The increasing need for OT cybersecurity

The growth of operations technology (OT) and its integration with IT in the industrial context is inevitable. This integration brings obvious operational benefits. It also brings new cyber threats. When the historically separated technologies of IT-OT become a single network, a fully integrated security system is essential. This paper explains why – and how it can happen.

Authors:

Samuel Tew,
Senior Manager

Ogulcan Kargul,
Manager

Matheus Bruni,
Senior Associate

Axon Consulting | September 2022 | axonpartnersgroup.com

Contents

Abstract

The growth of operations technology (OT) is unstoppable – and its integration with IT is inevitable.

The benefit this integration brings to companies, customers and societies from an operational point of view is well known. However, it also exposes OT, a previously isolated technology, to new and often unfamiliar cyber-threats.

Historically, the cybersecurity needs of IT and OT systems were dealt with separately. Today, however, they are increasingly seen as one single unit – a unit that needs protection from cyber-attacks through an equally integrated security system.

IT-OT networks are the future. But guaranteeing their stability is essential. Cybersecurity is fundamental to this. The lack of effective security systems could have disastrous consequences – anything from the leak of classified information to physical threats to citizens or workers. And cyber-attacks can come from many sources – internal or external – and in many forms. An effective security system must protect this network from any threat coming from anywhere.

The good news is that there is already some established guidance in the form of international best practices, standards and national-level OT cybersecurity regulations. These can act as a benchmark for cybersecurity assessments of OT networks, even as they continue to evolve.

1. Introduction

IT-based cybersecurity has evolved rapidly, an evolution driven in particular by the increasing exposure of IT assets to a connected world and the need to ensure data privacy across multiple industries.

Connectivity is the key to this. Connectivity plays a major role in areas as diverse as factories, airports, commercial centres and our own homes. It offers major operational benefits.

However, it also means greater convergence of IT and OT systems, which, in turn means that operational technology (OT) systems that were traditionally 'disconnected' are now online. OT is now vulnerable to malicious actors.

Greater convergence of IT and OT systems means that operational technology (OT) systems that were traditionally 'disconnected' are now online. OT is now vulnerable to malicious actors

If this convergence is mismanaged, OT, and the operations it controls, could face serious issues – such as physical damage of hardware, maintenance and recovery costs, leaks of classified information, and even physical danger to workers or citizens.

OT cybersecurity is the key to mitigating this risk. Cyber-attacks can come from many sources – internal or external – and in many forms. An effective security system must protect IT-OT networks from any threat coming from anywhere.

In this paper, we explore the growth of the OT sector and explain how it differs from IT systems. However, although IT and OT are fundamentally different, synergies are created when these two types of networks come together.

This convergence of IT and OT networks enables new technologies such as IoT devices, smart cities, smart grids and smart devices – the main developments driving the new Industry 4.0 movement. These new applications don't just have operational benefits – they also have environmental ones.

However, as we explain, they also increase the vulnerability of OT systems to cyber-attacks. We therefore examine cyber threats – both internal and external – to OT systems, especially in the light of the changing relationship between OT and IT.

IT-OT networks have until recently been separated. We highlight the need for a fully integrated security system to protect the single OT-IT unit.

Fortunately, measures do exist to minimise cyber-threats to OT networks – and they can be adapted to the changing OT-IT landscape. They include international best practices, standards, and national OT cybersecurity regulations.

These standards and regulations can be used as reference tools by anyone carrying out a cybersecurity assessment of OT networks. We introduce some of the methodologies that can be followed to perform a comprehensive assessment of OT networks, highlighting some of the international best practices and regulations currently available.

Measures do exist to minimise cyber-threats to OT networks – and they can be adapted to the changing OT-IT landscape

2. What is OT and how is it different from IT?

2.1. OT in a nutshell

Operational technology (OT) is the monitoring and controlling of physical devices, processes, and infrastructure using specialised hardware and software. Examples of operational technology deployments include the technology that moves an assembly robot in an automotive factory line, or an industrial control system driving production machines. However, OT also has applications in residential or commercial applications such as a fire management system protecting a building.

Rapid industrial growth and government support have meant that the OT market has been expanding over the past decade. According to a recent report[1], the global OT market was worth an estimated 157.9 USD billion in 2022. It is expected to reach 216.3 USD billion in 2027. That's a compound annual growth rate (CAGR) of 6.5% within the forecast period.

