FUJITSU

Why building a strong OT security network is key to support resilience and competitiveness

Jamie Wilkie
Product Owner OT
Security Services at Fujitsu

What is Operational Technology?

Operational Technology (OT) is the use of hardware and software to monitor and control industrial equipment, physical processes, devices, and infrastructure. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), remote terminal units (RTU), programmable logic controllers (PLC), as well as dedicated networks and organization units.

OT can be used to carry out several tasks ranging from monitoring critical infrastructure to controlling machines on a production floor. In essence, it's fundamental to our lives, literally controlling matters of life and death. Take water treatment, for example. Just the right amount of chlorine is needed to make drinking water safe. Too little and we get sick, too much and we might die. OT ensures vital production processes run smoothly to ensure employees are physically working in a safe environment.

Yet, it's historically been air-gapped from the rest of an organization's network. A strategy to not only protect them from malicious actors, but also from internal IT team interference due to the complexity of the estate.

Securing your OT estate

But times change. Organizations on their digitalization journeys need to free themselves of the idea that their OT and IT environments should be kept separate. It's a dangerous decision because you will only be able to identify and exploit new efficiency opportunities or meet sustainability goals by getting data out of your production environment.

Likewise, as organizations further look to drive optimization and sustainability into their operations, the need to use next generation technology and approaches – such as AI, digital twins, and self-healing capabilities – has become essential to success. Simply ignoring what's on offer from digitalization is not an option. Improving production and supply chain efficiencies with smart sensors and sophisticated analytics will bring OT into the 21st century. But with the introduction of any digital innovation, cyber security must be at the forefront of implementation – building in protection right from the start to keep customers and business data secure, prevent damage to infrastructure and avoid supply chain disruptions.

Cyber incidents have increased in recent years – in the US, more than **$43 billion has been lost through social engineering and phishing attacks** on business emails since 2016 and globally, 82% of CIO's believe their organizations are **vulnerable to cyber attacks targeting software supply chains**. With millions of Internet of Things (IoT) devices being added to industrial networks to reduce costs and deliver more value to customers, OT is becoming more connected – exposing organizations to new security threats.

IT has been dealing with cyber threats for decades. But the critical nature and physical implications of OT downtime makes addressing cyber security threats and responses unique. A greater focus now must be paid to OT security across production industries. Understanding the scope of the cyber security challenge – as well as the greater benefits that come with a secure OT estate – is essential to being productive, and then to digitally transform to remain competitive and relevant to your customers.

"We cannot control what we cannot see. In the past, our industrial control systems were air-gapped and isolated from more conventional networks. As the manufacturing industry is becoming increasingly digitized, we also had the challenge of greater connectivity and convergence between IT and OT in order to remain competitive and relevant.

We chose Fujitsu to do an OT assessment for RPM because of their experience within our industry. Their service is based on a proven methodology, supported by OT discovery and analysis technology, to give deep and actionable insights.

Mark Rankin,
Vice President of Global Systems at RPM International Inc.

Why is securing production industries so challenging?

In essence, IT and OT are starting from different places. IT cares about the confidentiality, integrity and availability of data, whereas OT cares about the availability of physical production processes and safety. The differences between the two are stark, and this can play out in reality in a number of ways.

IT systems are typically renewed every three to five years while OT systems can remain in place for decades. We see critical physical equipment being controlled by devices (e.g., PLCs) and OT systems (e.g., SCADA systems) that are completely outdated by IT-standards because they operate in a static configuration which cannot easily be updated. This represents a cyber security risk.

Also, IT is used to closely manage all devices on the network across the enterprise which also controls access rights. OT assets tend to be managed in a more ad-hoc fashion on a per-site basis. Access is less tightly controlled because of different needs such as shift-working and remote maintenance.

The workers and managers in OT environments tend to come from an engineering background and not an IT background. IT experts generally have a limited understanding of the imperatives of production. Traditionally they are organized in different reporting structures. Hence, the transition to digital production is a challenge to individuals as well as their management structures.

While OT is the heart of value creation, it's a vulnerable entity. This combination makes it an attractive target – according to IBM, **manufacturing was the industry most targeted by hackers in 2021**, accounting for 23.2% of incidents.

Why a secure OT estate is vital

Efforts to digitize operations are ramping up across all sectors of business – with an OT estate at the heart of innovation in the production industry. It's clear that, in future, those not striving for digital transformation will only be relevant as business school case studies of missed opportunities.

Businesses now need to be fit to play in this new and highly competitive environment. But this urgency means manufacturers often have limited time to align their digitization security strategies with their OT. Opening OT to digitalization without the right security measures exposes production to unexpected risks – leaving a lot for OT operators to contend with.

When it comes to creating a secure OT network, there are some essential models and standards that must be in place. However, most OT operators are still at the start of their security journeys in addressing OT and IT integration. Getting this right will be fundamental to future business resilience and growth.

