



Lifecycle Cybersecurity

How to secure a buildings mission critical power infrastructure.

Publication/ Presentation details

Anthony Ciccozzi,
Lead Cybersecurity Engineer

Eric Rueda,
Commercial Leader Software & Connectivity

John Robb,
Segment Leader Commercial and Industrial Buildings

Ciaran Forde,
Segment Leader Data Center and IT



Powering Business Worldwide



Contents

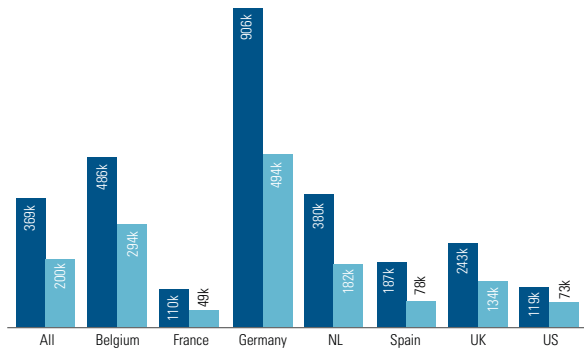
- Introduction 3
- What is Mission Critical Infrastructure? 4
- The difference between OT and IT..... 7
- Why attack Mission Critical Infrastructure? 8
- Protecting Mission Critical systems with full lifecycle cybersecurity..... 10
- Supply chain security – Vendor selection 11
- Secure by Design – meeting standards..... 12
- Conclusion 12
- Appendix A- Basic cybersecurity lifecycle maintenance checklist..... 13
- Appendix B- Useful references 14

Introduction

Tackling cybercrime has never been more important. The mean cost of all cyber security incidents recorded in 2019 was US\$369,000 per business. Globally, the impact of cybercrime is predicted to cost US\$10.5 trillion a year by 2025¹. If it were a country, it would be the world's third largest economy, after the US and China. However, 60 percent of losses are due to interruption to business rather than the attack itself².

Mean cost of cyber incidents (\$)

● Mean cost of all incidents ● Mean cost of single largest incident



Source: Hiscox Cyber Readiness Report 2019

Cybersecurity is often associated with data and Information technology (IT) or telecommunications networks. We are all too familiar with the concept and dangers of IT systems being 'hacked'. But what about systems outside the main data network, such as the system that enables that data network to function? Are these areas also vulnerable to cyber attack? Think about shutting down HVAC for instance that will cause servers to shutdown themselves to protect from temperature increase.

Electrical power is so intrinsic to our daily lives it is easy to take it for granted. But as digitalization accelerates across all sectors and applications, so too does electrification. You can't have digital transformation without electrification. So, when an application is **critical**, like a hospital, airport, or telecommunications network, the supporting electrical infrastructure and facilities automatically become **mission critical**. A failure in the operation of the associated building or facility and its supporting power network can mean a direct

failure in the critical application. This is especially true in the case of data centers. Extreme efforts are made at the design, build, and operational phases to ensure total reliability and continuous operation, or uptime. The sophistication of these environments means they, too, increasingly utilize digital and network connectivity to manage the power infrastructure and the overall facility. As approaches like Energy Management and Building Management systems evolve from basic monitoring and management to further automation management of the assets without human intervention and even artificial intelligence, one can see the criticality for these supporting systems to become cybersecurity at both software and hardware levels.

The role of data centers has changed dramatically in the last 20 years. They, and the telecommunication networks that support them, are essential to business operations and communications. IT communications are protected using advanced data encryption and firewalls. Physical access is also extremely tightly controlled. But what of the facility systems themselves? How are the power networks, HVAC, fire detection and suppression systems protected? As these systems evolve, so does the accompanying complexity and distributed connectivity. This, in turn, brings with it a series of cybersecurity risks.

Discussions around the lifecycle maintenance and cybersecurity of critical electrical infrastructure will often turn to the issue of responsibility. The traditional domains and roles of IT and Operational Technology (OT) are converging; Facilities Managers and Engineering teams need to understand more about networking and systems administration, while IT teams are required to know more about the types of technology they use and its availability needs. And this convergence doesn't just refer to technology and networks. It also impacts the skills and approaches needed to comprehensively maintain a facility's power infrastructure throughout its lifecycle. There are often increasing resource constraints too, due to budget restrictions and skills gaps that need to be addressed.

Recent cyber attacks on mission critical infrastructure have highlighted the growing importance of a robust cybersecurity strategy. But, given the challenges faced by both IT and OT teams today, the effectiveness of any strategy for integrating cybersecurity into a facility's overall lifecycle maintenance will depend on - at least - a basic understanding of critical power infrastructure, and the technology, connectivity, and cybersecurity risks involved.

¹Cybercrime To Cost The World \$10.5 Trillion Annually BY 2025 - Cybercrime Magazine, November 13, 2020

²The Cost of Cybersecurity Incidents is on the Rise, Mainly Due to Human Error or Systems Failure - Bitdefender Business Insights Blog, November 20, 2020

What is Mission Critical Infrastructure?

