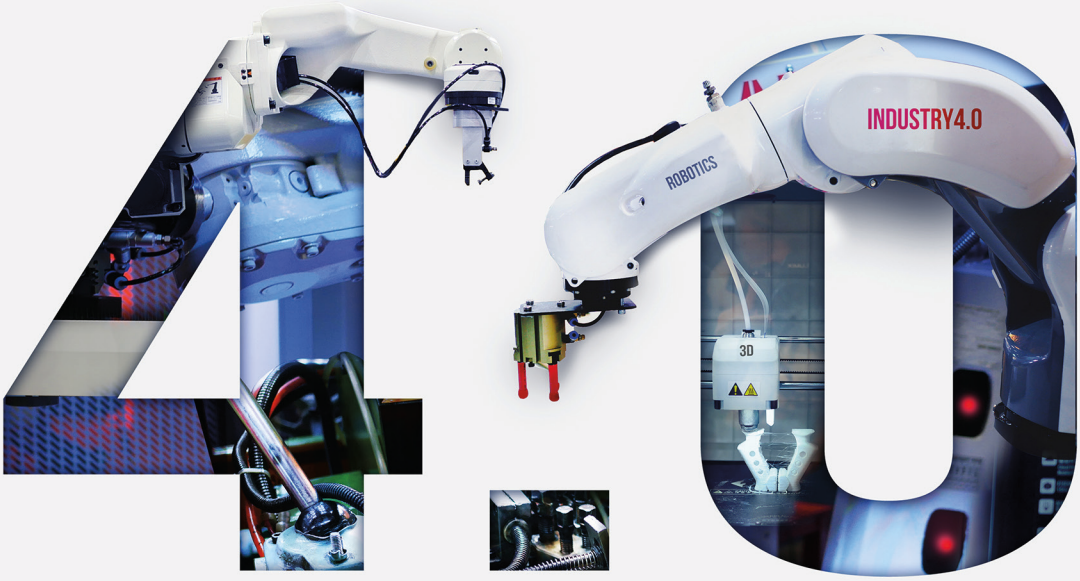
CGI

Experience the commitment®

Industry



and cybersecurity:

How to protect your business against cyber risks

A methodology for assessing and securing the OT environment

With the digitization of factories and digitally connected value chains, traditional IT security practices and solutions can only partly offer answers to protect manufacturing organizations.

Executive summary

Digital transformation, also referred to as Industry 4.0, smart industry and smart manufacturing, has risen to the top of the C-level agenda. This transformation is driving innovation in new products and services, digitization of business processes and the creation of new business models and ecosystems. This fourth wave is very exciting. At the same time, the shift to Industry 4.0 comes with significant challenges for manufacturers as it makes operations across the enterprise and supply chain more vulnerable to cyber threats.

Unsurprisingly, cybersecurity is on the critical path for digital enterprises, with board-level accountability. In fact, the 2019 CGI Client Global Insights reveals that there is a strong link between digital transformation and information and operational security in the organization. However, in the manufacturing industry, 59% of executives interviewed indicate they face cybersecurity challenges in implementing their digital transformation strategies.

With the digitization of factories and digitally connected value chains, traditional IT security practices and solutions can only partly offer answers to protect manufacturing organizations.

In this paper, we focus on the cyber risks faced in manufacturing operations and factories, industrial control systems and connected industrial devices. Based on best practices and CGI's extensive experience in this field, we share a methodology for assessing and securing the operational technology (OT) environment and recommend actions that executives, plant managers and operations staff need to take to effectively prepare for and address the growing complexity and speed of cybersecurity risks within Industry 4.0 environments.

[1]Annually, as part of the CGI Client Global Insights, CGI leaders around the world meet in person with client business and IT executives to gather their insights on the trends affecting their enterprises. In 2019, our local leaders met with more than 1,550 client executives across 10 industries.

Why Industry 4.0 poses an existential threat for manufacturing organizations

Industry 4.0 is driving unparalleled interconnectivity in manufacturing environments. Production facilities are increasingly integrating the Internet of Things (IoT) devices to monitor and control production systems, while brownfield plants are being upgraded to smart factories by adding wireless IoT devices. In fact, the total installed base of IoT connected devices is projected to be 75.44 billion worldwide by 2025.

Moreover, wireless connected sensors, networks and mobile devices like smart phones, tablets and wearables are entering the workplace. Modern industrial control systems (ICS) allow engineers to deploy fully automated and (almost) unmanned sites. Vendors of supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and manufacturing execution systems (MES) are offering mobile human machine interfaces (HMIs) and wireless communication facilities that enable operators and engineers to control equipment from physical locations both within and outside the plant. In addition, DCS controllers are now equipped with embedded servers that provide web access.

Equipment that perform the most critical and sensitive tasks in society such as controlling power generation and distribution, water purification and distribution, and chemical production and refinement are the most vulnerable on an industrial network. As ICSs become ever more connected to the internet, the threat of security breaches and possible damage to plant and processes has become very real. The specter of threat actors and cyberattacks targeting industrial networks and systems is growing exponentially, making cybersecurity in manufacturing more important than ever.

The specter of threat actors and cyber attacks targeting industrial networks and systems is growing exponentially, making cybersecurity in manufacturing more important than ever.

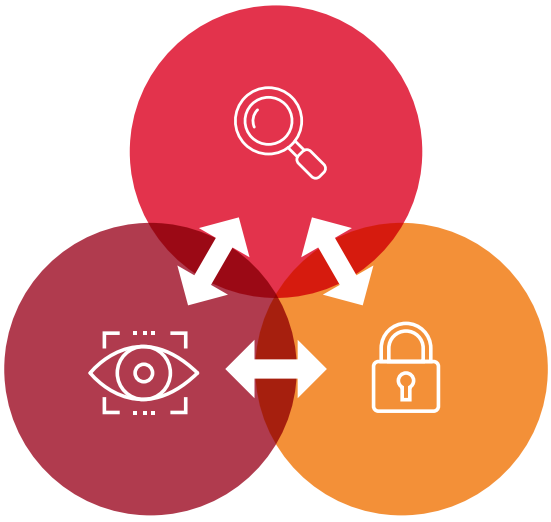
[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Dealing with cyber risks in manufacturing requires a holistic solution

With digital factories and a digitally connected value chain, there is a need for increased security, and traditional IT security is not enough to protect manufacturing organizations. Manufacturers need to take a holistic end-to-end approach—one that addresses people, processes, and technology—to adequately defend against growing cyber risks. That is why, we believe cybersecurity needs to become an integral part of a manufacturer's digital transformation strategy and roadmap, addressing both information technology (IT) and operational technology (OT), which includes ICSs. To achieve this requires a multi-pronged approach—one where cybersecurity policies, procedures, and controls are in place, there is greater awareness of cyber risks among employees, internal training programs are conducted regularly to stay current on skills and evolving threats, and there is access to the best cybersecurity talent and intelligence.

In the following pages, we share a proven methodology for this approach, helping organizations achieve a mature security level, safeguard their most valuable assets and ensure business continuity

Assess
Identify potential security risks from an organizational and technical point of view.



Monitor
Effectively monitor the industrial environment, assets and connections.

Secure
Mitigate identified security risks regarding people, technology and processes.