To drive efficiency and resilience across your estate, standardizing your processes using data from production is crucial in minimizing downtime to ensure operations can continue if an incident does occur. Here, technologies such as digital twins and advanced data analytics, made easily consumable using Fujitsu Uvance services , can be used to optimize production and maintain competitiveness. Fujitsu Uvance is a new global business brand delivering a transformation portfolio for a sustainable world. Seven key focus areas are identified within the new brand to accelerate business and challenges social issues.

"Before we can sell quality products, we need to manufacture them in a safe and secure environment. As production assets become connected, more smart, and use data to optimize the manufacturing value streams, that movement will expose those complex environments to be accessible by hackers. However, safe and secure products must be manufactured in a controlled environment where no one has hampered with the process! And this is vital for Consumer Packaged Goods, MedTech and all other industries."

Sebastiaan Laurijsse,
Global Head of Industry High Tech at ServiceNow

But there are also industry-specific reasons as to why you should secure your OT estate and integrate with your IT environment. For some, this might help drive progress for wider sustainability targets by using insights from data to reduce CO_2 emissions and energy consumption. For others, such as utilities and Critical National Infrastructure (CNI) organizations, the enhanced security measure ensures compliance regulations are being adhered to.

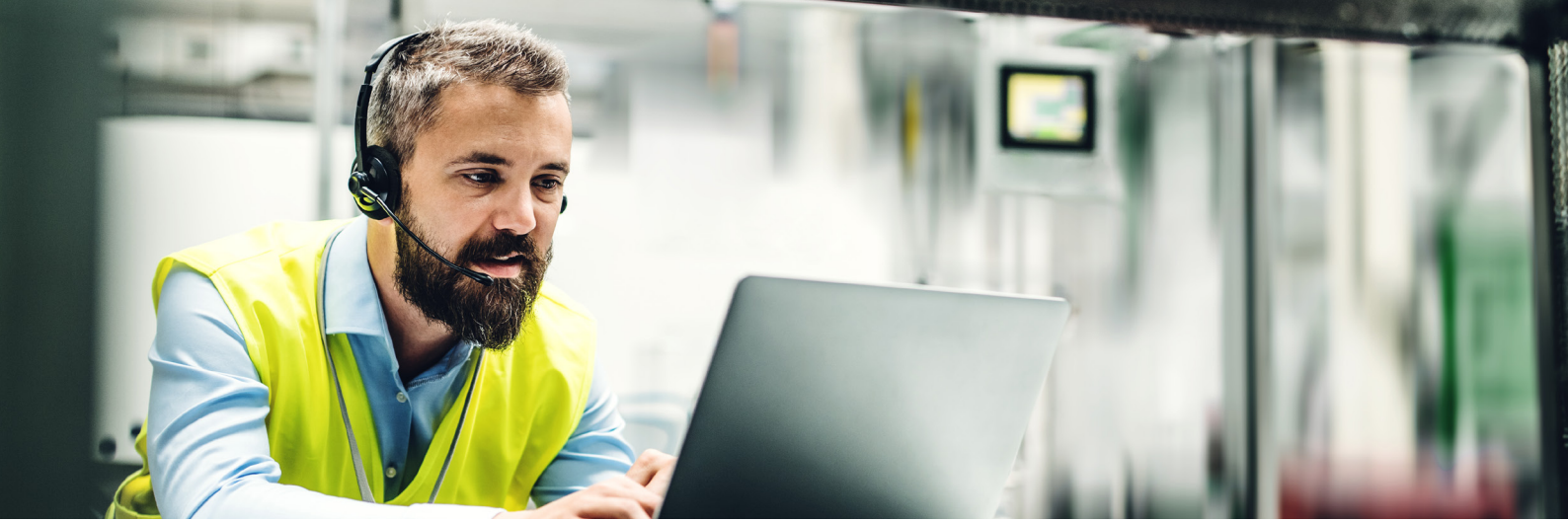
Consequences of an ineffective OT security strategy

Not having a strong OT security can lead to huge ramifications (like cyber breaches and ransomware). Take the ransomware attack on the world's biggest meat processor, for example, an **$11m ransom was paid** after a cyber attack shut down its operations.

In addition to cyber attacks, there are many downsides to having an ill-equipped OT security strategy.

These include:

- Violation of legal requirements in regulated industries.
- Loss of insurance support if specific compliance requirements are not fulfilled and the cyber security posture is unknown.
- Human safety issues, for example, if a machine breaks down due to lack of maintenance and leads to an accident in the factory.
- Production losses, which equate to financial losses.
- Harm to the environment, for example, if toxic elements are exposed to the air, water or food supplies. This is especially crucial in utilities and CNI organizations.
- Damage to brand reputation.