All critical infrastructure requires a supply of reliable, cost-effective power. An interruption to that supply will range from a minor inconvenience or reputation damage to issues around safety, health, public panic, or even life-threatening situations.

To better manage their critical power infrastructure, businesses employ systems such as Building Automation Systems (BAS), Building Management Systems (BMS), and Building Energy Management Systems (BEMS), each of which has some degree of processing capacity and is connected to the outside world.

These systems fall under the category of OT networks, examples of which are shown in Figure 1 on the right.

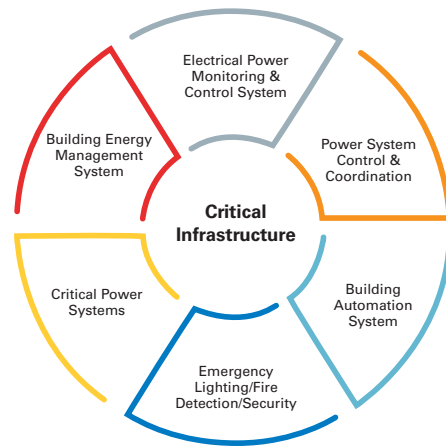


Figure 1: OT Networks in Commercial Facilities

OT networks monitor and ensure the safety of building infrastructure that operates key systems including lights, elevators, and heating and cooling systems.

Figure 2 shows many of these systems as they would typically be found in a commercial building.

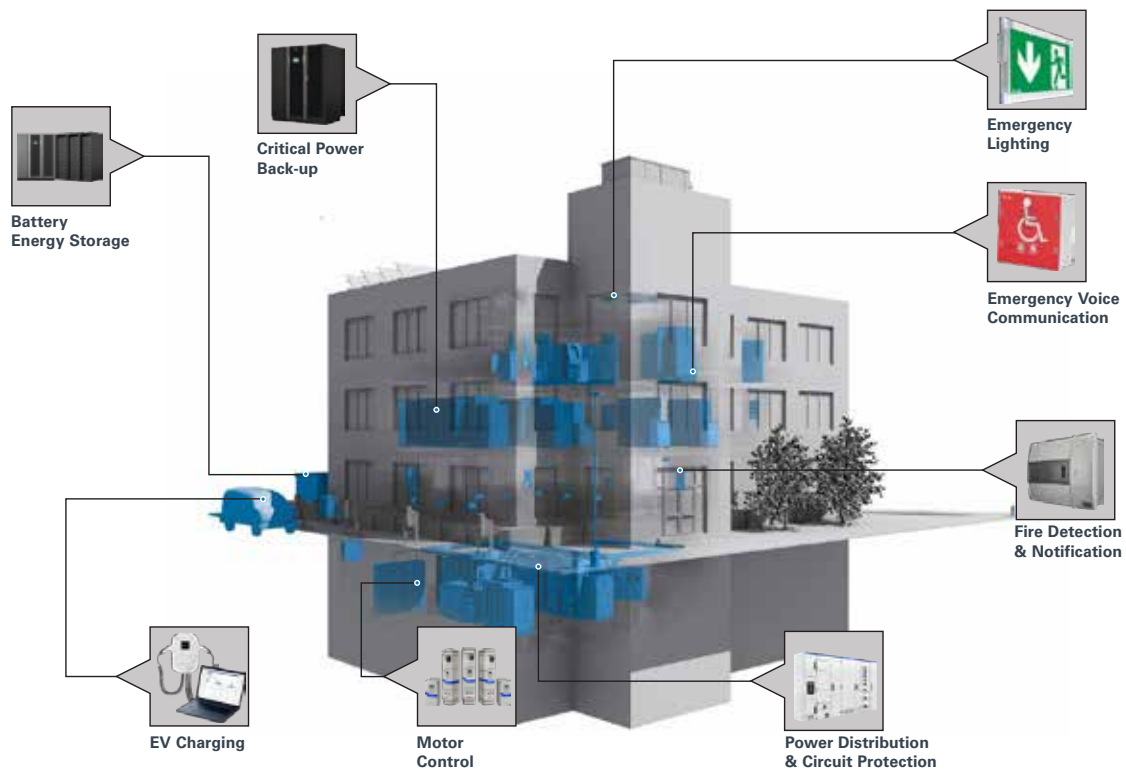


Figure 2: OT systems in a Commercial Building

Figure 3 shows several power system components as they would be distributed across a critical facility - in this case, a data center. These components would typically include switchgear, Automatic Transfer Switches (ATS), Uninterruptible Power Supplies (UPS), transformers, breakers, and protective devices. Although they're not shown in the illustration, we can also assume the inclusion of several Programmable Logic Controllers (PLC), and the Commercial Off-The-Shelf (COTS) switches, routers, and firewalls used to integrate these components into a coordinated OT control and monitoring network.