Figure 1: A holistic three-step cybersecurity methodology to secure OT environments

Part 1: ASSESS

Identifying potential security risks from an organizational and technical point of view

For manufacturers, developing a secure and resilient security strategy must begin with identifying the biggest risks to their primary production processes and ascertaining which elements are linked to their most valuable assets or “crown jewels.” Some of the key questions to ask include:

- What systems can impact the physical processes run by the factory?
- What would happen if a system fails? What is the corresponding impact?
- How fast can the systems be restored?
- Are the ICSs secure?
- Is our intellectual property safe?
- Is our supply chain vulnerable?
- What can we do to protect the business?

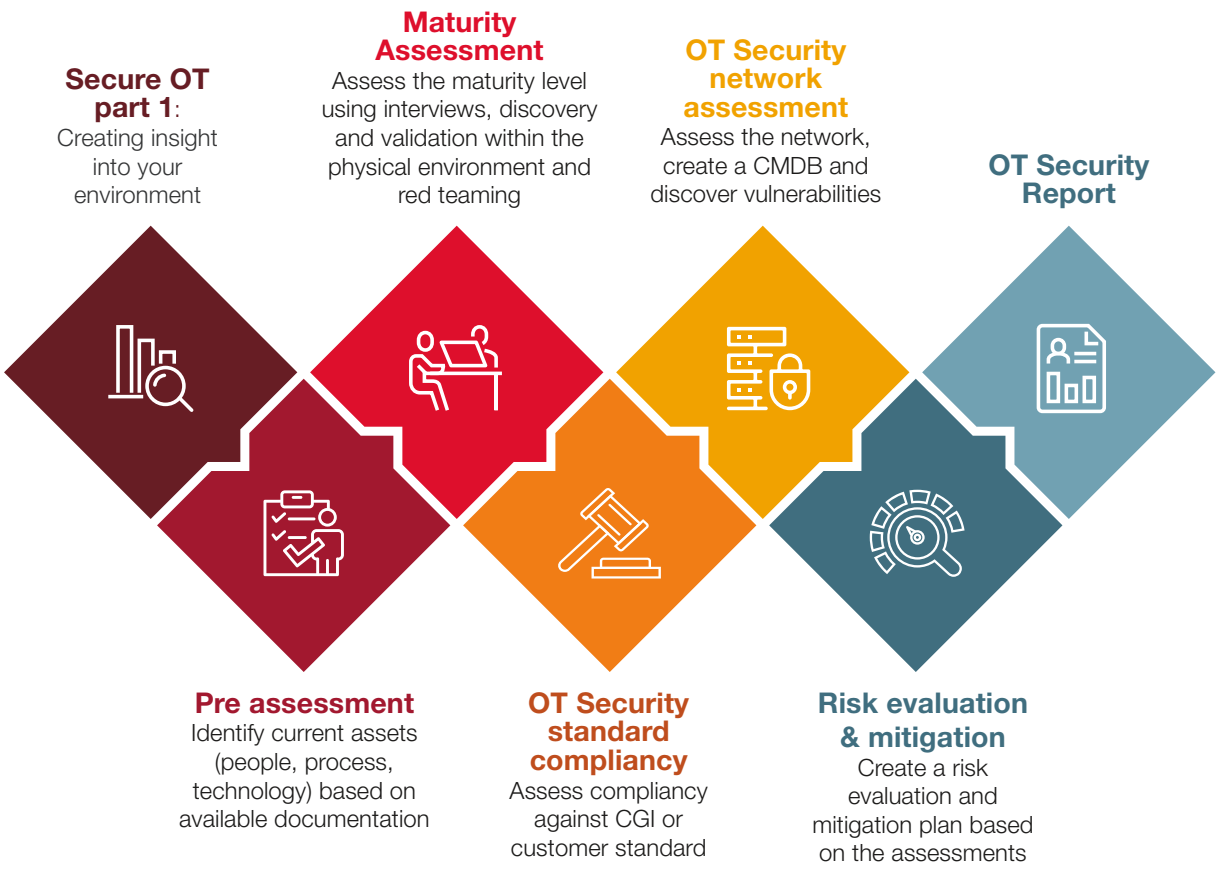


Figure 2: The steps involved in identifying potential security risks

The first step to effectively securing your OT environment is to examine it with respect to compliance requirements, threats, vulnerabilities and controls, and obtain a comprehensive overview of the security maturity level of the organization. The assessment needs to covers a broad range of security measures and their implementation within the OT environment and includes the following elements:

1. Pre-assessment:

This step provides an initial understanding of what and how security measures are implemented in the organization and in the factory or plant network. As part of the pre-assessment, assessors collect available documentation such as business impact analyses (BIA), network architecture diagrams, firewall rulesets and security policies.

2. Organizational maturity assessment:

This step provides an understanding of the security maturity level of the organization. It involves conducting interviews with various stakeholders across roles—from operator to management level—within the factory environment to gain an overview of the organizational setup and security governance, including the formal and informal structure. These interviews include international security standards such as the Industrial Automation and Control Systems Security (ISA-99/ IEC 62443), Information Security (ISO/ IEC 27002), NIST Special Publication 800-82, and NIST Framework for Improving Critical Infrastructure Cybersecurity. Questions must cover organizational governance, policies and frameworks such as BIA, risk frameworks, business continuity plans (BCPs), etc. as well as technical security measures (anti-malware, firewalls and -configuration, patching and hardening etc.). It is important for the answers collected during the assessment to be physically verified through in-factory inspections.

Figure 3: Multiple spider diagrams help to visualize the security maturity level of the organization

Based on the responses and their related scoring, multiple spider diagrams (Figure 3) are developed, illustrating the ambition level, levels shared during interviews and the ground reality based on the physical inspection of the factory or plant. These diagrams and the supporting detailed information gathered during the interviews will provide clear guidance on where to focus necessary improvement actions.

3. OT security standard compliance: While an Organizational Maturity assessment evaluates governance with regard to OT security, this assessment explicitly focusses on assessing practical OT security measures within the plant environment. Based on the combination of these two assessments, a comprehensive security baseline is developed. Topics addressed in the OT security standard compliance assessment should include network topology, anti-malware implementation, firewall settings, patch management, backup procedures, identity and access controls, etc. Answers registered during this assessment must also be physically verified during in-factory inspections.

4. OT security network assessment: This assessment provides clear insight into the active components present within the OT environment. During this assessment, one or more data streams from the OT environment are extracted (in a non-intrusive manner) to identify active assets, the interaction between them and the common protocols used. From this, an interactive topology drawing or network map (Figure 3) is created. Discovered vulnerabilities can be compared to an up-to-date database of known vulnerabilities and flagged for mitigation. The information gathered during this assessment can also be used to build, verify and/or enrich a manufacturer's configuration- or asset management database (CMDB).

