow an adequate response.
- **Respond**: Once a cyberattack is found, incident response is activated, and forensic investigations conducted. If needed, recovery can be made from a backup.

A regulatory snapshot and perspective

With Schneider Electric's cybersecurity services, for every decision taken and each action made, there is always a fundamental link to people, processes and technology.

In general, global cybersecurity policies and regulations are focused on the requirements of Internet of Things (IoT) devices. These regulations typically do not target OT specifically, instead, they combine OT into the broader definition of IoT devices. In other words, policy and regulation that Schneider Electric tracks targets any "connected devices" or "IoT device" regardless of the intended use or customer base. Below is a high-level overview of the key regulations that have a direct impact on the OT environment. Note that that these are the laws currently in place/effective today; many more are pending in various jurisdictions and the regulatory landscape is constantly evolving.

European Union (EU) Cybersecurity Act[12]: On March 12, 2019, the EU Parliament voted to adopt the EU Cybersecurity Act, a sweeping regulation that will establish certification schemes to apply to a range of online services and connected devices. The strategies are currently being contemplated by DG-Connect and ENISA and will be established over the next several years.

- The product certification strategies are organized into three categories: 1) Basic, 2) Substantial, and 3) High, which correspond to the perceived risk associated with the product function, data, and environment.
- Assurance level "High" is reserved for products used in critical infrastructure applications, where many Schneider Electric OT products could be impacted.
- There are also EU member state IoT requirements and certification programs. In general, the EU Cybersecurity Act aims to harmonize and standardize these programs into a European-wide cybersecurity certification program.

Chinese Cybersecurity Law[13]: This sweeping law governs industry, citizen, and government roles and expectations in cybersecurity and privacy. The law effectuates the implementation of several policies and regulations that have a direct impact on OT. Below are the selected highlights:

- ***Cybersecurity Classified Protection Scheme or Multi-Level Protection Scheme (MLPS) 2.0***[14]: MLPS is part of the Chinese Ministry of Public Security's critical infrastructure protection scheme, and it places requirements upon networks and devices depending on the sensitivity of their application.
- ***Critical Network Equipment Security Testing Implementing Procedures***[15]: Requires certain products (e.g. PLCs) to undergo security testing and certification prior to sale within China. In many cases, however, the underlying standards by which testing is to take place are still in progress.
- ***Cybersecurity Review Measures***[16]: Requires a "national security review" when products (including OT) and services may impact national security, and authorizes the exclusion of products and companies that pose a supply chain risk to the Chinese market.
- ***Cybersecurity Vulnerabilities Administrative Regulation***[17]: Specifies procedures and responsibilities for vendors and network operators who discover cybersecurity vulnerabilities (to include OT manufacturers). It also discusses patching, countermeasures, and reporting requirements to relevant government agencies.

U.S. NIST IoT Security Minimum Baseline[18]: This is a U.S. effort to harmonize international IoT security requirements into a voluntary minimum baseline. Once finalized, the baseline will likely be incorporated into federal and state procurement requirements for IT and OT devices. Below are two related legislative efforts that place new requirements on OT device manufacturers:

- ***IoT Cybersecurity Improvement Act of 2019***[19] – Legislation in the U.S. Senate that will, if passed, establish new security requirements (based on the NIST IoT security baseline) for most IoT devices sold to the federal government.
- ***CA Connected Device Law***[20] – This is a new California state law that places requirements on manufacturers of "connected devices" to ensure devices sold in California after January 1, 2020, are equipped with "reasonable security features".

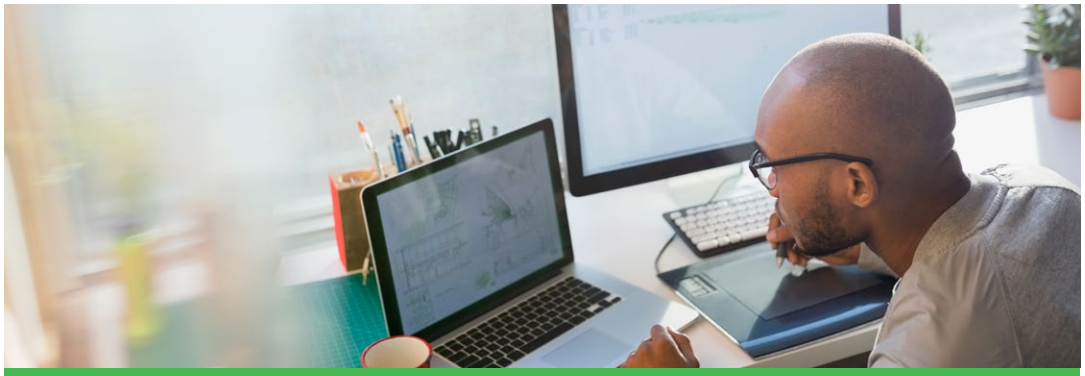
These country-specific requirements for IoT device manufacturers present several limitations. Instead of promoting widespread, open innovation, economic prosperity for the global digital economy, or consistent security protocols, disparate requirements will likely lead to regulatory fragmentation. As a result, only large players might be able to meet this myriad of requirements and consumers will be left to determine how secure a device is based upon where it is manufactured.