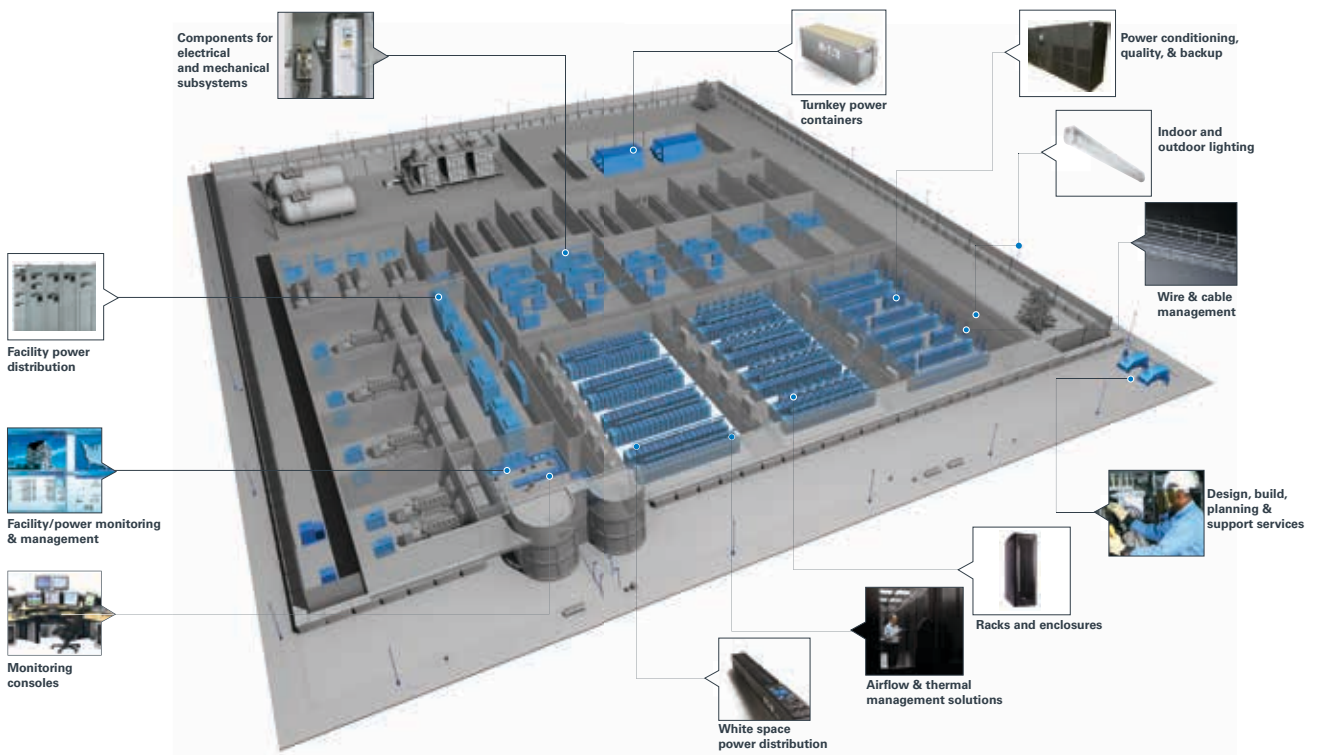


Figure 3: Mission Critical Power Infrastructure in a data center



Together, these systems and components form an attack surface, from which cybercriminals can gain access to a business and interact illicitly with its systems. By adding connectivity to your electrical power, building energy management, and fire detection systems, the Internet of Things (IoT) makes them potential targets for cybercriminals. Imagine the fear and chaos the loss of control and disconnection of your systems, or the disruption of your processes would cause to your company, employees, and customers.

In addition, other systems including HVAC, elevators, and security (camera/badge readers), collectively make up the entire OT infrastructure adjacent to and requiring power from mission critical power infrastructure, and are vital in helping businesses ensure they provide the round-the-clock capacity that critical infrastructure demands. This diversity and distribution of assets create an additional attack surface which cyber-attacks might use to achieve their objectives, even when the relevant IT systems are thoroughly secured. Figure 4 shows just how vulnerable some of these Industrial Control System (ICS) components - both IT and OT - are to attack, and highlights just how vital it is to ensure their protection.