Operational technology (OT) is the monitoring and controlling of physical devices, processes, and infrastructure using specialized hardware and software

Global operational technology market size
2022-2027, USD Billion

Exhibit 2.1: Global Operational Technology Market Size, 2021
[Source: Axon Consulting, based on MarketsandMarkets[1]]

The global operational technology market was estimated at 157.9 USD billion in 2022 and is expected to reach 216.3 USD billion in 2027

1 Markets and Markets, 2021; Available at: https://www.marketsandmarkets.com/Market-Reports/operational-technology-market-175373380.html

Among the reasons for this growth is the need for industries and companies to adapt to an ever-growing demand for products and services. As competition among players intensifies and customer requirements for quantity and quality become more demanding, many companies have invested in OT across their facilities to speed up tasks and create a competitive advantage.

2.2. IT – and how it differs from OT

Information technology (IT) is about storing, transmitting, manipulating and managing data generated through an organisation via data centres and cloud infrastructure. This could involve multiple forms of hardware (such as computers, physical servers and network equipment) and software (such as applications and operating systems). Whether we pay bills with our debit/credit cards when shopping, watch a movie from a digital broadcaster, or arrange an appointment at a doctor's office, there is always an IT system running in parallel. In fact, IT services have been part of our daily lives since the introduction of the term in an article by Harvard Business Review in the mid-20th century.

At the same time, with the introduction of Industry 4.0, OT services have enjoyed global growth. The Industry 4.0 movement has seen organisations invest in new OT and IT technologies to optimise operational processes and create competitive advantage. Monitoring machinery and streamlining processes are now more vital than ever – which is where OT comes in.

As networking, cloud and cybersecurity company Cisco[2] points out, even though OT and IT network infrastructure have similar elements like switches, routers, and wireless technology, there are several distinctions between them. For example:

- **Form factor:** OT devices are in smaller and modularized form factors in order to embed them easily into various places, such as rails, walls, light poles and cars
- **Hardening:** OT network infrastructure is more robust as it needs be resistant to severe industrial conditions
- **Network interfaces:** OT network devices may support a variety of networks, such as LoraWAN, to connect IoT devices

Though OT and IT network infrastructure have similar elements like switches, routers, and wireless technology, there are several distinctions between them

The Industry 4.0 movement has seen organisations invest in new OT and IT technologies to optimise their operational processes and create competitive advantage

While OT and IT are fundamentally different, there are strong synergies driving their convergence

2 Cisco, 2022; Available at: https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html#~q-a

- **Protocols:** OT network devices have different communication protocols such as Modbus, Profinet, and Common Industrial Protocol (CIP). This is not the case for traditional IT devices

In short, from an organisational point of view, IT services are leveraged for the daily data and information flow. OT services monitor the backend, – the production side.

2.3. OT-IT convergence

While OT and IT are fundamentally different, there are strong synergies driving their convergence. For example, in Industrial IoT some organisations have started to integrate their OT and IT systems to have seamless production lines and continuous monitoring. In fact, the convergence of IT and OT is fundamental to Industry 4.0.

The idea is to bring the physical equipment from OT services into the digital world provided by IT services to increase efficiency and competitive advantage. Several companies are already replacing their OT monitoring and control systems with IoT alternatives. According to a survey of more than 400 global manufacturing companies conducted by McKinsey in 2021, 94% of the respondents indicated that they are running operations using Industry 4.0 solutions; 56% claimed that these solutions are critical for their organisation[3].

Depending on an organisation's needs and requirements, IT-OT convergence can be seen in process convergence, software convergence, and physical convergence. In the transportation industry, for example, organisations deploy the necessary hardware on the OT side and integrate it with a digital system that allows the collection, transfer and analysis of data (the IT side). In this way, organisations benefit from optimised routes and reduction in fuel cost, staff cost or other costs.

Depending on an organisation's needs and requirements, IT-OT convergence can be seen in process convergence, software convergence, and physical convergence

3 McKinsey & Company, 2021; Available at: https://www.mckinsey.com/business-functions/operations/our-insights/operations-blog/industry-40-adoption-with-the-right-focus