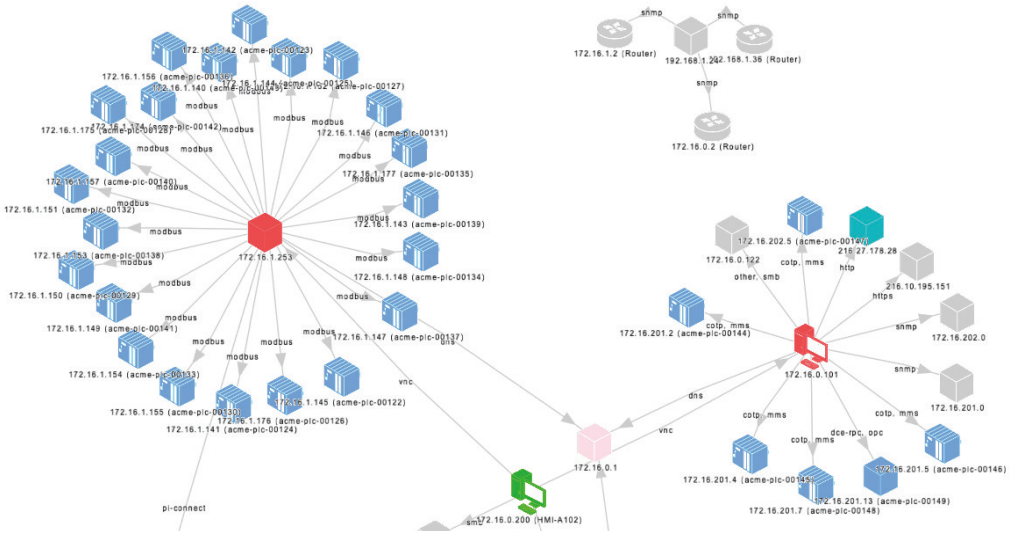


Figure 4: Example of a network map which indicates regular communication based on TCP/IP (blue), common protocols in the OT environment (purple) and potential vulnerabilities (red)

[2] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

5. Risk evaluation and mitigation: Findings from the previous assessments are translated into a risk heat map (Figure 5) that provides a concise, visual representation of potential security risks that threaten the organization's industrial environment. This enables visualization and mapping of identified risks within a risk matrix based on potential impact and probability. At this stage, mitigation measures to reduce the risks to acceptable levels, including prioritization and budgetary indications can be identified.

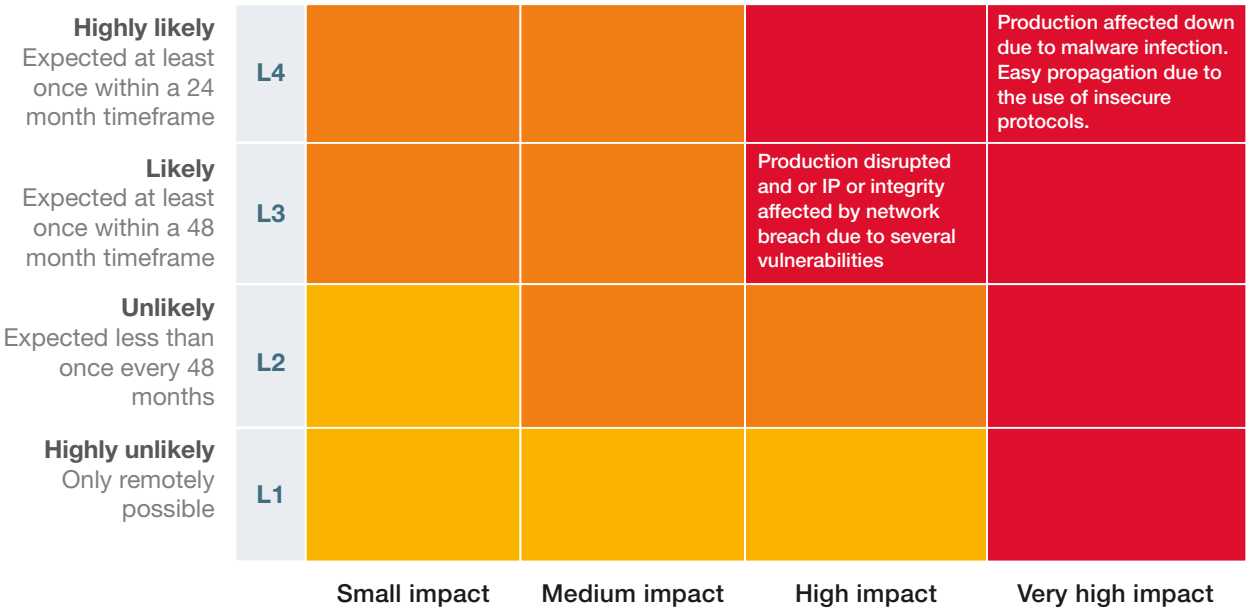


Figure 5: Example of a risk heat map

OT security report

Once the assessment is completed, observations and findings can be summarized in a comprehensive OT security report that states risk exposures and defines baselines along with clear guidance on the "how-tos" to improve security at the plant locations.

Common findings

The diagram below illustrates commonly identified vulnerabilities that require mitigation actions to reduce business risks. These findings are based on numerous CGI assessments of various OT environments in the manufacturing, oil and gas, utilities and food industries.

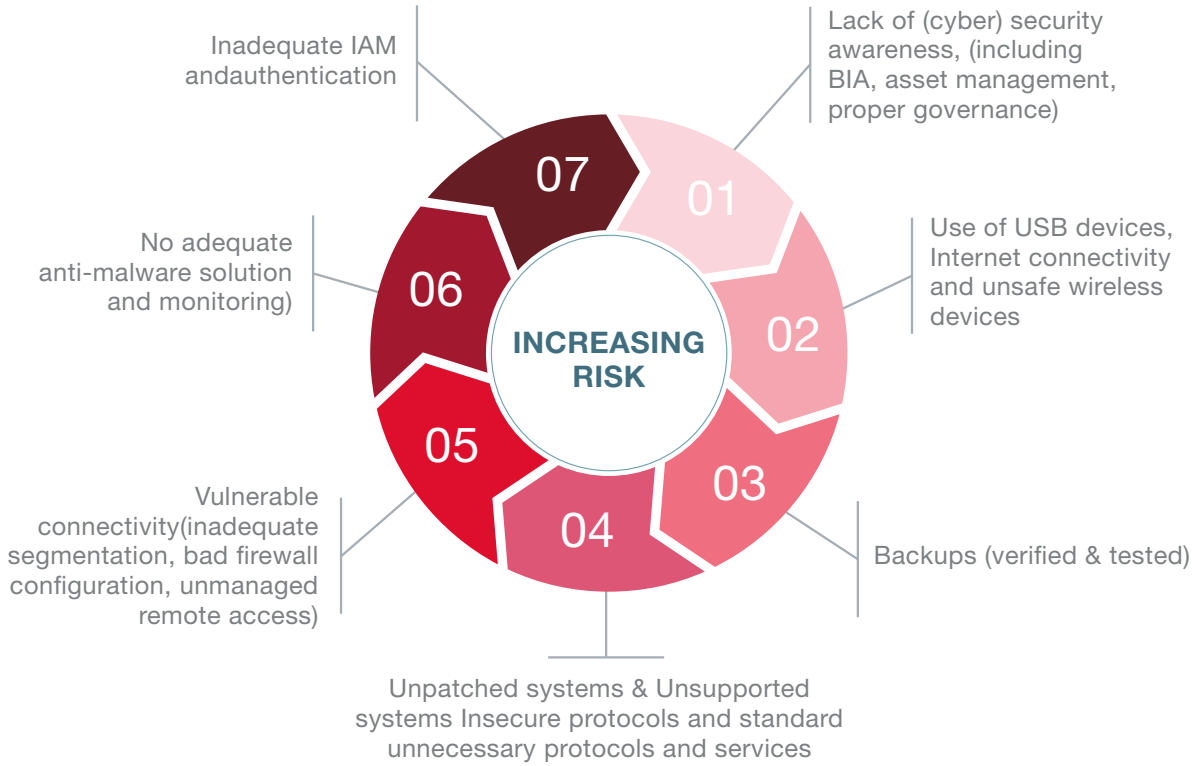


Figure 6: Commonly identified vulnerabilities

The numbers do not represent a ranking, however, we see the lack of cybersecurity awareness and governance in OT environments to be the highest priority as they are the biggest drivers of increasing risk. From our assessments in 2019, the most significant causes for loss/impairment of systems availability affecting either production capacity or integrity that emerged were:

- **Malware infections** – Industry 4.0 in combination with one or more of the above vulnerabilities and multiple attack methods form a perfect storm and since 2015 has led to the exponential growth of successful malware attacks on OT environments.
- **Remote targeted attacks** – Increased connectivity in combination with the use of malware and/or vulnerabilities mentioned in the diagram enable cyber criminals to gain unauthorized and unmonitored access to factories and plants.