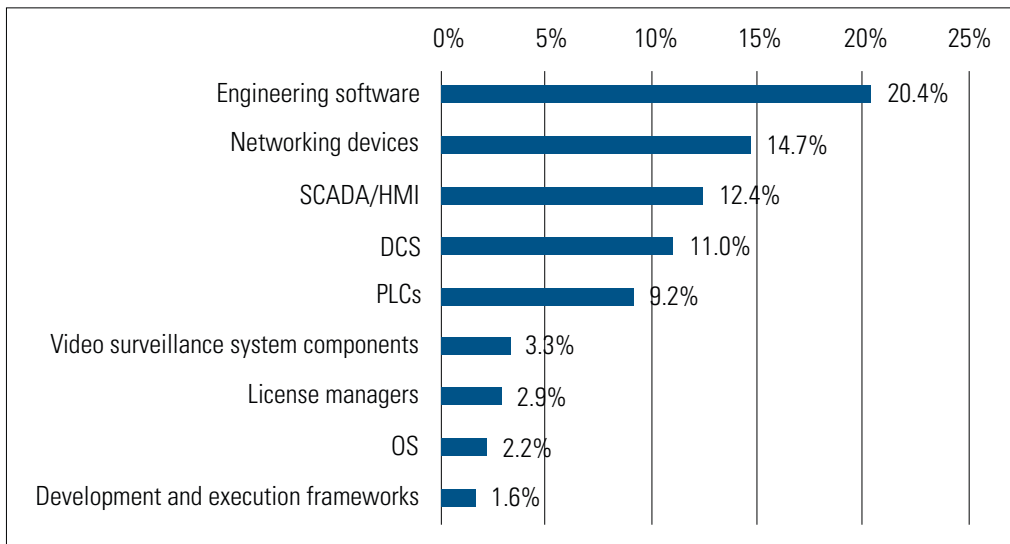


Figure 4: Percentage of vulnerabilities identified in various ICS components to all vulnerabilities³

³Threat landscape for industrial automation systems. Vulnerabilities identified in 2019 - Kaspersky ICT CERT

The difference between OT and IT

When it comes to cybersecurity, there is a risk that businesses have been focusing almost exclusively on their IT infrastructure. Because IT deals with the acquisition, storage, processing, and sharing of data and information, it can feel like the obvious target for cyber attacks. While there can be gaps in protection and the threat landscape is continually evolving, IT technology is generally well defined in terms of standards, policies, practice, and technologies. Focused on controlling the physical world, the security of OT is less well understood and defined. But as businesses become ever-more digitally driven, the opportunities for cyber attacks are growing beyond the IT infrastructure. IT technologies are increasingly embraced by OT. As a result, OT has now inherited the threats IT has faced for years.

There are several gaps in securing the OT networks that control the physical world, and support building infrastructure

that operates key facility systems. The different objectives and technologies used in each discipline means cybersecurity for OT networks needs to be considered differently from cybersecurity for IT. Some IT methods and tools can also be applied to OT, but they need to be applied in such a way that they don't impede or impact the real-time operation of the system. Focused on protecting data, IT security may be willing to compromise on the uptime and availability, for example, both of which are an essential focus for OT.

But, as IT cybersecurity measures are traditionally applied and adapted to address the demands of constantly changing technologies, this can often lead to an assumption that the risks to OT assets are also addressed. Due to the differing characteristics and objectives outlined in Figure 5, though, many organizations can be partially or wholly incorrect in making this assumption.

Parameter	IT	OT
Focus	Data and information	Controlling aspects of the physical world
Responsibility	IT/Networking staff	Engineering/Facilities teams
Asset types	Servers, workstations, laptops, software, mobile devices, network devices, storage, virtual assets	Programmable logic controllers (PLCs), remote terminal units (RTUs), Human machine interfaces (HMIs), sensors, actuators, input/output (IO) modules, general embedded devices
Lifecycle	3 - 5 years	> 10, 20, 50 years
Priorities	1. Confidentiality 2. Integrity 3. Availability	1. Availability 2. Integrity
Patching/upgrades	Well-defined and supports automation (e.g. for Windows servers)	Limited (technically not possible or practical due to operational concerns) Automation generally not possible
Network traffic	Dynamic and diverse	Static and repeatable
Security tools	Widely available (e.g. Antivirus for workstations or servers, web firewalls, network monitoring tools)	Partially applicable in some cases (e.g. firewalls) but generally requires capability embedded into devices

Figure 5: IT vs OT characteristics

Fundamentally, OT is the hardware and software that keeps critical infrastructure running. It often relies on IT infrastructure, however, especially when communicating with assets across different locations. Consider a system that, while monitoring OT assets in a substation or control room, relies on a data center in a remote location. The OT assets depend on both the IT network and the data center infrastructure to facilitate communication and data processing. This then leads to a situation of distributed authority where, when looking at the end-to-end implementation, responsibility for the monitoring the OT assets is distributed among IT, networking, and engineering and facilities staff.

OT systems and assets have long lifecycles - more than 10 years in most cases - which can result in them using out-of-date software and legacy hardware, that may not be actively supported. This makes these systems difficult to patch and more vulnerable to exploitation by malicious actors. This highlights the need to select products and vendors that actively review the cybersecurity state and provide updates throughout the expected lifecycle. It also highlights the need to maintain accurate inventories and continuously assess the system for vulnerabilities and weaknesses and actively mitigate the resulting risks.

Why attack Mission Critical Infrastructure?

While most cyber attacks target traditional IT infrastructure, there have been several in recent years which have targeted OT or Industrial Control System (ICS) networks. One attack on a nation's power grid left over 225,000 households without electricity. Using spear phishing emails to gain a foothold in the network, the attackers installed malware on SCADA systems, which enabled them to trip circuit breakers and turn off the power to the utility's customers. A subsequent denial-of-service attack on its call center meant those customers were unable to report or receive information on the outage.

