



# **White Paper: Modern Managed Services as an enabler of safety-critical operations**

Focus on what matters to your stakeholders by leveraging trusted partnerships to deliver safety-compliant control centre solutions, networks support solutions and services.

## Abstract

Safety-critical control centre solutions and networks hinge on the technology solutions and services in place to deliver messages when it matters. With the increasing integration of Information Technology (IT) and Operational Technology (OT), and the rapid pace of innovation in communications solutions, it is more crucial than ever to have the right services in place to support safety-critical and -compliant communications.

Challenges in terms of aligning IT and OT, responding to the ever-evolving regulatory landscape, managing physical security, preventing data breaches, and maintaining service levels and performance are increasingly front-of-mind for executives leading communications-critical organisations.

There are many delivery models that can be used to address these issues, including self-managed, outsourced, 'as-a-Service', and Managed Services solutions. With each having strengths and weaknesses, it can be difficult to understand what will work best in the connected, contemporary communications environment.

Modern Managed Services look to the strengths of each of these models and integrate them into a new, future-ready solution to support mission-critical communications.


With a capable, trusted partner delivering Modern Managed Services, organisations can simplify the approach to successfully supporting mission-critical communications. By establishing a close relationship with a trusted delivery partner that has the domain expertise, experience, trust of clients, global footprint, and capabilities across industries, organisations can focus on their core business and what really matters to their stakeholders.

## The current IT-OT convergence challenge

Control centre solutions and network technology matters more than ever in our increasingly connected and 'on-demand' global society. Many organisations with safety-critical communication requirements rely on OT solutions to deliver messages when it matters most.

OT includes the hardware and software that monitors and manages physical equipment and processes across an organisation. While OT solutions take many forms, including Industrial Control Systems, Supervisor Control and Data Acquisition (SCADA), and Voice Communications and Control Systems, they share common support, maintenance and management requirements across organisations. This extends to the commonality of OT management challenges across sectors, including Air Traffic Management, Public Safety, Defence, Public Transport and Maritime Shipping.

Separately, these same organisations have dedicated IT teams to oversee technology service management and service delivery, the practice known as IT Service Management (ITSM). Historically, IT and OT teams within many organisations have worked separately to support technology solutions, including those technology systems designed to deliver safety-critical communications. This separation of support teams is increasingly outdated in the new era of ubiquitous communication solutions and services, leading to degraded service levels, increased safety risks, lower solution performance, and increased support complexity for OT systems.



Previously isolated OT systems are becoming open, connected systems that leverage IT components. These integrated communications systems demand sophisticated ITSM support services and service integration. This further increases the interdependency between IT and OT, and the need for both areas to be seamlessly integrated to support these open, connected systems.

Ultimately, this context arises because classic OT organisations have worked with closed systems in the past, to some extent due to regulatory directives to ensure IT-OT network separation. IT organisations on the other hand usually have little experience with industrial systems teams. Both areas therefore still generally work in silos, rather than together.

There are therefore several specific challenges for IT and OT teams to jointly work through in any organisation that seeks comprehensive support for its safety-critical, integrated communication technologies.

These specific challenges include:

» **Difference in solution and service lifecycle**

The typical IT investment timeframe is three (3) to five (5) years, whereas OT systems typically span a 10- to 15- year timeframe. Aligning service management, particularly maintenance and asset lifecycle management, over this timeframe demands the balance of competing forces.

» **Security risks impacting safety**

Threats to safety are not a new concern to OT teams; they've been implementing safety measures into industrial systems for decades. However, OT teams are now facing threats that are potentially outside of their control. Integrating machines and control systems to ubiquitous IT systems introduces a safety threat due to security-compromised components, which could potentially injure or cause death to individuals (e.g. false alarm on drone intrusion into airport-related airspaces; disruption of communication between operations control centre and emergency services; breach of data integrity; lack of system resilience).

