White Paper

How to Navigate Operational Technology (OT) and IT Integration

Definition of operational technology (OT)

Operational Technology (OT) encompasses hardware and software used to implement processes and support monitoring and control. Industrial Control Systems (ICS) refers to these systems when deployed to perform industrial processes. Extended Internet of Things (EIoT) and especially Industrial Internet of Things (IIoT) refers to an increasingly common body of technology for providing direct access from devices on the factory floor to the cloud for easy access and integration with business systems.

Fujitsu operational technology (OT) security

Differences between IT and OT

The differences between IT and OT are not only in technology but also in people, training, organisation and culture.

IT mindset

- The world is virtual
- Priority is data confidentiality, availability and integrity
- Corporate management of networked assets
- Agility

OT mindset

- The world is physical
- Priority is safety, availability and resilience of production processes
- Plant-level management of networked assets
- Measuring overall equipment effectiveness
- "Don't touch, don't break" culture

In the past, OT and IT teams operated independently, posing a potential threat to the safety, reliability, and resilience of your IT infrastructure. In an era of unprecedented cyber-attacks driven by our growing digital dependence, the deployment of seamless networks that enable widespread connectivity also necessitates a robust defence for OT against cybersecurity threats.

It's imperative to recognise that integrating OT and IT is essential not only for security but also for effective management, as both are pivotal to your overall success.

The importance of system integration

OT systems also include Building and Energy Management Systems (BMS & EMS). Integration of control and telemetry from these systems with ICS can be leveraged to create business benefits including

- improved energy efficiency
- streamlining of operations
- enhanced safety and security

Opportunities in modern industrial control systems (ICS)

Modern ICS operate in a complex eco-system of requirements stemming from the necessity for companies to comply with safety, security and quality regulations; decrease waste so increasing the sustainability of operations; and increase productivity and competitivity.

The vital role of data in ICS

Without data from ICS any improvements are just someone's best guess; to truly optimise across these often conflicting priorities businesses must utilise the data from the process.

Security regulations and incident response

With security regulations, audit logs are required to support incident response processes, and security telemetry is required to identify incidents.

Sustainability through process monitoring

For sustainability, process monitoring needs to occur to ensure that the process is operating within efficiency parameters and emissions need to be recorded for carbon reporting.

Productivity enhancement through secure remote access

Productivity requires secure remote access to unmanned facilities so that you can get the most out of a stretched workforce of OT maintenance staff – this also contributes to lower miles, improving sustainability statistics.

Business benefits of ICS integration

It also has significant business benefits such as the ability to integrate manufacturing and logistics with order and billing systems for greater automation of these processes as well as enabling data-driven insights and increased flexibility and agility by breaking down silos and creating a connected ecosystem.

Addressing the challenge of integrating OT and IT systems for improved OT Security

All this integration creates pathways between the OT and IT systems which if not treated carefully begin to break down the solid network and infrastructure security foundations of the defence-in-depth which is provided by following the Purdue model. If connectivity between the OT and IT systems becomes exponentially more complicated, then the effort required to secure these communications grows with similar complexity – leading to mistakes.

Security implications of integration

The issue is not just in securing of communications. Dependencies between OT and IT for exchange of data (such as manufacturing/logistics, and ordering/billing systems) makes the risk landscape more complex. If customers cannot place an order, and you don't have warehousing sufficient to store produced goods, then you may need to cease production until the functionality of the ordering system is restored.

Clearly, we need a solution that enables secure and resilient integration between OT and IT systems, and a platform which supports the integration of mitigations that are required in the changing landscape of threats, risks, and regulation.

The solution

Fujitsu believes that the solution has three parts. Future chapters will go into greater detail about how each of these should be implemented, but the concepts are introduced here.

1. Build solid foundations for network and infrastructure

In this stage, companies should take steps to ensure that their OT environments are well understood with continued good visibility, that governance is in place to inform security decisions, that appropriate connectivity is established to allow security operations, and that IT and OT security are effectively implemented and managed with defined processes and responsibilities for network, data, and application management.

Leveraging a hybrid core & cloud model

For many companies, a hybrid core & cloud model cannot be avoided. Where many services are required to broker communications to support OT/IT convergence and secure remote access, local management would create an unmanageable burden. If these services are federated in the cloud, then companies can take advantage of IaaS to deploy these services with many potential advantages including:

- Reduced costs compared to managing own data centres

- Accessibility – including remote access

- Scalability – services scale with demand. Relatively easy to onboard new facilities

- Disaster recovery and backup – cloud services offer robust data and configuration backups for services in the cloud environment. These are managed by the cloud provider easing burden on site personnel.

- Advanced analytics

Managing edge compute for secure cloud connectivity

But with the added benefits comes the requirement to manage a secure connector from the facility to the cloud. This connector comes in the form of edge compute which must normally be managed from the facility – requiring local qualified and experienced IT staff to provide the maintenance that such a complex feature requires.

Fujitsu offers an edge compute capability as a managed service making this transition easier. As well as providing the essential services of a connector, Fujitsu's Virtual Edge can be deployed with many options improving quality of life including intrusion detection with managed monitoring as a service, secure remote access, CAF compliant centralised and automated backup, virtual workstation capability, data historian and others.

The net result is a secure and scalable infrastructure for security operations and management which has several additional benefits. Fujitsu can relieve burden for management of security from IT staff and enable them to focus on their normal responsibility. This is extremely valuable, as when staff are overstretched in management of security – it is often OT which suffers the consequences.

2. Leverage data to drive transformation

Once established and configured, the edge compute capability can be used as a platform for data exchange between the OT and IT systems. This is referred to as OT/IT convergence. When data is appropriately collected, processed, and analysed, it provides knowledge which can be a powerful asset to a business.

Intelligent Industrial Operations starts with this knowledge. Data about your process can be used to train machine learning algorithms which can react to patterns in data that humans may not recognise. Examples of this include predictive and preventative maintenance, OEE measurement and monitoring, root cause analysis, asset risk management and energy and

emissions management. Fujitsu works with leading providers of these solutions to bring these benefits and more to manufacturers.

It is also possible to use the solid foundations to enable the industrial workforce through secure remote access to industrial facilities allowing engineers to maintain sites from any location. This results in less time spent travelling between sites and frees staff up to perform more maintenance opportunities.

3. Digitally transform

Digital transformation is a process which is driven from the top down. Top in two senses, from board-level sponsorship and from the core goals of the organisation. Adding features and technology to an operational environment, and hence increasing its connectivity, increases complexity which is the enemy of maintainability and security.

This should only be done if it supports the business' high-level goals e.g. increased revenue and profitability owing to increased productivity, enhanced overall equipment effectiveness, assured compliance to regulatory frameworks and improved sustainability of operations.

If any of these are priorities for your business, then this connectivity is going to be essential as these all rest on secure foundations and leverage data to drive transformation. The battle then becomes about how to achieve this functionality with minimal complexity and in a scalable and maintainable way.

About Fujitsu

Our Purpose is to make the world more sustainable by building trust in society through innovation.

To fulfill the Fujitsu Group Purpose, we will enhance our ability to stay in tune with global society, while continuing to make agile changes, and creating value. We offer a broad range of products, services and solutions, and have approximately 130,000 employees supporting customers from over 50 countries and regions.

To find out more about Navigating Operational Technology and IT Integration, please email askfujitsu@fujitsu.com and/or +44 (0) 1235 79 7711 and quote 4217.