SECTRIO

CYBERSECURITY IS A KEY ENABLER OF INDUSTRY 4.0

www.sectrio.com

The ongoing convergence of systems connected with Information Technology and Operational Technology (OT) has given rise to Industry 4.0 and the Industrial Internet of Things (IIoT). Industry 4.0, is transforming traditional manufacturing and allied industries by introducing new capabilities through digitisation, decentralization of decision-making and value chain integration. Industry 4.0 is joined at the hip to cyber-physical systems that are enabling intelligent and connected infrastructures including Smart Manufacturing infrastructures by enhancing their quality of service provisioning.

Industry 4.0 and the exponential growth in the quantity of connected devices it enabled along with the rapidly increasing volume of cyber security incidents stresses the need for strengthening cyber resilience and understanding of complex threats especially among the operators who are just beginning to utilise IoT solutions. Devices connected with Industry 4.0 deployments increase the complexity and vulnerability of industrial control system (ICS) networks that were previously isolated but are now exposed to many of the same cyber security attacks that traditional machines are exposed to.

Recent cyber attacks on Industry 4.0 and Smart Manufacturing are leading to operators paying more attention to aspects related to the security of technical solutions and the safety of employees and other stakeholders who rely on them. This subject is also significant as the potential impact exerted by new threats ranges from compromising physical security to production downtime, spoilage of product, damage to equipment and the ensuing financial and reputational losses.

SECURITY CHALLENGES

The benefits of deploying Industry 4.0 technologies and enabling smart manufacturing do bring significant security challenges. While stakeholders are aware of the problem to some extent, there is still room for awareness and action especially since the threat environment surrounding industry 4.0 deployments continues to turn riskier for businesses and investments.

According to Sectrio's own research, the attacks on devices and networks associated with Industry 4.0 have grown by as much as 23 percent in the period between November 2018 and April 2019. This highlights the gravity of the situation and the need for immediate action. The following are some of the security challenges associated with such deployments:

Components

Industry 4.0 entails use of a diverse family of devices and connectivity flavors. This means ensuring the security of an enormous number of connected assets. Further, IoT security cannot be expected to function in isolation. Instead it draws from and works along with IT security, data security, OT security and physical security as well. Thus, the disciplines involved makes cybersecurity a broader concept. Manufacturing entities need to handle typical vulnerabilities in a multitude of systems. In industrial environments this poses a considerable challenge as most systems of this type were not designed with cybersecurity in mind and thus vulnerabilities in this hardware are becoming more and more common.

Processes

In addition to the large attack surface in terms of connected devices, a multitude of complex processes involved in Smart Manufacturing should also be considered. Management of processes with cybersecurity in mind poses a challenge for Industry 4.0 companies, especially since functionality and production efficiency are usually seen as having a higher priority than cybersecurity.

Increased connectivity

Manufacturing processes need to interact with objects and environments on a global scale and systems used in Smart Manufacturing need to enable collaboration across multiple levels.

IT/OT convergence

Industrial control systems are not isolated islands anymore. Blending with IT network- enabled organisations has simplified the management of complex environments. It has also introduced new security risks and managing IT/OT integration has become a significant challenge. Insecure network connections (internal and external), utilisation of technologies with known vulnerabilities that introduce previously unknown risks into the OT environment, and insufficient understanding of requirements for ICS environments are areas of concern. Holistic security practices must also cover digital twins and actual physical implementation.

Supply chain

Manufacturing companies are rarely able to produce every part of the product in-situ and often rely on third parties' components. Developing sophisticated products leads to an extremely complex supply chain with the involvement of a large number of people and organisations making it highly demanding in terms of management. This also means the addition of a large number of weak points from which an attack could be perpetrated.

Legacy ICS

Legacy hardware is a significant barrier to adoption of the Industrial Internet of Things by over a third of the respondents according to a recent survey. Manufacturers build new systems on top of legacy systems, and this may result in outdated protection measures and contain unknown vulnerabilities that have been inactive for years. Adding new IoT devices to outdated hardware raises concerns that it may allow attackers to find a new way to compromise systems.

Insecure protocols

Manufacturing components communicate over private industrial networks using specific protocols. In modern network environments, these protocols often fail to ensure proper protection against cyber-threats. According to a recent report, 4 of the 5 least secure protocols are ICS specific.

Human factors

Adopting new technologies means that factory workers and engineers have to work with new types of data, networks and systems in novel ways. They are unaware of the risks associated with gathering, handling and analysing that data and can thus become an easy target for attackers. This is becoming all the more disturbing given that the industry most targeted by phishing emails in 2016 was Manufacturing.