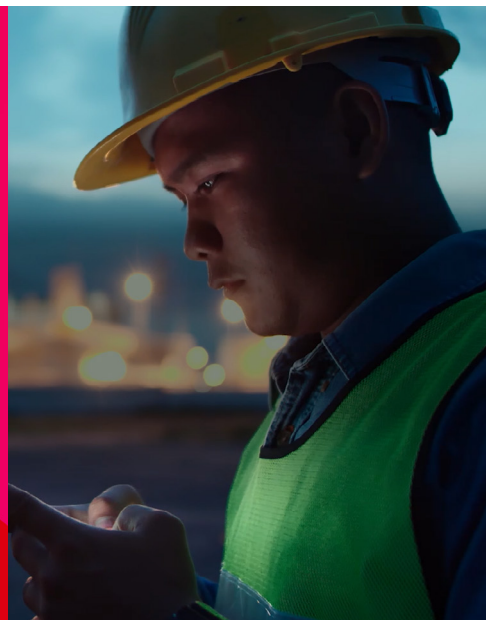
Benefits of OT security

Cross-enterprise visibility on networked production assets is key for cyber security and for a broader digitization program. One of the first steps in creating a secure OT environment is having visibility. This in turn enables the implementation of good OT asset management techniques to support business resilience, enhance competitiveness, and move the business forward.

For instance, you'll be able to know in advance when a machine is due for maintenance and plan ahead for downtime – rather than an unexpected event costing businesses collectively **billions in annual revenue**.

"Before you can protect your industrial assets, you need to increase visibility. That level of visibility needs an ecosystem of tools orchestrated by a single platform to manage the total lifecycle of the production environment. As this enables you to orchestrate work and manage risks at any level of the organization."

Sebastiaan Laurijsse,
Global Head of Industry High Tech at ServiceNow



By having a secure way to obtain data from the production environment, organizations can process data and use the insights to enhance Operational Equipment Effectiveness (OEE), track CO_2 emissions and optimize energy consumption (not only in the overall factory, but across the different production processes) to drive competitiveness – all while reaching their sustainability goals.

OT cyber security helps prevent financial, intellectual property and reputational loss through the impact of cyber incidents and is a major contributor to compliance with regulations such as Europe's NIS-D regulation or the American NIST standards.

What should your OT security strategy include?

- Organizations need to understand their business drivers. Is the goal to digitally transform production across the enterprise or is there just a need to locally improve the security of one site? This will help scope the OT security strategy.
- A typical OT cyber security journey starts with securing the perimeter of production plants and then separating the IT and OT networks, as described in IEC 62443. Following this process allows secure communications with OT while reducing exposure of the OT assets to threats emerging in enterprise IT. For instance, through malicious email attachments. These basic protections are then enhanced with security processes.
- Access and identity management are required to securely support processes such as remote maintenance.
- The NIST 800-61 cycle of Prepare-Protect-Detect-Respond-Recover is implemented in many IT environments but is typically missing in OT. Roles and responsibilities need to be clarified. We see many CIOs being charged to cover OT security in addition to IT. To do this they need to bring OT competence in their teams and to develop relationships with production management and the production teams.

A Gartner study showed 60% of companies are at the start of their OT security journey, 30% are engaged in fundamental remediation and only 10% are at the level where OT security is a standard part of their operating procedures and recognized as a building block for digitization.

The message is clear – if you don't have an OT cyber security strategy yet, then you are not alone. But it's time to get started.

How Fujitsu can help

At Fujitsu, our commitment to our customers is ensuring you have a strong OT security posture to facilitate the digital transformation needed to drive your business forward.

Every organization is at a different stage of their transformation journey and, with this, comes unique and varied needs. So, we provide services that cater to each business' requirement:

OT assessment & asset discovery service: we can evaluate your OT environment to establish an overall understanding of your assets and technology, carry out a risk analysis on possible vulnerabilities and then take that risk analysis to the business process level. We can upload asset data discovered into a Configuration Management Database (CMDB) to help drive your overall OT management.

Uplevelling your people: we evaluate the level of training your employees currently have and your existing processes. So, for example, in the IT world, there's a response process put in place to respond to threats if an IT incident of any type happens. But this doesn't exist on the OT side for most organizations. We look to expose these kinds of weaknesses and make recommendations for best practice.

Managed continuous service: this allows us to continuously monitor the traffic on an OT network to detect any irregular events. For example, let's say you have a machine that's fired up on a Monday morning and is put to bed on the Friday afternoon. And suddenly on Wednesday afternoon, it's getting temporary stop commands and OT protocols that nobody else understands. We would be able to spot that and alert you to the discrepancy so it can be swiftly dealt with – minimizing the risks to your production.

Factories need to be maintaining uptime, physical safety, compliance and driving forward sustainable practice. Becoming more data driven can help you achieve these outcomes. But first, you must create a secure network for your OT estate in order to spur the digital transformation that will enable this to happen.

Get in touch to learn more about how we can help you develop a strong and secure OT network to facilitate your digital transformation journey.

Click here

FUJITSU