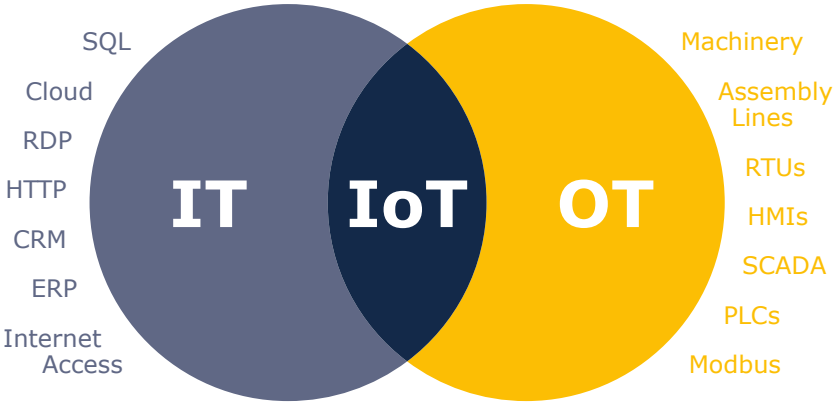

Exhibit 2.2: Illustration of IT-OT Convergence, 2021, [Source: Axon Consulting, based on TANAND TECHNOLOGY[4]]

But IT-OT convergence is not limited to new IoT devices. Many IoT applications are coming together to create solutions that once seemed futuristic: think of smart cities, smart factories, smart grids, and smart agriculture. In fact, today, any OT hardware can be converted into a 'smart' device thanks to developments in internet connectivity, artificial intelligence and machine learning. Combining several of these 'smart' devices can lead to entirely automated environments that may one day become the norm. These applications, which are driving the Industry 4.0 movement, bring benefits not only in terms of efficiency but in terms of reduced energy consumption.

Today, any OT hardware can be converted into a 'smart' device thanks to developments in artificial intelligence and machine learning

4 TANAND TECHNOLOGY, 2021; Available at: https://www.tanand.com.my/it-ot-convergence-how-does-it-benefits-digital-manufacturing/

5 See case study energy and smart cities across the EU

Case study: energy and smart cities across the EU[6]

The EU is a pioneer in the development of energy-efficient solutions; sustainability is taken very seriously across all member states. A smart city, according to the EU, is a "place that integrates physical, digital and human systems in traditional networks and services to better use energy resources and reduce emissions to the benefit of citizens and businesses".

Smart city applications are connected and automated in order to make efficient use of resources. Electricity grids can detect when energy consumption is higher or lower and automatically adjust production levels to meet demand. Buildings can project room occupancy rates and automatically regulate cooling / heating systems accordingly. Homes can be equipped with integrated renewable sources and energy storage systems able to power all the needs of a common household. Waste disposal facilities can increase recycling efficiency thanks to augmented visual AI technology.

OT is fundamental to the smart cities concept. It is the bridge between sensors and data, revealing changes in the physical environment. OT is already driving several of our day-to-day activities and is a key resource for companies and businesses. In the years to come, traditional 'offline' OT hardware and software will be replaced with 'online' alternatives thanks to the integration of IT and OT: fully automated and functional smart cities will be the result.

In the years to come, traditional offline' OT hardware and software will be replaced with their new 'online' alternatives

5G connectivity allows devices to connect and communicate with previously unheard-of speeds and accuracy; this is fundamental to the creation of fully reliable autonomous environments

The benefits of IT-OT integration become even more noticeable when smart devices are coupled with advanced connectivity. 5G connectivity, for example, allows devices to connect and communicate with previously unheard-of speeds and accuracy; this is fundamental to the creation of fully reliable autonomous environments. 6G connectivity and beyond will further boost the potential of IT-OT solutions.

6 European Commission, 2022; Available at: https://ec.europa.eu/info/news/focus-energy-and-smart-cities-2022-jul-04_en

3. The OT attack surface layer

Which brings us to cybersecurity. As more devices become connected and interconnectivity increases at the facility level, the surface that needs to be protected also grows – and grows significantly. A higher number of connected devices also implies more 'entry points' to OT systems. But many of these systems were not originally designed to cope with sophisticated cyber-attacks.

A higher number of connected devices also implies more 'entry points' to OT systems

The lack of 'cyber-readiness' of OT devices has much to do with the historical development of the embedded systems that underpin their functionality. It also points to another important difference between OT and IT equipment. The latter employ a handful of well-known and compatible OSs, making cybersecurity updates (just like any other software update) much more easily available and simple to install, or develop.

This is not the case for OT devices, which most often run on bespoke, vendor-specified systems that have limited or no accessibility and are therefore often reliant on the manufacturer to update. This can of course raise many problems for the flexibility and speed in applying cybersecurity solutions proactively, let alone recovering from incidents. In addition, the extremely limited overheads inherent in deeply embedded systems – both in terms of the physical space available for security code and its latency implications – make it tough for manufacturers to prioritise security over functionality.