At Schneider Electric, there is hope for an alternative path — one that fosters both innovation and security for industry players, governments, and global citizens. It is a path where governments, vendors, and industrial companies work collaboratively, through open dialogue, to find a common regulatory ground. Ideally, this path would lead to harmonization and interoperability between IoT security requirements and corresponding certification schemes, enabling more secure devices to more quickly reach the users who need them.

Conclusion: Strengthening digital trust

Governments and industry have an opportunity to come together to work collaboratively on common solutions that will benefit all citizens. Doing so allows industry stakeholders to facilitate the tectonic shift in industrial revolution can be catalyzed by accelerated digitization in a safer, more productive, and more efficient way in our hyper-connected world.

At Schneider Electric, we strive to do our part. We are highly focused on safety and the legendary reliability and cybersecurity of our solutions to ensure business continuity in protecting people, assets, and data. As members of both the Cybersecurity Coalition and the Global Cybersecurity Alliance, we will work across industry, governments, and our customers to secure the global digital economy. Only together can we raise the bar on protecting the industry at large and strengthening digital trust and confidence as global industry pursues the benefits of the IIoT.



References

[1] Gartner. (2017). Leading the IoT: Gartner insights on how to lead in a connected world. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[2] Hutt, R. (January 23, 2016). 9 quotes that sum up the Fourth Industrial Revolution, World Economic Forum Agenda. Retrieved from https://www.weforum.org/agenda/2016/01/9-quotes-that-sum-up-the-fourth-industrial-revolution/

[3] Zetter, K. (November 29, 2010). Iran: Computer malware sabatoged uranium centrifuges. Wired. Retrieved from https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/

[4] Heiligtag, S., Maurenbrecher, S., and Niemann, N. McKinsey. (February 2017). From scenario planning to stress testing: the next step for energy companies. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/from-scenario-planning-to-stress-testing-the-next-step-for-energy-companies

[5] Reuters. (May 14, 2017). Cyber attack hits 200,000 in at least 150 countries: Europol. Retrieved from https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries- europol-idUSKCN18A0FX

[6] Menze, T. ARC Group and Kapersky. (July 2019). The state of industrial cybersecurity report 2019. Retrieved from https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

[7] Abbosh, O., and Bissell, K. Accenture. (2019) Reinventing the Internet to secure the digital economy. Retrieved from https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

[8] Schwab, W. and Poujol, M. CXP Group and Kapersky. (July 2018). The state of industrial cybersecurity report 2018. Retrieved from https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf

[9] Schneider Electric. (July 29, 2010). Schneider Electric is Founding Member of ISA Global Cybersecurity Alliance. Retrieved from https://www.se.com/ww/en/about-us/press/news/corporate-2019/founding-member-of-isa-global-cybersecurity- alliance.jsp

[10] Opiah, A. (August 14, 2019). ISA Global Cybersecurity Alliance Welcomes Schneider Electric As Founding Member. Retrieved from https://data-economy.com/isa-global-cybersecurity-alliance-welcomes-schneider-electric-as-founding-member/

[11] Schneider Electric. (March 4, 2019). Schneider Electric Affirms Role in Strengthening Digital Trust by Joining the Cybersecurity Coalition. Retrieved from https://www.se.com/ww/en/documents/Press/2019/03/04-release-cybersecurity-coalition-tcm50-463982.pdf

[12] The EU Cybersecurity Act. Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

[13] Creemers, R., Triolo, P., and Webster, G. (June 29, 2018). Chinese Cybersecurity Law Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

[14] Lu, X., Triolo, P., Sacks, S., Creemers, R., and Webster, G. (July 18, 2018). Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/

[15] L, C., Neville, K., and Webster, G. (June 12, 2010). Translation: New Draft Rules for 'Critical Network Equipment Security Testing' in China. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-critical-network-equipment-testing-implementing-measures-draft-comment

[16] Sacks, S., Creemers, R., Laskai, L., Triolo, P., and Webster, G. (May 24, 2019). China's Cybersecurity Reviews for 'Critical' Systems Add Focus on Supply Chain, Foreign Control (Translation). Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control- translation/

[17] Peterson, D., Zhong, R., (June 19, 2019).Translation: Chinese Rules for Managing Cybersecurity Vulnerabilities Published in Draft Form. Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-rules-managing-cybersecurity-vulnerabilities-published-draft-form/

[18] NISTIR 8259(Draft). (July 2019). Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers. Retrieved from https://csrc.nist.gov/publications/detail/nistir/8259/draft

[19] S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017115th Congress (2017-2018). Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt

[20] CA Connected Device Law. SB-327 Information privacy: connected devices.(2017-2018). Retrieved from https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Schneider Electric USA
800 Federal Street, Andover, MA 01810
Telephone: 978-794-0800
www.schneider-electric.us

998-20728901_GMA-US Rel. 12/19