» **Loss of productivity and quality**

Losing control of communications processes or related devices is any OT team's worst nightmare. Security breaches impacting on the organisation's critical components can quickly impair productivity and service levels, in addition to dramatically reducing production quality, resulting in significant loss of revenue and potentially even indemnification payments.

» **Data leaks**

While data breaches have long been a significant concern for traditional IT teams, they are somewhat new territory to OT teams that are used to working with closed systems. Given the nature of the types of open, connected industrial systems that are coming online, such as utilities, aviation and manufacturing, it is critical to ensure the privacy of transmitted data throughout the entire safety-critical environment.

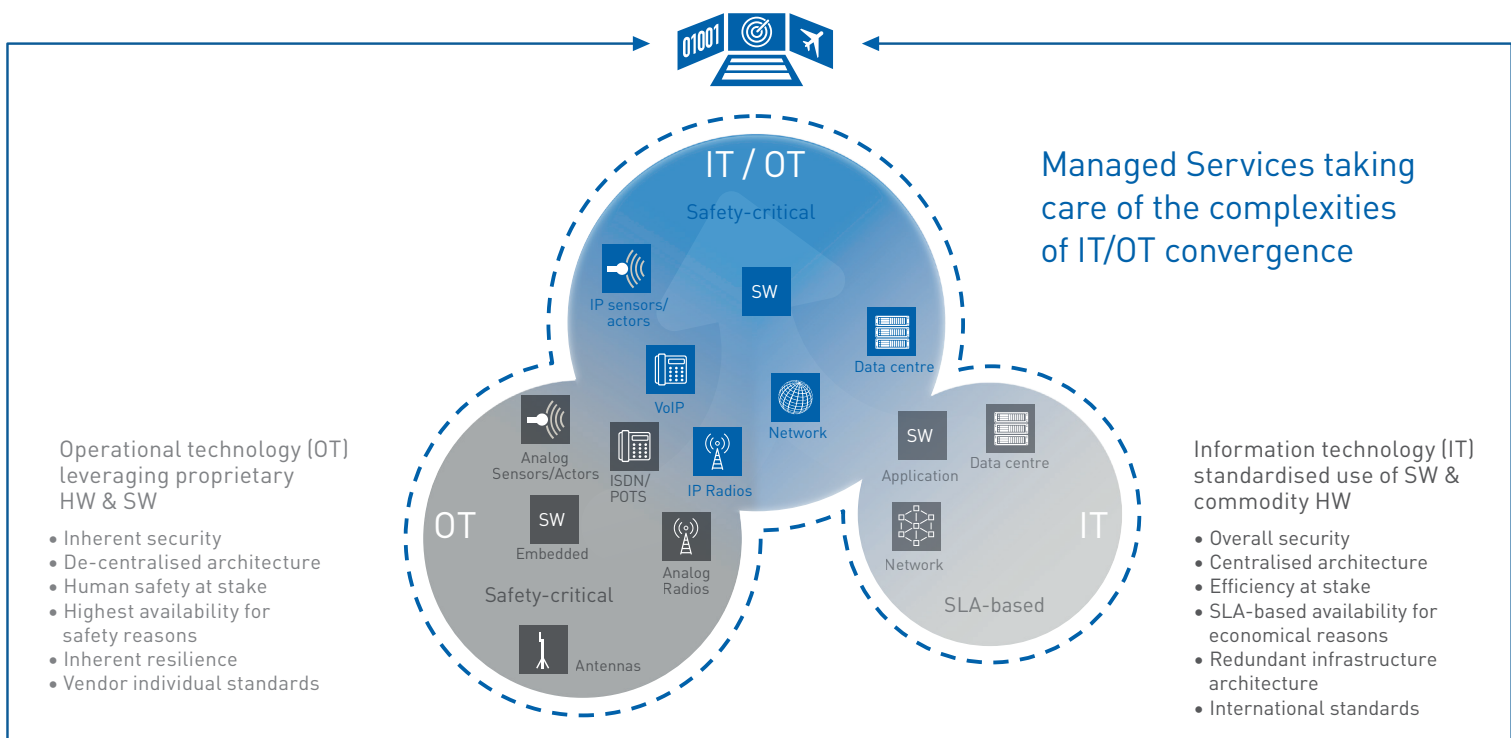
## » Working together with IT

One of the more unexpected concerns for OT teams is how to work with IT to solve security threats when IT teams generally have little experience with industrial systems, manage different approaches to resilience in IT and OT contexts, and typically use traditional IT security solutions that aren't compatible with safety-centric legacy control systems. While many OT leaders see the benefits of moving to open, connected systems that deliver higher performance and new opportunities to connect, the perceived lack of experience and potential solutions on the IT side means that security concerns persist, causing some resistance.

## » Standards and regulations

The regulatory and standards landscape for technology is rapidly growing in complexity, for both the IT and OT. This is evident in:

- varying regulatory frameworks across countries;
- increased focus on privacy and security at national and supra-national levels;
- differences and sheer scale of standards frameworks across standards organisations (e.g. ISO, NIST, EU Standards, Standards Australia) and regulators (e.g. ICAO); and
- the delicate balance between safety (which demands transparency to create trust and is generally the domain of OT systems) and security (which places limitations on access to and between systems per the classical Confidentiality-Integrity-Availability [CIA] triad, and is generally an IT-driven function).



Alignment and compliance with all of these requirements is difficult and expensive for even the largest, best-resourced global organisations, let alone organisations without these same economic advantages in-house.

#### » **Rapid evolution of technology**

Both IT and OT technologies are evolving and spreading across all areas of the organisation more rapidly than ever before. There is enormous value to be driven out of smart investments into these new solutions. However, being able to review, evaluate and adopt these in isolation without expert insight can be extremely challenging.

