Building cyber resilience in Industrial Systems

FUJITSU

Contents

As organisations strive to achieve the benefits of digitisation in their core operational processes, ensuring effective cyber security can appear to be just another cost or to be at best a necessary compliance requirement.

However, cyber security is more; it is a key characteristic of high-quality digital products and services. This whitepaper explains how cyber resilience is a crucial part of the value an organisation gives to its customers and stakeholders, and describes a live project, which Fujitsu is helping a leading UK Critical National Infrastructure Provider to deliver.

Market overview

All industries which deal with physical assets are facing the opportunities but also the challenges of digitisation.

While seeking increases in efficiency and innovation, it is paramount to maintain the availability and quality of the goods and services being produced and to ensure the physical safety of workers, customers and indeed whole communities.

At the same time new regulations and directives such as the EU NIS D place compliance demands on regulated industries and raise the bar of expectation for non-regulated industries.

Cyber threats exacerbate the existing challenge of Business Continuity. Operators face both generic and targeted cyber threats. Generic threats often aim at enterprise IT but can also severely impact operations.

Think of the disruption caused by the ransomware WannaCry at a European vehicle production plant, in transportation and in British hospitals in 2017.

More targeted threats aim for operations technology itself. Stuxnet, which partially disabled the Iranian uranium enrichment programme in 2012, is often considered the first major military-grade cyber attack on Operational Technology (OT).

The Black-Energy-3 attack on the Ukranian electricity supply in 2015 is a further high-profile example of a very specific infrastructure targeted by well-resourced, possibly state-sponsored, actors.

These attacks have a real human cost. The Ukranian power outage left almost a quarter of million people without electricity for about 6 hours. The Wannacry incident resulted in 19,000 medical appointments being cancelled by the British health system.

In comparison, a 2018 case of misusing a SCADA system regulating sewage treatment in order to mine crypto-currency[1] appears relatively harmless but illustrates the vulnerability of OT systems to generic, non-targeted threats.

The commercial and national security value of OT makes it an attractive target. As more toolkits specialising on OT infrastructure appear on the black market, operators can expect to see themselves facing more assaults on their OT.

Tackling the security challenge

Historically organisations have largely separated the management of their enterprise IT and their Operational Technology.

While IT security has mainly focused on data protection and confidentiality, OT's focus is on process continuity and physical safety. The advent of digitisation requires both engineers and management to understand the priorities and to embrace the strengths of both the OT and IT disciplines.

While IT equipment is typically replaced every few years and software updates occur regularly, OT equipment may be in use for decades and stable configurations are not changed in order to avoid re-certification.

IT communications are highly standardised while OT uses a plethora of communication protocols. So how can the techniques, technologies and learnings from IT Security be applied to OT security?

[1] https://radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/

How we can help

We take a modular approach to improving the cyber security of OT. We look at the connectivity of equipment and locations and prepare for standardised, IP-based connectivity.

We logically and physically segment the network in accordance with the best practices recommended by standards such as IEC 62443 and NIST SP 800-82, in compliance with relevant legislation such as the UK's Network and Information Systems Regulations 2018.

We provide monitoring of the networked and segmented OT estate from our global Advanced Threat Centres (ATC), continuously monitoring traffic on the infrastructure and communicating closely with our customers' own operations centres to deliver relevant and timely intelligence that helps detect and respond to threats to OT in a proactive way. We leverage our consulting and professional services to assess current challenges against the standards and to deploy leading partner technologies such as firewalls and monitoring systems.

Outcomes

We believe that investing in the necessary foundations for cyber security for OT can help open the door to many business benefits.

For example, creating a secure and reliable network serves the needs of both security and productivity. The network will collect data for predictive maintenance and at the same time be monitored for security. Knowing the state of equipment at remote locations increases security but also helps reduce the number of engineer inspections and ensures that when an engineer does go out, the right spare parts are in the van.