Part 2: SECURE

Mitigating identified security risks to people, processes and technology

Based on the risks identified in the OT assessment, the next step is to adopt adequate security measures to protect the industrial environment. To do so correctly, publicly available security standards, guidelines and frameworks such as IEC 62443, ISO 27001 and 27002, NIST Special Publication 800-82 and the NIST Framework for Improving Critical Infrastructure Cybersecurity should be applied. These frameworks offer best practices in key areas such as computer system hardening, zones, conduits and access control.

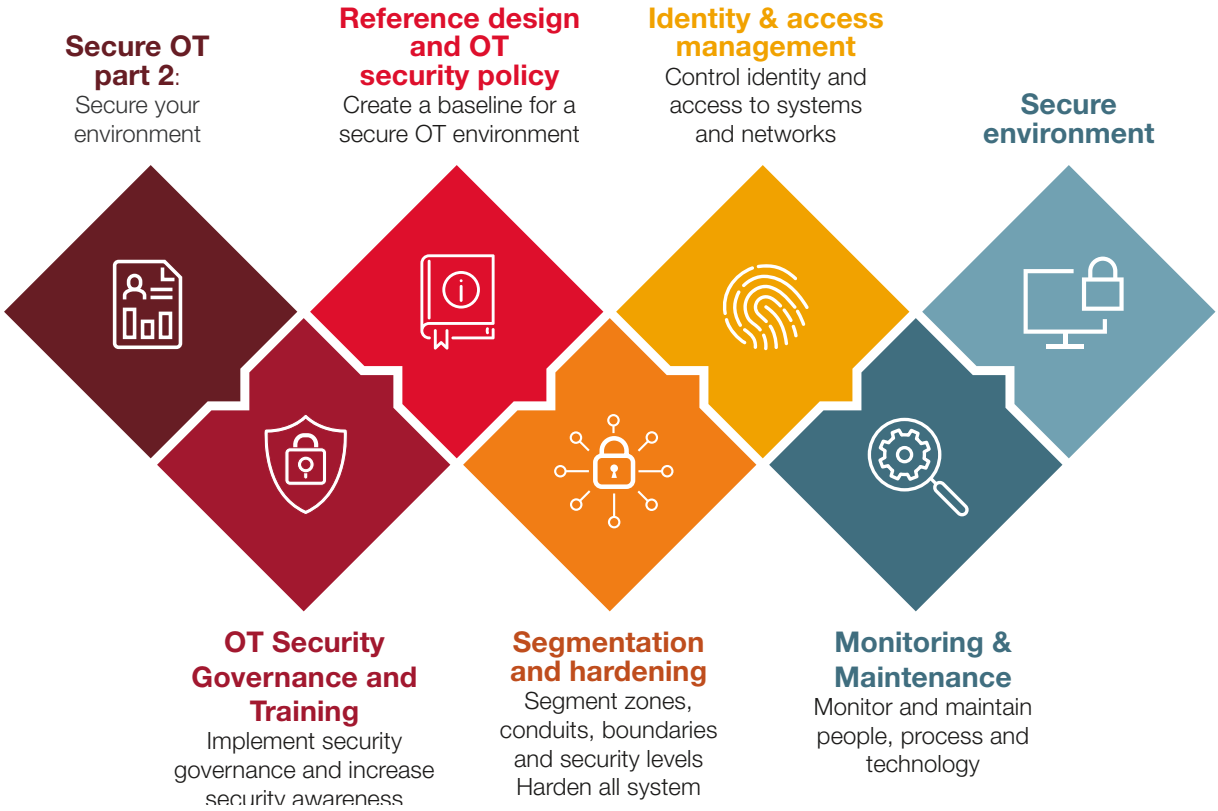


Figure 7: Five steps to mitigate security risks to people, processes and technology

[3] CGI also closely monitors new OT Security initiatives such as NAMUR Open Architecture (NOA) and Open Process Automation Forum (OPAF) and will adapt new standards if applicable into the CGI OT Security methodology.

1. OT Security Governance and Training

- **Make a clear distinction between IT security and OT security, while keeping safety paramount**
  Trying to enforce IT security guidelines in OT environments is not viable as the manner in which measures and controls are implemented and the nomenclature used is different for the two environments. In addition, the IT security priorities of confidentiality, integrity and availability are in fact, inverted in the OT environment. Here's why. In manufacturing, while the process itself is of course a trade secret, the safety of the plant is of higher importance. If IT security is applied to the OT environment, accidents and safety issues can occur. For example, an IT-driven decision may require a door to be kept closed for confidentiality purposes, but an OT-driven decision requires the door is left open so people can flee in an emergency.

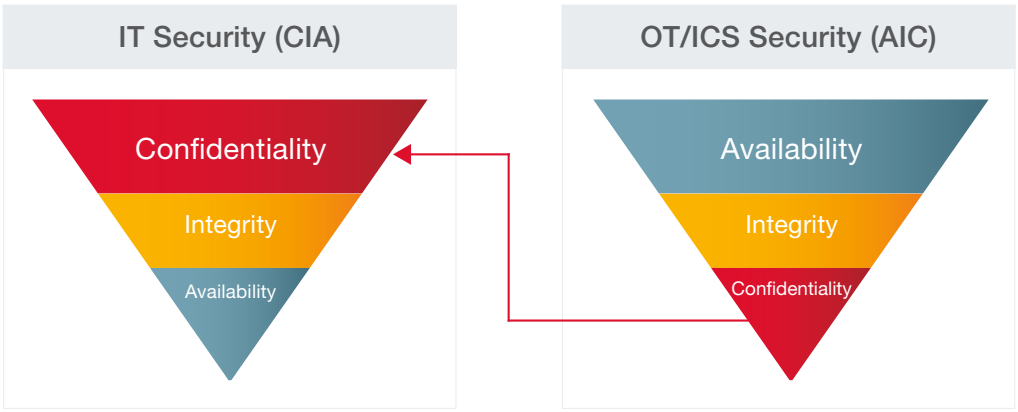


Figure 8: IT security priorities are inverted in an OT environment

Another reason the priorities are reversed is because OT confidentiality could likely be completely covered in the IT environment. Understanding these principles and the difference in IT and OT cultures is key to improving and optimizing the security of both environments.