This particular incident highlights how malicious actors can initiate complex attacks on mission critical infrastructure. Motivations may range from financial reward - a ransomware attack, for example, will lock a company's entire network until

a ransom is paid; information theft - where sensitive personal, corporate and financial information can either be used to carry out further attacks or sold on the black market; to meet some political, military, or terror objectives; or simply to delay and disrupt services.

Attackers must gain access to their target's system in order to achieve their objectives. They often initiate supporting attacks to cause further disruption but also delay the identification and isolation of the targeted subsystems as well as the recovery from their primary attack. This requires them to exploit the attack surface, the term used to describe the sum of entry points to a system. As illustrated in Figure 6, below, once inside the system, they can pivot, moving from asset to asset, listening, learning, and exfiltrating information, often lying undetected for months before taking control of the system.

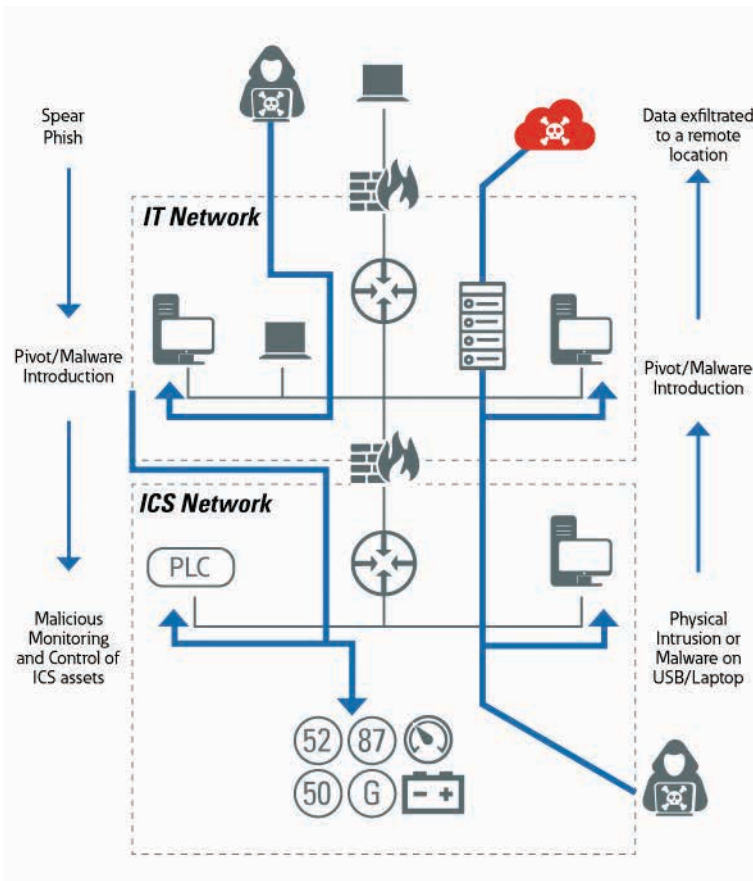















Figure 6: Example chain of events in an attack

This image is showing the sequence of events for two kinds of compromises- Left half of the image shows how an attacker could leverage spearphishing to ultimately reach a point to monitor & control the ICS assets. While the right half depicts how through physical intrusion an attacker could reach corporate assets and ultimately exfilter sensitive corporate data.

The following table lists some of the common vulnerabilities and weaknesses that can be exploited by criminals to allow them entry to mission critical infrastructure.

Common Control System Vulnerabilities and Weaknesses

	No clear authorization boundaries (distributed assets = distributed authority)
	Inadequate Remote Access Controls
	Improper segmentation/architecture
	Inadequate boundary defenses (to EPMS, Electrical Power Management System)
	Lacks separation of duties/functions
	Malware/malicious code
	Lack disaster recovery/incident response
	No visibility/security monitoring
	Inadequate boundary defenses
	Weak System Access Controls (RBAC Role-based access control, Least Privilege, Authentication)
	Rogue Asset/Infected Transient Cyber Asset
	Infected USB/Removable Media
	Out of date components/known vulnerabilities

Once again, it comes down to the question of responsibility. The abundance of vulnerabilities and weaknesses commonly found in mission critical infrastructure is largely due to the fact that multiple groups are responsible for different aspects of the system - the IT team is responsible for the network on which the workstations in the equipment room run, but facilities are

responsible for the electrical system that powers both the workstations and the network they run on. Not only does this silo-based approach cause a potentially dangerous level of uncertainty around a system's security, but it can also inhibit an organization's ability to respond to an incident and recover availability.