So how can organisations deploying OT services guarantee their security? Take the safe operation of plants and the reliable transmission of data for time-critical applications.[7] Here, OT is subject to several external threats, such as these, highlighted by cyber security and network architecture experts Nomios:[8]

7 Siemens, 2022; Available at: https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-network-solutions/ot-it-networks.html

8 Nomios, 2022; Available at: https://www.nomios.com/news-blog/top-five-ot-security-threats/

- **Malware infiltration via external hardware and removable media** Executable files and applications could contain malicious code that may result in data leakage and malware infection. An infected computer could quickly infect systems and components from within the same network
- **Malware infection via Internet and Intranet** Enterprise networks are often infected by web servers and databases. Online vulnerabilities are found and then used to deploy malware to gather unauthorised information
- **Compromising cloud components** OT cloud cybersecurity threats include disrupted communication between local OT and outsourced (cloud) components due to distributed denial of service (DDoS) attacks

Threats are not just external. Devices are often 'online' and sometimes they connect with other devices by accident. This can create problems at the operation level. Human error – from internal employees and external personnel – is another threat: systems may be compromised by unauthorised or incorrectly configured software and hardware. Thus, the system needs to be protected from intentional external threats, but it also needs to avoid accidental interconnections within the operation.

Moreover, the need for more OT security solutions is a consequence of IT-OT convergence (as we noted in 2.3). This transformation from a closed to an open system is leading to new cybersecurity risks such as DDoS attacks and IoT-botnets.

With a wide range of IoT devices using several communication protocols (such as Wi-Fi, cellular or near field communication), security systems become increasingly more vulnerable; each type of technology has its own security challenges. Mitigating large traffic volumes using DDoS protection solutions will be a priority in reducing the impact of cyber-attacks in years to come.

Devices are often 'online' and sometimes they connect with other devices by accident. This can create problems at the operation level

This transformation from a closed to an open system is leading to new cybersecurity risks such as DDoS attacks and IoT-botnets

Historically, IT and OT systems have been monitored separately even though they share common tools. This is due to their physical and virtual isolation from one another.

IT cybersecurity typically focuses on the CIA (confidentiality, integrity and availability) standard. **Confidentiality** is seen as the most relevant factor. Information and data drive IT networks; privacy matters.

OT security, on the other hand, tends to follow the AIC standard – in other words, **availability** plays the most important role.[9] Why? Consider the following scenario: electricity is distributed from a main power source into different villages through different branches. A malicious actor interferes with the main source in two ways. Firstly, the attack is carried out in a way that ensures information about electricity distribution to the different villages is gathered without consent. Secondly, the attack damages the source, cutting off electricity to a certain village. In this case, not having electricity is more damaging than unauthorised data being exposed.

Availability, in the OT context, is also often linked with the concept of **safety**. When OT systems are not available, the safety of personnel and the environment could be affected.

Cybersecurity is key to the stability of the converged IT-OT network. Without effective security systems leaked classified information could harm entire companies or industries and the lives of people could be put at risk. But there are many different cyber-attacks and they can come from many internal and external sources. An effective security system must protect a network from any threat coming from anywhere.

Cybersecurity is key to the stability of the converged IT-OT network. Without effective security systems leaked classified information could harm entire companies

9 Security Delta, 2021; Available at: https://securitydelta.nl/images/HSD_Rapport_OT_mei_2021.pdf

4. Solutions enabling OT cybersecurity

There is a clear need to assess current OT infrastructure and understand the potential vulnerabilities in the combined OT-IT network. What cybersecurity needs do these vulnerabilities create? Once cybersecurity measures are in place their maturity level should be mapped to the identified needs of the organisation. The resulting gaps will indicate the areas that need improvement.

There is a clear need to assess current OT infrastructure and understand the potential vulnerabilities in the combined OT-IT network

There are several international standards in place that can be useful in securing the OT-IT network:[10]

- **ISA/IEC 62443:** This framework is aimed at reducing current and future security vulnerabilities in industrial automation and control systems.
- **ISO 27000 Series:** These standards support organisations in strengthening their information security practices (particularly ISO WD 27030 – Guidelines for Security and Privacy in IoT)
- **ENISA guide 'Protecting Industrial Control Systems':** A document compiling ICS security related standards, guidelines and policy documents
- **Homeland Security:** Cybersecurity assessments of the Industrial Control Systems Guide
- **MITRE ATT&CK ICS Framework:** A globally accessible knowledge base of tactics and techniques used by cyber threat actors.