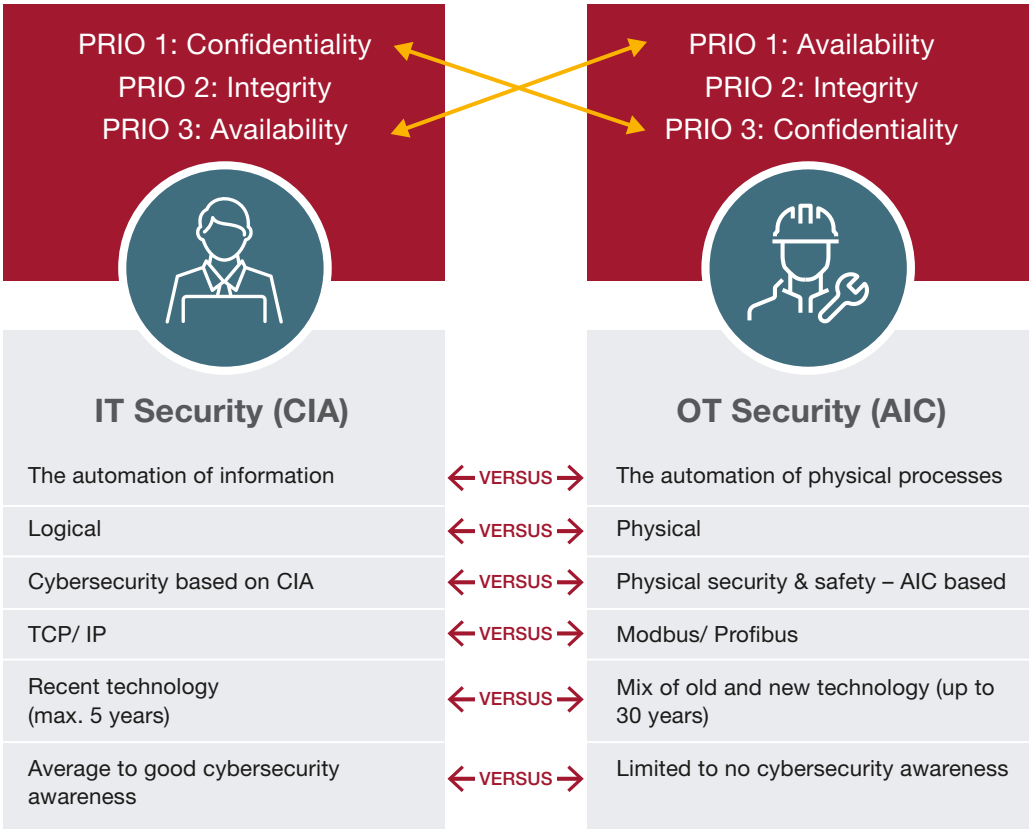


Figure 9: Key differences between IT and OT

Identify who is responsible for security: In most organizations, cybersecurity is the responsibility of the Chief Information Security Officer (CISO). However, the scope of this role often ends where physical production begins, i.e., from enterprise IT up to and including the firewalls that surround OT. However, within the OT environment, physical security is the responsibility of the safety & health manager or the plant manager, and often does not cover the logical or cybersecurity aspects, leaving the automation of physical processes unguarded from cyber threats. To help improve governance, we recommend appointing a Chief Operational Security Officer (COSO), responsible for OT security on an interim basis until these responsibilities can be adopted either by the CISO (preferred), plant or safety manager.

Educate employees on cybersecurity: Every employee authorized to (remotely) access OT and IT data and/or to use field devices must receive appropriate security trainings to lower the risk of internal breaches. Without the right training, employees may not fully comprehend the consequences of say, using a USB storage device, adding a new Wi-Fi printer or creating a link from one system to another to obtain a seemingly non-critical piece of data for reporting. OT security must be integrated into existing safety programs to protect against a breach that could potentially have a safety impact. For instance, a USB device carried by an employee could be accessed to trip the plant or throw off utility systems by introducing malware.

In addition, it is very important to improve awareness among both management and employees about the threats to OT security and the risks of making unsecured connections between OT and the enterprise network. While it can be a challenge to keep security top of mind for executives and employees, senior IT leaders can play a key role in socializing this topic through information sharing and ongoing training programs across all levels of the organization.

Another important aspect to keep in mind is that training is essential, but it is only effective if aligned to the trainee's basic knowledge level and the facilities available. A "one size fits all" program will not work. For instance, employees that perform a daily OT security role will benefit from the Global Industrial Cyber Security Professional (GICSP) training, while a standard ICS security SANS training is more suitable for upper level management. For factory workers, providing video-based trainings developed within their own factory environment will make the information more relatable.

Develop a culture of vigilance: Nobody is better placed to disrupt a plant than someone within the plant itself. In fact, most security breaches come from inside an organization. Employees who work onsite are the most important factor to consider when stepping up security measures. Vetting all employees, contractors and externally employed staff and actively controlling their access to sensitive information and systems can help to close any gaps in security. Guests also need to be closely monitored. Strict identity and access management protocols should be in place to ensure employees can only access the information and physical sites required to carry out their duties. Organizations should embed and encourage a culture of security. For example, if an employee is found accessing a control system he or she would normally not access, it should be acceptable to question the employee's motives.

2. Reference design and security policy: IT security policies cannot arbitrarily be applied within OT environments. Within OT, there are different security requirements for networked assets and plant personnel that call for dedicated OT security policies such as those related to access management, physical and environmental security, hardening, patching, backups, etc. For example, in most cases, patching procedures within an OT environment strongly diverge from IT patching practices. Since availability in OT environments is a top priority, very limited patching and rebooting of assets can be performed and only at pre-defined timeslots.

Manufacturers with multiple factories often face challenges implementing such policies at their various site locations. Different production processes, network infrastructure, vendors and local solutions make factories that seem outwardly similar, differ greatly. Developing a reference design that describes the desired OT environment, including (security) solutions that individual factories can adopt, will ultimately lead to an unambiguous industrial landscape.

3. Segmentation and hardening: To guarantee security, manufacturers need to ensure there is sufficient segmentation and segregation between assets and non-authorized users as per industry standards/Purdue model (Figure 9). It is important to group assets that have a common set of security requirements, both physically and logically. It is equally important to control communication and interconnections between these zones, using conduits that determine the information flow that is allowed between the zones.