Protecting mission critical systems with full lifecycle cybersecurity

A discipline of risk management, cybersecurity isn't about making a binary choice between "secure" and "not secure". Neither is it something that can be applied just once and left alone, or considered at procurement and then forgotten about. Instead, cybersecurity must be applied across the entire lifecycle of a system - considering every asset from product selection through weekly, monthly, and yearly maintenance, to decommissioning. The security of a network or system is only as strong as its weakest link. Organizations should therefore employ basic cybersecurity hygiene, and continuously analyze emerging threats to ensure systems are deployed securely. In addition, they should take inventory of everything connected to their networks, and employ a zero-trust model.

The key tenets of effective cybersecurity lifecycle maintenance are:

- Know what you have
- Know how it's connected
- Know how it's configured
- Know its patch state
- Know how to recover
- Know who to contact
- Look for overlap and efficiencies






An effective cybersecurity strategy for a facility's operational technology requires a comprehensive strategy that covers **People, Processes and Technology.**

People tend to be the weakest link in the chain when it comes to security. Skilled attackers abuse the element of trust to make their way into an organization's systems via social engineering techniques such as phishing. Defending your organization by training your people, vendors and internal stakeholders should therefore become the first line of defense.

Your own processes, too, should consider the security of all the components in your infrastructure, and should have defined roles, responsibilities for both your IT and OT teams. Ensure you have robust plans for vulnerability management and incident response, as well as a dependable disaster recovery plan.

Furthermore, it's important to ensure you work with trustworthy suppliers who understand the importance of cybersecurity and have a robust cybersecurity program in place. Select products, systems, and solutions that are designed with cybersecurity in mind and that meet industry standards throughout their full lifecycle. They should be regularly assessed for potential vulnerabilities and patched to address discovered security loopholes and vulnerabilities on a regular basis. It's also imperative that your facility's OT network and assets are periodically assessed for cybersecurity measures.

See Appendix A for a checklist of suggested steps in full lifecycle cybersecurity maintenance. A summary is listed in the image below.

	<p>Inventory... all connected hardware, software, dataflows and correlate with reality, monitoring, and drawings</p>
	<p>Collaborate... with vendors and internal stakeholders to review roles & responsibilities and identify gaps in governance (e.g. disaster recovery and incident response)</p>
	<p>Integrate... cybersecurity into overall lifecycle maintenance (look for overlap in activities, skillsets, and competencies)</p>
	<p>Train... staff on OT-specific cybersecurity considerations including best practices and policies around USB and maintenance laptops</p>
	<p>Assess... facilities, OT networks, and assets to evaluate the attack surface and discover known vulnerabilities and weaknesses</p>

Supply chain security – Vendor selection

As more manufacturers and industries build and deploy IIoT devices, the security and safety of systems providing essential operations become more important and more difficult to manage. These complexities are due, in part, to a lack of a global, universally accepted cybersecurity standards and conformity assessment schemes designed to validate connected products.

The economic challenges to safeguarding IIoT ecosystems spawn from the complex manufacturing supply chain and the difficulty of assigning clear liabilities to manufacturers and system integrators for any vulnerabilities introduced. Most products and systems assemblies consist of components from different suppliers. So, where should the element of trust begin and end if there is no global conformity assessment scheme to ensure that products and systems are designed to be compliant with the global standards defined by the industry?

There are currently a multitude of different standards and regulations created by various organizations, countries, and regional alliances across the globe. All of these standards and regulations address the urgent need to secure our connected world, however they also create the potential for confusion and possibility of weak links in critical infrastructure ecosystems.

For the purposes of supply chain cybersecurity, NIST (National Institute of Standards and Technology) best practices rely on the need to assume a zero-trust environment to encourage organizations to deploy appropriate controls. For greater clarity, ISO 27034, IEC 62443 4-1 provides guidance around a Secure Application/Product Development Lifecycle (SDLC) for application security.

Securing mission critical infrastructure starts with selecting vendors and components that provide a level of supply chain cybersecurity assurance. Key things to look for are vendors whose components are secure by design, and that apply SDLC principles to all their products. SDLC considers a wide range of industry standards and best practices, such as IEC-62443 or UL2900, full-lifecycle vulnerability management, secure remote access methods, and supports authenticity and integrity, assuring that the firmware/software running on the device is authorized by the vendor. As illustrated in Figure 7, below, SDLC spans from inception through to deployment and maintenance, enforcing cybersecurity best practices via training, threat modelling, requirements analysis, implementation, verification, and ongoing support. Ideally, the vendor and products will have some type of third-party validation or certification of their processes to provide additional assurance beyond their claims.