According to IEC 62443,[11] a fully integrated security system should consider the following domains:

10 Garland Technology, 2022; Available at: https://www.garlandtechnology.com/blog/https/www.garlandtechnology.com/blog/understanding-ot-frameworks-and-standards-for-a-more-secure-industrial-network

11 IEC, 2013; Available at: https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Den.pdf

Exhibit 4.1: System security requirements and security levels according to IEC 62443 [Source: Axon Consulting, based on IEC 62443]

An OT network security system can be assessed against the domains portrayed above using the standard IEC 62443. What is the 'Achieved Security Level' (known as the 'SL A') of an OT control system? How does this compare with the target state security level of the control system ('SL T')? What capabilities or 'control requirements ('CR's) have to be implemented to match this level?

For example, a certified security level ('SL') 1 device has achieved SL1 in all domains portrayed in Exhibit 4.1 based on the CRs implemented. This value symbolises the integrity of the device / system: the security level achieved ('SL A') compared to the 'SL T'.

The IEC 62443 standard also offers assessment via what are called 'maturity levels'. Here, organisations are audited on the capabilities they have to carry out a given security process. These are rated from 1 to 4, with level 4 being the most mature. Note, however, that there is no defined relationship between the security level and maturity level within an organisation.

In some territories, governments have taken steps to support and protect their national organisations by implementing their own guidelines or even regulatory standards

In some territories, governments have taken steps to support and protect their national organisations by implementing their own guidelines or even regulatory standards; some are based on the international standards mentioned above. Notable examples include the efforts undertaken by NIST (National Institute of Standards and Technology) in the United States through its Guide to Industrial Control Systems (ICS) Security (2015)[12] and Guide to Operational Technology (OT) Security (2020)[13] (currently in draft edition). Also relevant is the NCA (National Cyber Security Authority) in the Kingdom of Saudi Arabia, via its regulatory cybersecurity control document Operational Technology Cybersecurity Controls (OTCC) (2022),[14] which aims to develop national-level regulation on the control of operational technology cybersecurity.

The USA and the Kingdom of Saudi Arabia ranked in first and second place respectively in the ITU's last Global Cybersecurity Index (GCI)[15] in 2020. The NCA regulation is featured in the case study on the next page.

12 NIST, 2015; Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

13 NIST, 2020; Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

14 NCA, 2022; Available at: https://nca.gov.sa/otcc_en.pdf

15 ITU, 2020; Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Case study: NCA's operational technology cybersecurity controls

NCA's regulatory control document for OT cybersecurity was developed according to a comprehensive study of multiple national and international cybersecurity frameworks and standards. Published in 2022, it is meant to be implemented as an extension to NCA's Essential Cybersecurity Controls (ECC-1: 2018). The regulation is primarily intended for facilities deemed as 'critical' and owned / operated by government organisations (such as ministries, authorities, establishments etc.), as well as private sector organisations owning, operating or hosting Critical National Infrastructures (CNIs), whether they are in the Kingdom or abroad. Nevertheless, any organisation in the Kingdom may leverage these controls to implement best practices and improve their OT cybersecurity. The term Industrial Control Systems (ICS), which is the focus of this regulation, refers to all devices, systems or networks used to operate / automate industrial processes. The objective of the control document is to ensure higher levels of national cybersecurity through the protection of OT infrastructure within the regulated entities.

5. Conclusion

- OT-IT convergence is a fast-moving, fast-changing situation that will require much more relevant cybersecurity expertise.
- Industrial entities undergoing digital transformation mustn't neglect securing their OT-IT networks as a part of their IT infrastructure.
- While standards exist and are useful, supporting expertise for companies wishing to apply them is in short supply.
- Axon knows the standards landscape and how and when a given standard or regulation can be applied to IT-OT convergence. Axon can assist entities or government agencies in this process.
- Contact us to understand how we can help.

About
Axon Consulting

Axon is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's cybersecurity practice is central to its business and an increasingly important service area for clients. Its work in this field includes strategy, policy/regulation, and research at business and governmental level. Axon works closely with national representatives to help them understand their cybersecurity needs and to define actionable recommendations aimed at improving their cybersecurity ecosystems.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com

Madrid (HQ)
Calle Sagasta 18,
3rd Floor,
28004, Madrid

Brussels
91, Avenue du Roi,
1190, Brussels

Istanbul
Buyukdere Cad.
No. 255 Nurol Plaza,
B0434450 Maslak,
Istanbul

Bogota
Calle 100 #13-95,
Torre Empresarial FD,
100 Piso 6,
Bogota

Riyadh
3141 Anas ibn,
Malik Road, Building B,
2nd Floor,
Al Malqa, Riyadh

AxonPG

axon-partners-group