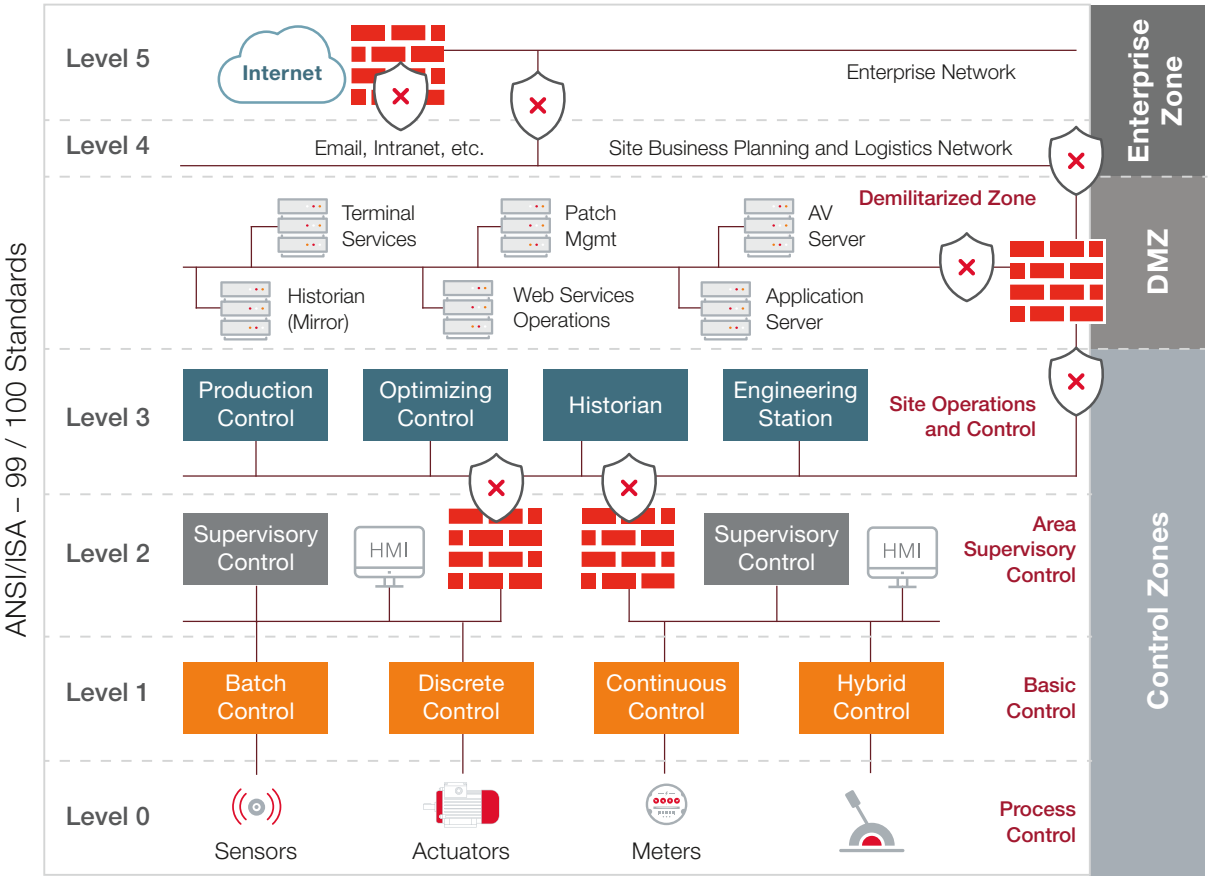


Figure 10: Key differences between IT and OT

Zones can be defined in terms of "enterprise zones" and "control zones." In the **enterprise zone**, a distinction can be made between the internet, that connects manufacturers to the outside world and the enterprise intranet. The creation of a **demilitarized zone (DMZ)** secures the control zone from interaction, exploitation and access by users in the enterprise zone. In the **control zones** a distinction should be made between:

- **Operations control zones**, containing MES, historians and engineering workstations (EWS)
- **Supervisory control zones**, containing HMIs, SCADA systems and DCSs used by operators to interact with remote terminal units (RTUs), intelligent electronic devices (IEDs) and programmable logic controllers (PLCs)
- **Basic control zones**, containing control devices such as PLCs to open valves, move actuators, start motors, etc.
- **Safety zones**, containing safety instrumented systems (SIS) intended to detect a potentially hazardous state of operation and place the system in a safe state
- **Process control zones**, containing sensors, actuators and controllers to manage a physical or chemical manufacturing process

It is advisable to create a separate secured wireless network for IoT devices belonging to the production environment and to keep personal IoT devices like mobile phones and wearables out of the workplace or at least limited to a guest network. Each of these zones should have their specific security requirements and well-defined conduits.

4. Identity and access management: Secure access procedures must control any flow of information, whether automated or manual. For example, when maintenance is carried out, there should be an agreed timeline to access OT systems and corresponding connections should be automatically terminated at the agreed time. This prevents a situation where a maintenance worker may open access to sensitive information by failing to reset a system correctly.

5. Monitoring and maintenance: The result of the previous risk remediation recommendations should be followed up by monitoring, which provides essential input and insight for the proper maintenance of the OT environment. The 'next section of this paper describes how effective monitoring can be achieved.

Tips for hardening your systems and endpoint devices

Manufacturers should deploy only secure, hardened, devices, systems and applications. This begins with choosing device manufacturers and software developers that can demonstrate the implementation of secure coding practices throughout the hardware and software development life cycles.
In general, IT professionals are concerned with the security of and access to IT endpoints devices (internet protocol-based desktops, laptops, mobile devices, database-, application- and web-servers), which can easily be updated automatically as they are connected to the internet and intranet.
On the other hand, OT professionals, in general, are less concerned about the security and access to OT endpoint devices. Most believe these systems are less vulnerable since they are not connected to the internet and the enterprise network, and have specialized environments, protocols, communication channels and proprietary hardware. OT endpoint devices that are purposely separated from the internet and intranet are also not automatically updated.

Considering the need for hardening both systems and endpoint devices, it is critical to protect ICSs at the host level, application level, operating system level, user level, and physical level. A non-exhaustive list of measures that can be taken to harden systems include:

- Installing firewalls
- Keeping security patches and hot fixes up to date
- Closing ports that are not necessary for the functioning of the system
- Installing intrusion detection systems to detect spyware and malware
- Removing unnecessary programs and user accounts
- Using encryption where possible
- Using access and identity management (both physical and digital)

Part 3: MONITOR

Effectively monitoring the industrial environment, assets and connections

Enable continuous monitoring: Staying vigilant to possible threats requires continuous monitoring of systems, networks, devices, personnel, and the environment. Both OT and IT systems must be monitored based on parameters that are considered 'normal network behavior.' If these parameters are exceeded—even slightly—they must be investigated. OT monitoring solutions identify anomalies that stray from everyday behavior and send an alert to be actioned. For instance, if a remote terminal suddenly begins communicating with a device at a different substation, or the level of data generated by an electronic device suddenly peaks, this should raise questions like, "has this situation arisen because someone has hacked into the system or is there a fault in the OT environment?" Some ways to enable continuous monitoring include:

A. Applying security information and event management (SIEM) systems and services to monitor both the enterprise network and the control networks (including the wireless networks). They support:
    - Threat detection and security incident response through real-time collection and historical analysis of security events
    - Compliance reporting
    - Incident investigation through historical data analysis
B. Making use of a dedicated Security Operations Center (SOC) for cost-effective access to the above services and advanced levels of protection on a scalable platform to quickly adapt to business and risk environment demands, and achieve and maintain compliance
C. Using OT security monitoring platforms to perform continuous monitoring and detection across the entire attack surface
D. Applying artificial intelligence (AI) to detect security and operational threats

Create redundancy: Manufacturers are faced with unique security challenges. Unlike an IT environment, it simply is not possible to shut down OT systems for maintenance, software updates or patches. Production flow cannot be interrupted and therefore it is necessary to find a solution that contains the threat and holds it at bay until more comprehensive action can be taken. This can be achieved by designing systems keeping redundancy in mind, where each critical component has a redundant counterpart that can be taken off-line for updates, without impacting the production process. Another way is by swapping between redundant networks to keep the production flowing while devices are patched, and then swapping back afterwards.