The opportunity goes further. The ATCs are the perfect integration point for unified, intelligence driven monitoring of the entire IT and OT estate, opening the door to holistic monitoring of our customers' end to end business processes. This allows customers to be prepared for threats and to respond to them before they have a costly impact on their machinery, operations, customer service levels and ultimately the business' reputation and bottom-line.

Co-creation – engage with Fujitsu

There is no off-the-shelf solution that matches the needs of all industries and customers.

That's why Fujitsu offers established building-blocks and best practices based on our extensive experience as a global system integrator to help build digitisation programmes within the utilities and CNI industries. We can apply our capabilities as a leading global security service provider to co-create and securely enable the convergence of OT and IT.

Contact us to share your thinking and ours.

We can meet at one of our Digital Transformation Centres and jointly develop your secure digital transformation journey. Read on to take a closer look at how we are already doing this with a leading water services supplier.

Case study

Customer's goals and benefits

A UK provider of public drinking water and waste water services is engaged in a multi-year transformation of its service provision to consumers and businesses.

Aims of the transformation include improving drinking water quality, protecting the environment and supporting economic growth in the catchment area. These high-level aims break down into specific measurable goals such as reducing water loss through leakage, reducing disruption in communities through maintenance work and reducing operational costs. Central to the achievement of these goals is increasing the visibility that the water service's operational control centre has on the current and predicted state of the overall system.

Centralising and digitising control

Centralising and digitising control of remote locations opens the door to process optimisations such as reducing time spent sending engineers to inaccessible locations and ensuring that engineers have the right equipment and information available to them when they are at remote sites ("intelligent hands").

Relevant and current data

Relevant and current data will constantly be available to the control centre and the insights made possible by analysis of the data will improve operational efficiency in the short term and lead to further beneficial use cases not yet envisaged – the investment in digitisation will drive future innovation with the associated customer and business benefits.

Customer situation

The water service provider has a sizable existing estate. This consists of physical locations and operational equipment.

Much of the equipment is already locally monitored and controlled using various generations of PLC[2] and SCADA[3] systems. In some cases rudimentary connectivity is available through telephone network technologies. A data centre supports enterprise applications and some of the operations of the physical estate.

Connect all locations

The aim is to systematically connect all locations and equipment to a consistent IP communications infrastructure. This enables standardised monitoring, analysis and control, thus improving the manageability of the OT related components and processes. This is a brown-field undertaking, requiring significant changes to a running system while making best use of previous investments.

Safety and availability

The safety and the availability of water services are sacrosanct and the top priority of the service provider.

Data which represents intellectual property or which can be associated with individuals must also be protected. Security by design is therefore a core principle of the new architecture.

[2] Programmable Logic Controllers: control physical equipment and connect to SCADA systems
[3] SCADA: Supervisory Control and Data Acquisition – process management systems close to the physical infrastructure. Frequently based on personal computer technology

Blueprint for Industrial Security

Understand what is required

As an Operator of Essential Services (OES), defined by the UK's Network and Information Systems Regulations 2018, the water service provider must take "appropriate and proportionate technical and organisational measures" to manage security risks and minimise the impact of incidents involving its network and information systems[4].

The OES is required to demonstrate this using the Cyber Assessment Framework (CAF), authored by the National Cyber Security Centre[5]. The CAF makes reference to various technical and process standards, in particular to the IEC 62443 series[6]. Industrial security standards such as those from IEC and NIST[7] emphasise the principle of defence-in-depth to contain the spread of any breaches that do occur.

Define responsibilities

In common with other companies, this water service provider is placing the responsibility for the management of IT systems used by OT in the hands of the IT group. This includes SCADA systems and historians[8].

Over time, this will allow IT to introduce standard practices such as backup, restore, patch and vulnerability management and controlled access to the management systems.

The complexity lies in the detail: SCADA systems, for instance, often have very specific software configurations closely linked to the underlying PLCs and physical devices.

Real-time systems are sensitive to performance degradation and latency increases caused by running IT management processes on them. Any changes to these systems may affect their operation. Given the complexity of the underlying infrastructure and its long life cycles, it will take many years to completely change the management paradigm, but a start is being made.