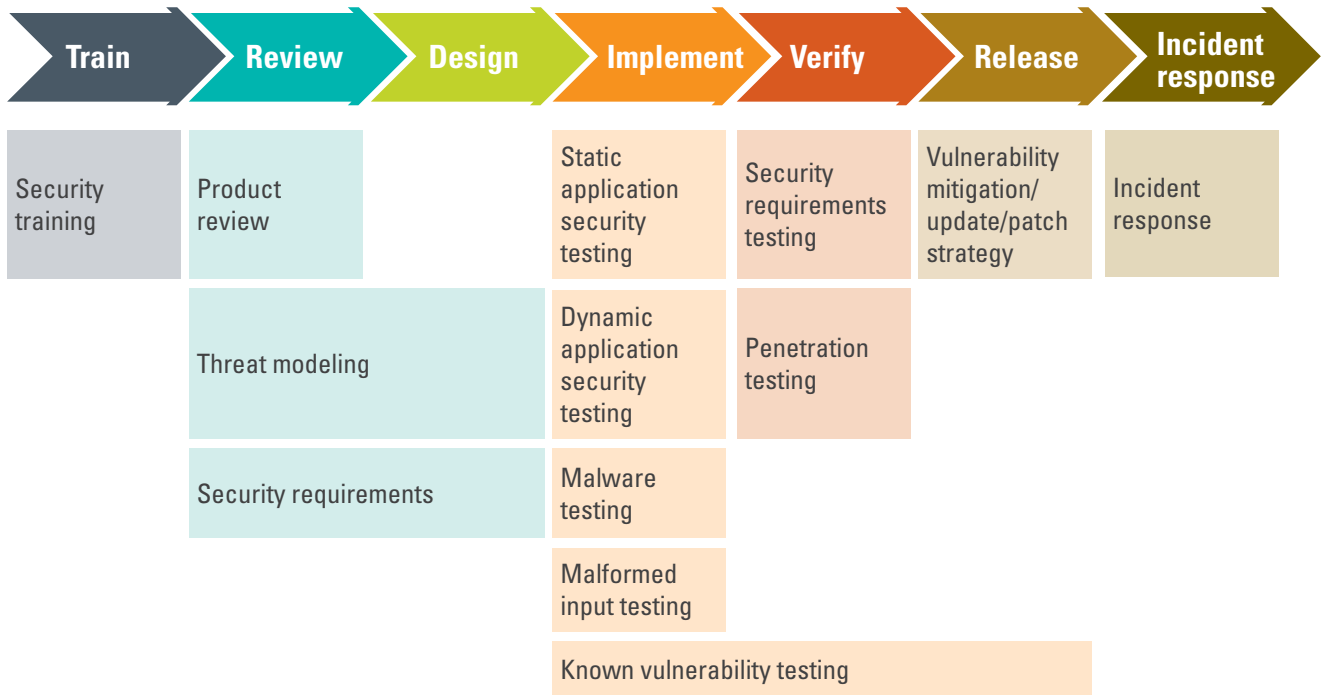



Figure 7: Secure Development Lifecycle (SDLC)



We would advise prospective buyers to look for established vendors with recognized levels of cybersecurity hygiene and governance, in addition to well-documented, repeatable, and measurable processes for providing assurance to their customers.

In summary, supply chain cybersecurity for devices centers around the following:

- Authenticity and integrity of firmware/software
- Secure by Design (i.e. minimized attack surface out of the box)
- The ability to be deployed securely in a system (e.g. strong access controls, optional secure remote access capability)
- Being part of a Secure Development Lifecycle (SDL or SDLC) to manage cybersecurity risks
- 3rd party validated SDLC
- Full Lifecycle Vulnerability Management
- Secure storage and governance

Secure by Design – meeting standards

To ensure equipment isn't the weakest link in an organization's cybersecurity posture, solutions must be deployed securely across an entire system to ensure the authenticity and integrity of every instance of firmware and software. It's important, too, that it forms part of a Secure Development Lifecycle (SDLC), as outlined above.

Crucially, the concept of an SDLC doesn't only apply to the consideration of cybersecurity risks over an asset's lifetime - inception, design, development, deployment, integration, maintenance, and decommissioning; it also applies to the asset to which it's applied.

Further assurance can be granted by ensuring devices and systems meet certain industry standards.

The 2900 Standard for Software Cybersecurity for Network-Connectable Products (UL 2900), for example, was the first guideline of its kind, including processes to test devices for security vulnerabilities, software weaknesses and malware. Introduced by global safety certification company, Underwriters Laboratories Inc.'s (UL), this standard confirms that a device manufacturer meets the guidelines for:

- Risk management processes
- Evaluation and testing for the presence of vulnerabilities, software weaknesses, and malware
- Requirements for security risk controls in architecture and product design

UL also provides a Data Acceptance Program for manufacturers, which certifies testing laboratories with the global capability to test products with intelligence or embedded logic to key aspects of the UL2900 standard. By purchasing products tested in these specialized labs, customers can rest easier, knowing their devices are compliant with the industry's highest cybersecurity requirements before they're installed in critical systems.

Similarly, the IEC adopted the 62443 series of standards, which provides a framework to address the cybersecurity of Industrial Control Systems. These standards provide requirements for all of the principal roles across a system's lifecycle – from product design and development through integration, installation, operation and support. In 2018, the IEC added 62443-4-2 to improve the security of products.