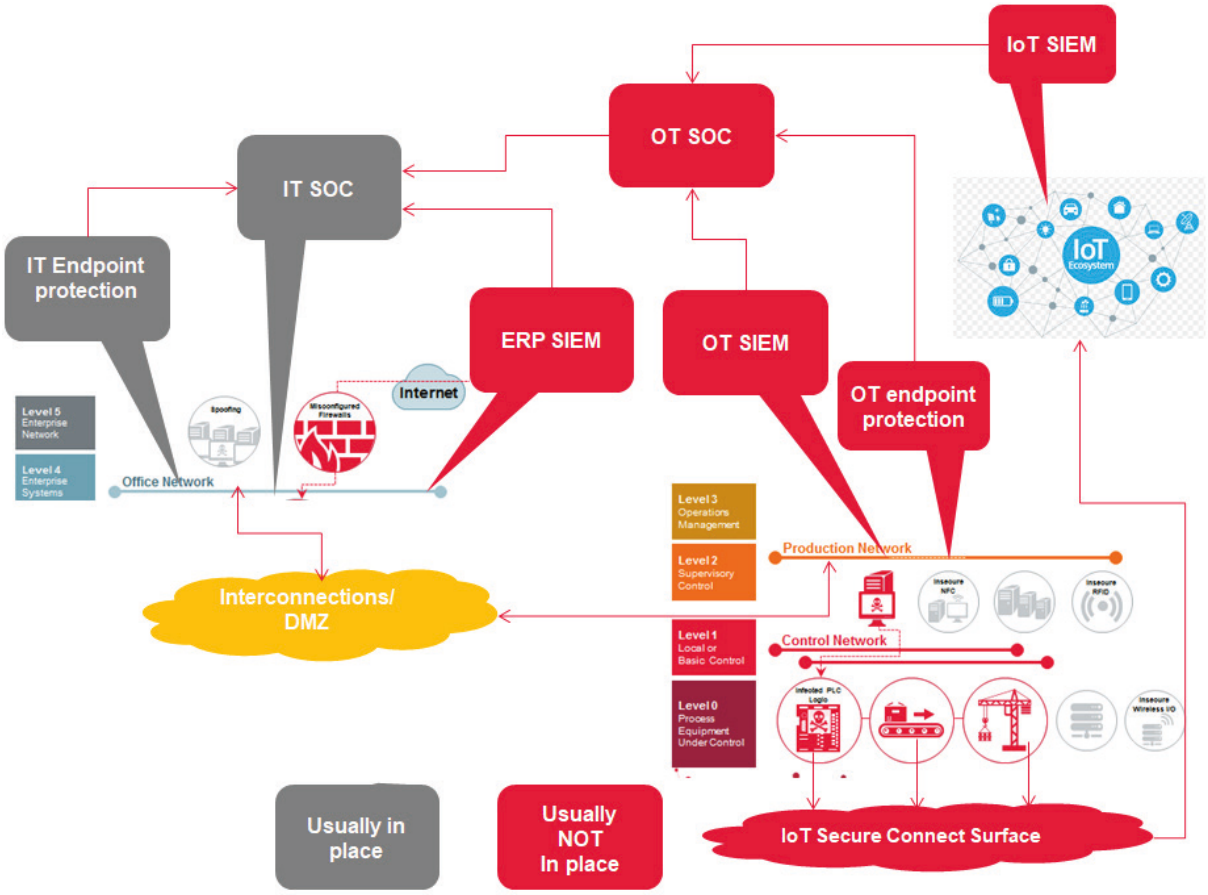


Figure 11: An integrated Security Operations Center (SOC); security measures marked in red are often not in place for manufacturers

Be resilient

In a constantly shifting risk landscape, incidents do happen. What matters is that for each system, there is an appropriate recovery process in place, one that takes into account the system's criticality, maximum acceptable recovery time and recovery method. This requires asking some key questions including:

- Do we take regular backups of our systems and data?
- Do we have a disaster recovery plan?
- How long would it take to recover from an incident?
- How quickly can we remediate the effects of an incident?

Conclusion

Staying vigilant and resilient

In the past, manufacturers viewed cybersecurity as a separate endeavor. Today, we see enterprises increasingly viewing it as an integrated activity as they implement and operationalize more digital transformation strategies, including adopting Industry 4.0. In this era, only a holistic approach across people, process, technology and governance can provide the best defense against the increasing speed and array of cyber threats. To stay ahead of cyber crime, manufacturers need to stay vigilant and be resilient. Assessing, securing and monitoring OT systems on a regular basis is key to adequately protecting against today's—and tomorrow's risks and staying in business.

How CGI can help

CGI has been a trusted adviser for years to global leaders, including the world's top automotive, mining and metal, chemical, high tech and aerospace manufacturers. Our comprehensive and integrated IT and OT cybersecurity solutions and services protect the digital enterprise and secure the digital continuum across the value chain. In the past 15 years, CGI has developed and delivered OT-specific solutions to help manufacturing executives and plant managers address challenges in safeguarding the production process and workers from cyber threats.

In this whitepaper, we have shared CGI's methodology for assessing and securing the OT environment, covering our best practices and experience in the field. We invite you to get in touch with us if you would like to:

- Conduct a comprehensive assessment to identify and qualify the current state of the operational environment, the organization, business risk assessment and prioritization,
- Validate and enhance your cybersecurity strategy for the OT domain, based on industry-standard and CGI best practices, and/or
- Improve and run your security services, monitor your networks and assets, detect, hunt and respond to cyber threats using specialized OT SOCs

Cybersecurity is part of everything we do

CGI has a 40+-year heritage of creating and securing critical business systems in complex environments across the globe, including the defense and intelligence sectors. We have invested heavily in establishing our credentials, working closely with international security associations and standards bodies. While cyber threats are global, we know that requirements vary locally and challenges are unique to each organization. Through our expert talent, deep technical and business knowledge, security operations centers, best practices and frameworks, we work to ensure security is "baked in, not bolted on". As such, enterprises look specifically to CGI to help identify security risks, build secure outcomes, and continue to operate with confidence.

Keywords and definitions

One of the challenges of writing—and reading—about cybersecurity is that there is a world full of jargon, acronyms and technical terms. Below we share a brief glossary.

Artificial Intelligence	**AI**	Artificial intelligence is an area of computer science that aims to create intelligent machines
Attack Surface Reduction	**ASR**	attack surface is the totality of all vulnerabilities in connected hardware and software that are accessible to unauthenticated users. The attack surface can be reduced by closing unnecessary ports and limiting resources available to untrusted users and the Internet
Demilitarized Zone	**DMZ**	is a secure network or path between an organization's internal network and the external network. A DMZ is primarily implemented to secure an internal network from interaction with and exploitation and access by external networks
Distributed Control System	**DCS**	is a computerised control system for a process or plant usually with a large number of control loops, in which autonomous controllers are distributed throughout the system, with central operator supervisory control
Endpoint Device		"Typical IT endpoint devices are desktop or laptop computers, portable devices like tablets and smart phones, database-, application- and web-servers connected to the internet and intranet. Typical OT endpoint devices are application servers, database servers, manufacturing systems, Human Machine Interfaces, workstations and control systems"
Enterprise Resource Planning	**ERP**	is a process by which a company manages and integrates business processes.C23 An ERP management information system integrates areas such as planning, purchasing, inventory, sales, marketing, finance and human resource management
Hardening		The practice of making a system more secure. It includes removing or disabling unused protocols and services, changing defaults, keeping systems up to date, enabling firewalls, and using Anti Virus software.
Human Machine Interface	**HMI**	is a software application that presents information to an operator about the state of a process, and to implement the operators control instructions. Typically information is displayed in a graphic format. An HMI is often a part of a SCADA system
Identity and Access Management	**IAM**	"is the security discipline, framework of policies and technologies that enables the right individuals to access the right resources at the right times for the right reasons for ensuring the proper people in an enterprise have the appropriate access to IT resources"
Industrial Control System	**ICS**	is a general term that encompasses several types of control systems and instrumentation used for industrial process control. refers to level 1, 2 and 3 of the purdue model
Industry 4.0	**I4.0**	The fourth industrial revolution
Information Technology	**IT**	the use of computers in the context of an enterprise (levels 4 and 5 of the Purdue Model)