Unused functionalities

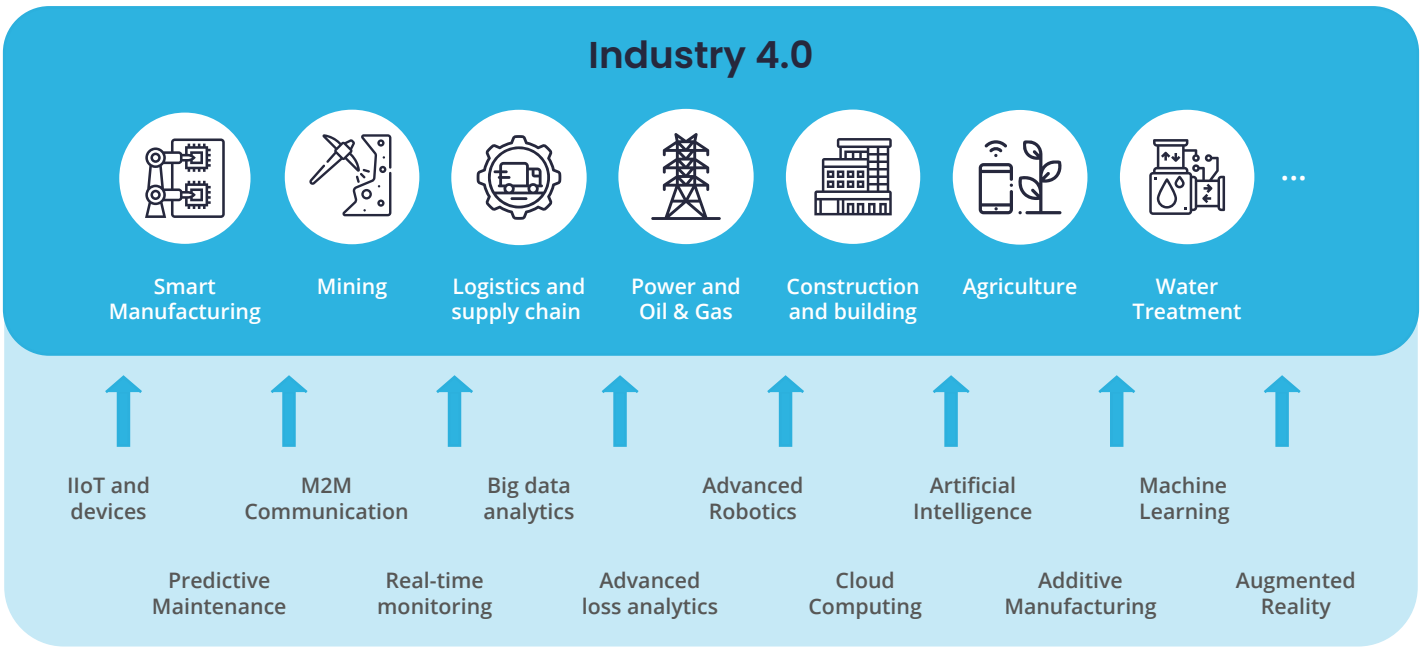
Industrial machines are designed to offer a large number of functions and services, many of which may not be necessary for operation. In industrial environments, machines or their selected components often have access to unused functionalities that may considerably expand the potential attack area and become gateways for the attackers.

Safety aspects

The presence of actuators that act on the physical world makes safety aspects very relevant in IoT and Smart Manufacturing. Security for safety emerges as an objective of paramount importance.

Patches

Applying security patches is an extremely challenging task as the particularity of the user interfaces available to users does not allow traditional update mechanisms. Securing those mechanisms is in itself a daunting task, especially considering Over-The-Air updates. In OT environments in particular, applying updates may be challenging since this operation needs to be scheduled and performed during downtime.



TOP THREATS

Scenario	Probability
Against the connection between the controller (e.g. DCS, PLC) and the actuators	High
Against sensors (modification of measured values/states, their reconfiguration, etc.)	High
Malware	High
Against actuators (suppressing their state, modifying the configuration)	High
Against the information transmitted via the network	Crucial to High
Manipulation of remote controller devices (e.g. operating panels, smartphones)	High
Against IIoT gateways	High
Against the Safety Instrumented Systems (SIS)	Crucial to High
DDoS attack using (IoT) botnets	High
Stepping stones attacks (e.g. against the Cloud)	Medium
Highly personalised attacks using Artificial Intelligence Technologies	Low to Medium
Human error-based and social engineering attacks	High

SECURITY MEASURES

Insecure protocols

Organisation principles and governance are among the most indispensable factors that are usually critical in terms of company security. From incident management to vulnerability management and training and awareness, organisations should have unambiigous policies in place to guide employees and other stakeholders to operate with the highest level of diligence and sensitivity to security needs.

Technical practices

Apart from implementing policies and organisational practices, security also needs to be addressed through the appropriate technical capabilities of IIoT solutions and the environments where they are deployed.

Proactive risk and threat management

Every aspect of operation should be analyzed to determine the risks and those risks should be addressed in a time-bound manner.

Business continuity

Security should be managed from a business continuity perspective as well.

Protect data

Security measures should be in place to protect confidential data.

Software patches

Patching should be done without fail and no unpatched software should be part of the whole eco-system.