Conclusion

Digitalization offers businesses greater automation, speed and flexibility when it comes to monitoring and controlling the supply of power to critical infrastructure. The benefits of digitalization are only possible if it's secure. As attacks such as that on the power grid demonstrate, IT networks can be used as a way in to attack OT systems. OT itself therefore needs to be hardened against attack.

Businesses need to be confident that the technology they buy to make their buildings work won't leave them vulnerable to attack. Security shouldn't be a secondary consideration for OT systems. In order to trust that their critical infrastructure is safe, it's vital that businesses consider lifecycle cybersecurity alongside function when choosing new control systems and assets. When it comes to Cybersecurity, 'If it ain't broke, don't fix it' strategy, unfortunately, does not work in favour of the customers, but works to the advantage of the adversaries.

To find out more about full lifecycle supply chain cybersecurity considerations for your critical infrastructure, please visit www.eaton.com/cybersecurity or contact Eaton.

For years, Eaton has maintained strict procedures at every stage of the product development process. Eaton is the first company to have its product development processes certified by both the International Electrotechnical Commission (IEC) and global safety science organization UL.

Appendix A

Basic cybersecurity lifecycle maintenance checklist

<input type="checkbox"/>	Does a cybersecurity awareness & training program exist (for employees and vendors)?
<input type="checkbox"/>	Are only authorized devices communicating on the network?
<input type="checkbox"/>	Is remote access to system assets secure (strong access controls, boundary defenses, etc.)?
<input type="checkbox"/>	Are unaddressed vulnerabilities present on any system assets?
<input type="checkbox"/>	Is network traffic monitored for unauthorized, anomalous, and malicious behavior?
<input type="checkbox"/>	Are strong system access controls in place and least privilege applied (e.g. no default passwords)?
<input type="checkbox"/>	Are asset owners, authorization boundaries, and responsibilities clearly defined?
<input type="checkbox"/>	Do accurate inventories of authorized hardware, software, and dataflows exist?
<input type="checkbox"/>	Do accurate network/topology drawings exist showing all connected devices?
<input type="checkbox"/>	Are secure configurations for all assets defined and deployed (no default credentials, only necessary ports, and services running/open, disable unused physical ports, etc.)?
<input type="checkbox"/>	Does an asset (device) qualification and decommissioning program exist?
<input type="checkbox"/>	Are trust boundaries identified and segmentation/boundary defenses deployed?
<input type="checkbox"/>	Are malicious code detection/prevention mechanisms deployed and up to date?
<input type="checkbox"/>	Are assets included in a security monitoring and protection program?
<input type="checkbox"/>	Are all assets synchronized to the same (accurate) time and time zone?
<input type="checkbox"/>	Does a vulnerability management program exist?
<input type="checkbox"/>	Are vulnerability assessments performed on the system (at least yearly)?
<input type="checkbox"/>	Does an incident response program exist?
<input type="checkbox"/>	Does a backup and disaster recovery program exist?

Appendix B - Useful references

Integrating Cybersecurity into Industrial Control System Lifecycle Maintenance -

<https://www.eaton.com/content/dam/eaton/services/eess/eess-documents/eaton-cybersecurity-lifecycle-maintenance-wp027017en.pdf>

Carnival takes remedial action after cyber breach -

<https://www.rivieramm.com/news-content-hub/carnival-takes-remedial-action-after-cyber-breach-60636>

Eaton Secure Development Lifecycle -

<https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/eaton-cybersecurity-secure-development-lifecycle-brochure-lr-en-us.pdf>

Cybersecurity in hyper-connected utilities and industrial applications -

https://www.eaton.com/content/dam/eaton/markets/utility/knowledge-center/infographics&listicles/Eaton_Cyber_Security_Infographic_FINAL.pdf

Cybersecurity considerations for electrical distribution systems -

<https://www.eaton.com/content/dam/eaton/products/industrialcontrols,drives,automation&sensors/c441-motor-insight-motor-protection-relays/cyber-security-white-paper-wp152002en.pdf>

Security best practices checklist reminder -

<https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf>

Eaton Secure Development Lifecycle brochure -

<https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/eaton-cybersecurity-secure-development-lifecycle-brochure-lr-en-us.pdf>

Eaton Electric Limited
252 Bath Road
Slough
SL1 4DX
Customer Support Centre
Tel: +44 (0)8700 545 333
Fax: +44 (0)8700 540 333
email: ukcommorders@eaton.com

© 2021 Eaton
All Rights Reserved
Printed in UK
Publication No. WP083040EN
February 2021

Changes to the products, to the information contained in this document, and to prices are reserved; so are errors and omissions. Only order confirmations and technical documentation by Eaton is binding. Photos and pictures also do not warrant a specific layout or functionality. Their use in whatever form is subject to prior approval by Eaton. The same applies to Trademarks (especially Eaton, Moeller, and Cutler-Hammer). The Terms and Conditions of Eaton apply, as referenced on Eaton Internet pages and Eaton order confirmations.

Eaton is a registered trademark.

All other trademarks are property of their respective owners.