Keywords and definitions

Intelligent Electronic Devices	**IED**	is a microprocessor-based controller of power system equipment, such as circuit breakers, transformers and capacitor banks.
Internet of Things	**IoT**	is a term for hardware pieces (sensors, devices and machines) that work together through internet of things connectivity to help enhance manufacturing and industrial processes.
Internet Protocol	**IP**	is the communications protocol defining the digital message formats and rules for exchanging messages between computers across a network using the Internet Protocol Suite
Intrusion Detection System	**IDS**	is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks.
Manufacturing Executions System	**MES**	is a is an information system that connects, monitors and controls manufacturing processes and data flows on the factory floor in real time. The main goal of an MES is to ensure effective execution of the manufacturing operations and improve production output.
Operation Technology	**OT**	the use of computers in production (level 1, 2 and 3 of the Purdue Model) The term OT has been introduced to make a difference between the IT office environment and the Industrial Control Systems production environment
Programmable Logic Controllers	**PLC**	is a ruggedized computer used to automate a specific process, machine function, or production line. They are specially designed to survive in harsh situations and shielded from heat, cold, dust, and moisture.
Purdue Model		a reference architecture for Industrial Control Systems
Remote Terminal Unit	**RTU**	monitors the field parameters and transmits data the distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems.
Security Information and Event Management	**SIEM**	is an approach that combines security information management and security event management functions into one security management system. SIEM systems are used for centralized data collection and analysis of data, from various systems and devices on a network, identify deviations from the norm, detect threats and take appropriate action such as investigation, containment, mitigation, or remediation.
Security Operations Center	**SOC**	a centralized facility that houses an information security team dedicated to and organized to prevent, detect, assess and respond to cybersecurity threats and incidents, and to fulfill and assess regulatory compliance
Supervisory Control and Data Acquistion	**SCADA**	is an industrial control system at the core of many industries such as manufacturing, energy, water, and power production ad distribution

Your contacts for next steps

This white paper has been developed by Hans van Veen, Lucien Sikkens, Tom van Boheemen and Michiel Tenge. A team of senior CGI experts with more than 25 years of experience in the manufacturing, oil and gas, and utilities industries, advising leading organizations on their transformation and supporting complex transformations. In this paper, they share their deep understanding of manufacturing organizations' processes as well as their expertise and knowledge in the latest technologies, software and methodologies for the digital century.

For more information or next steps, please contact:

Luciën Sikkens
Director OT Security

Luciën is responsible for CGI's OT security services and solutions and client engagements in this area. He has over 20 years of experience in both the physical and logical security of IT and OT environments. Luciën comes from a business background and firmly believes in the principles of securely facilitating businesses, putting the business first and delivering fitting solutions to secure and enable business outcomes.

Tom van Boheemen
OT Security Consultant

Tom helps clients across different sectors identify security risks within the OT environment and mitigate these risks by implementing and optimizing various security controls. As a criminologist, Tom recognizes the importance of evolving behavior within the security landscape and understands how to translate complex security threats to clients.

Michiel Tenge

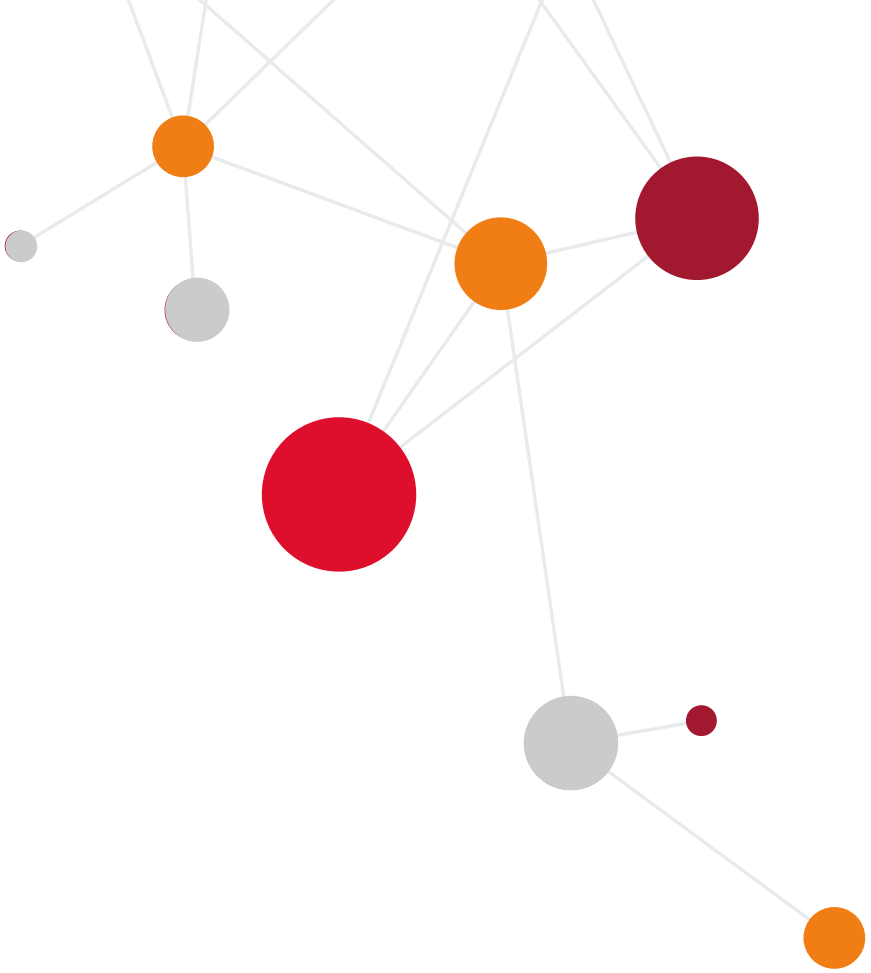
Director Consulting

Michiel is a cybersecurity expert with over 21 years of consultancy experience in Information Risk Management with a focus on design, implementation and cost-effectiveness of security and regulatory compliance. Michiel offers broad technical insight, drives results and excels in building relationships across the client's organization, from the operational and tactical to strategic levels.

Willem Jan de Graaff

Director Consulting Services

Willem Jan is as Director Consulting Services responsible for CGI's OT security business and client engagements in the Netherlands. He has over 25 years' of extensive experience in the Oil & Gas, Utilities and Manufacturing industries. Willem Jan and his team of OT security experts have worked with a range of customers on developing security frameworks, performing plant assessments and remediating the identified organizational, network and asset security risks. Willem Jan in his career, has successfully completed many complex transformation programs in the infrastructure and application domain for multinational customers in the US, Europe and Asia.



CGI

About CGI

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI delivers an end-to-end portfolio of capabilities, from strategic IT and business consulting to systems integration, managed IT and business process services and intellectual property solutions. CGI works with clients through a local relationship model complemented by a global delivery network to help clients achieve their goals, including becoming customer-centric digital enterprises.