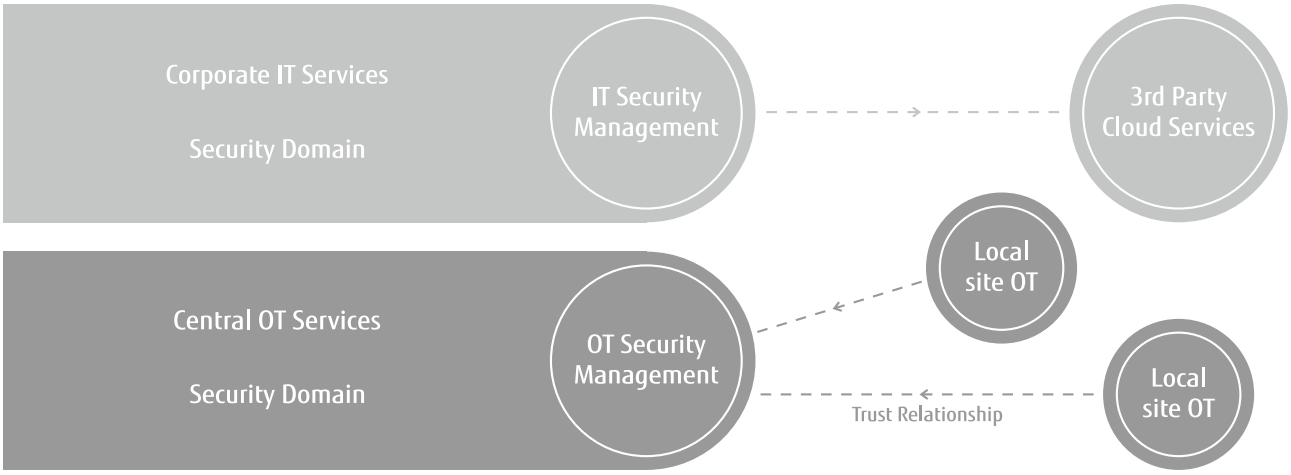
However, the responsibility for the Operational Technology processes as such – for instance, regulating the amount of chlorine added to drinking water – must remain firmly in the hands of the OT experts.

[4] STATUTORY INSTRUMENTS 2018 No. 506 ELECTRONIC COMMUNICATIONS The Network and Information Systems Regulations 2018, §10
[5] https://www.ncsc.gov.uk/collection/nis-directive/cyber-assessment-framework
[6] Published sections available at https://webstore.iec.ch/home
[7] NIST SP 800-82r2, Guide to Industrial Control Systems (ICS) Security
[8] Historian: a time-series database capturing data from operational equipment

Segment the networks

Having clarified responsibilities, it is possible to move to the design of the new architecture. Enterprise IT and OT networks are often not sufficiently separated and compartmentalised. This weakens security, integrity and compliance.

A high-level separation of security domains and levels of trust (see illustration) guides the overall design. Note that we do not assume a trust relationship between Corporate IT and Operations Services.



A key best practice is network zoning or segmentation: logically separating enterprise IT from operations IT and introducing sub-zoning to control the access of one location from another and from one OT device to another. This approach is applied both in the central data centre and in the outlying facilities.

The aim is to prevent intruders from finding a weak entry point to the overall system (e.g. a phishing email in corporate IT or an infected USB stick inserted to an OT system), and if they do gain access to one part of the infrastructure, preventing them from branching out to other areas.

At the same time, controlled flexibility must be maintained. For instance, to support emerging use cases which foresee communication between collaborating OT devices and further automation.

The new architecture reflects the "zones and conduits" recommendations of IEC 62443-3-2 and enables the security layering described in IEC 62443-3-3.

A prerequisite for the correct implementation is the clarity on IT and OT responsibilities. For example, correctly configuring and managing the firewalls protecting the OT locations and equipment is a key part of implementing the network design. The firewall rules must allow the desired operations and innovations while precluding abuse as far as possible.