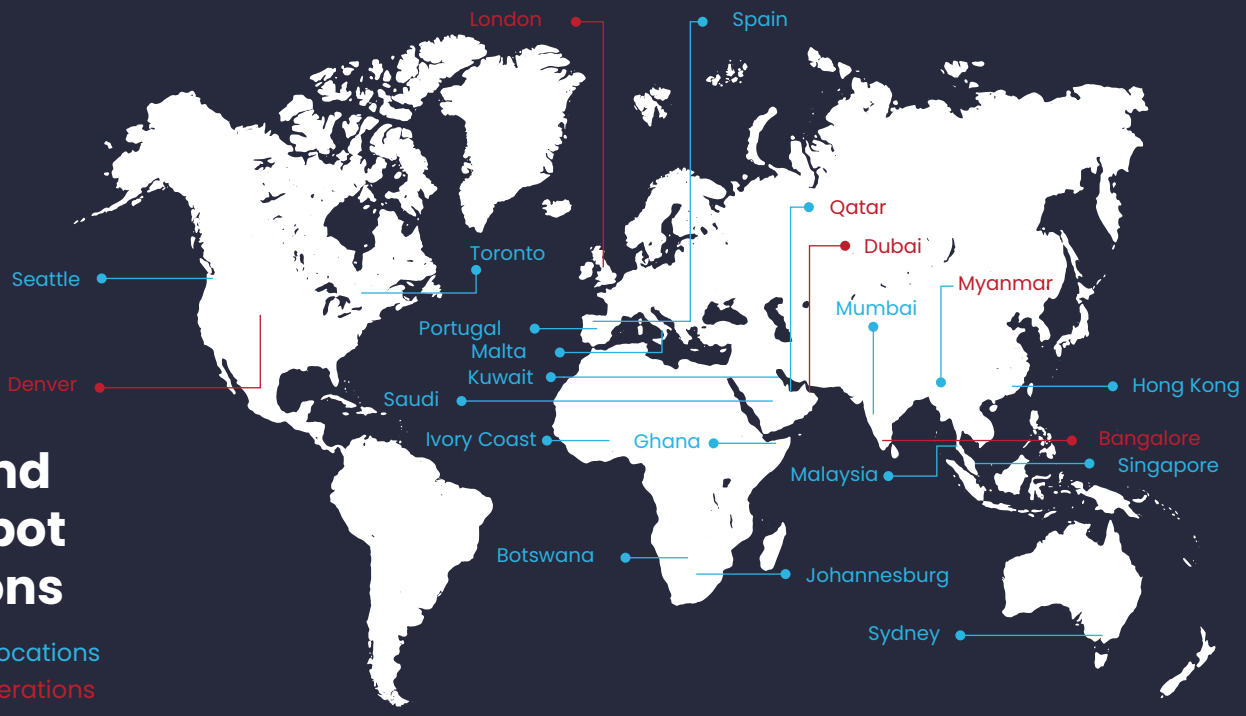
Access control

Security measures should be in place regarding the control of remote access, authentication, privileges, accounts and physical access.

Network, protocols and encryption

Security measures should be evolved to ensure security of communications through proper protocols implementation, encryption and network segmentation.

ABOUT SECTRIO



ISOC and Honeypot Locations

- Honeypot Locations
- Security operations

Sectrio is a division of Subex Digital LLP, a wholly owned subsidiary of Subex Limited. Sectrio is a market and technology leader in the Internet of Things (IoT), Operational Technology (OT) and 5G Cybersecurity segments. We excel in securing the most critical assets, data, networks, supply chains, and device architectures across geographies and scale on a single platform. Sectrio today runs the largest IoT and OT focused threat intelligence gathering facility in the world. To learn more visit: www.sectrio.com

INDIA

Pritech Park-SEZ, Block 9,
4th Floor, B Wing, Survey
No. 51 to 64/4, Outer Ring Road,
Bellandur Village, Varthur Hobli
Bangalore – 560 103

Tel : +91 80 6659 8700
Fax : +91 80 6696 3333

AMERICAS

12303 Airport Way, Bldg.
1, Ste. 180, Broomfield,
CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

EUROPE

1st Floor, Rama Apartment,
17 St Ann's Road, Harrow,
Middlesex, HA1, 1JU

Tel : +44 207 8265300
Fax : +44 207 8265352

REGIONAL - MUMBAI

Level 13, R-Tech Park,
Nirlon Knowledge Park,
Goregaon (East),
Mumbai - 400063
India.

Tel : +91-22-4476 4567

MIDDLE EAST & AFRICA

#Office number 722,
Building number 6WA,
Dubai Airport Free Zone
Authority(DAFZA,Dubai
United Arab Emirates

Tel : +9 714 214 6700
Fax : +9 714 214 6714

ASIA PACIFIC

175A Bencoolen Street
#08-03 Burlington Square
Singapore 189650

Tel : +65 6338 1218
Fax: +65 6338 1216