The firewalls on the IT and OT sides are managed separately by the respective IT and OT teams within the overall governance framework. As part of a longer-term transformation, this architecture allows the best possible isolation of systems that can neither be patched nor readily replaced.

Define access rights – who, what and why

As in many industries, the water service provider works closely with third party system suppliers who provide and maintain equipment used in the provider's facilities.

These system suppliers need access to their equipment and the data it generates. This can be useful both to ensure the availability of the equipment (e.g. predictive maintenance, installation of updates) and to support new business models (e.g. pay-per-use).

Today this access is often provided by physical access to the device by employees of the system supplier or by "side-door" remote administrative access to the system software.

The new architecture allows more control of this process: for instance by restricting the time window for administrative access and requiring stronger authentication of the engineer, e.g. through multi-factor authentication.

Over time it is to be expected that physical access and "side-doors" will be replaced by less vulnerable techniques which still satisfy the business requirements of both partners.

Continuous monitoring

The IT devices at each location on which OT processes run (e.g. SCADA systems) are managed in a central asset database. This provides valuable data to help with the management of the device's lifecycle, in particular vulnerability management and software version management.

The above foundational steps are essential to allow the implementation of continuous cyber security monitoring of the OT estate.

In this project the focus is on securing the IT controlling OT. In terms of the Purdue reference model this means Layers 2 and 3 and above. The devices, the network health and the SCADA network traffic are monitored.

Log files are gathered from the devices while performance-neutral monitoring of the OT network traffic is conducted.

The monitoring data is securely transmitted to Fujitsu's Advanced Threat Centre (ATC) where it is automatically filtered according to agreed rule sets, correlated with other relevant data and visualised for human comprehension. Anomalies in the OT traffic are identified, and regular reports generated for the customer.

Real-time alerts, where appropriate, are forwarded immediately to the customer's Operational Control Centre, and co-ordinated action taken through established and rehearsed procedures.

The overall security architecture and processes enable the customer to provide evidence of best practices, for compliance with the NIS Regulations.

The end-to-end view of cyber security complements end-to-end management of the OES's critical operational processes, enabling improved service delivery to the community while ensuring business continuity and safe water service provision, keeping regulators, customers and shareholders satisfied.

Future development

The reach of the security process will be extended in future as operators exploit services available in the cloud.

The OT infrastructure will not be directly connected to the cloud but techniques such as "digital twins" will make it possible to manipulate representations of the infrastructure in the cloud.

For example, diagnostic or pay-per-use data for physical equipment can be made available in the cloud by the operator. The equipment vendor then accesses the required data in the cloud without physically accessing the control units or the equipment itself.

Cloud service providers have invested heavily in making their infrastructures secure and they are themselves subject to the requirements of NIS.

However, enterprises connecting to the cloud have a responsibility to ensure that consistent security controls are applied to data in the enterprise and in the cloud[9].

[9] https://www.i-cio.com/strategy/cloud/item/mastering-the-art-of-multi-cloud-security

Conclusion

Managing shared responsibility for the security of the overall end-to-end system emerges as a recurring theme of digitisation.

It applies internally between IT and OT responsibilities. It applies externally in the operator's relationship with OT system suppliers, IT and cyber security service suppliers and to suppliers of cloud services.

The ability to manage this distributed security responsibility and to demonstrate the cyber reliability and resilience of one's own organisation is a key characteristic for compliance and for participation in the new digital economy.

Investing in cyber security is not just a cost. It is an investment in quality, which underlies new business model enablement, growth and profitability.

Digital Transformation Centre workshops

Our DTC is a purpose built space that uses digital content and tools and empowers organisations of all kinds to consider the future of their businesses and develop concepts that securely accelerate their digital transformation.

If you would like to know more about how Fujitsu can help you define the blueprint for your OT Security then contact us today to book a DTC session:

enterprisecybersecurity@uk.fujitsu.com

askfujitsu@uk.fujitsu.com
+44 (0) 1235 79 7711
Ref: 3953