The challenges of converging IT and OT systems and solutions extend beyond these key items and demand careful attention in today's mission-critical communications world.

## **Core capabilities required**

Addressing the abovementioned issues of complex, integrated and evolving IT-OT systems is possible with coverage of the right capability areas. Certain capability areas of focus can help organisations address these challenges.

#### » **Technology**

- Bring a 'digital services' and 'design-thinking' mindset to developing integrated IT-OT solutions;
- Aligning the very different systems' lifespans and lifecycle approaches across IT and OT, and maintaining and refining this alignment over time;
- Creating a balance between the competing demands for safety-driven OT systems, and security-driven IT services and functions;
- Implementation, ongoing use and maintenance of fit-for-purpose monitoring systems and solutions across IT and OT components; and

- Embedding resilience, redundancy, and recoverability into the design and operations of IT-OT integrated systems.

#### » **Processes**

- Matured ITSM that considers the nexus of IT and OT solution and service components and their configuration;
- Carefully orchestrated change and release management capability, which includes IT and OT focus on release planning, testing, and continuity management; and
- Leveraging partnerships with key vendors to the benefit of service and solution performance, quality of service, and access to market and technology insights and leading practice.

#### » **Human skills**

- Maintaining adequate (and mandatory) training on a rolling basis for staff, including cross-training IT and OT talent, and
- Ability to take a partnering approach with business and other end-users of integrated solutions to enable continued innovation and alignment of solutions to requirements.

Getting these aspects right can support seamless integration between IT and OT systems, while also addressing the challenges of managing these types of integrated, 'open' solutions. Integrating IT and OT teams and components while simultaneously addressing the key convergence challenges set out above is demonstrably complex. It is therefore unsurprising that many organisations with safety-critical communications solutions look to trusted partners to deliver solution services, allowing the customer to focus on their core business.

## Partnering to let you focus on the core

There are a range of service, commercial and partnering models that are typically used where an organisation chooses to engage a specialist provider to supply safety-critical communications solutions spanning IT and OT.

The table below sets out the most widely utilised models, along with their core characteristics, and relative strengths and weaknesses.

Every model has strengths and weaknesses in any given context. Typically, we find that communications-critical businesses prefer a managed services model as it allows retention of asset ownership that lowers lifecycle Total Cost of Ownership (TCO), while also leveraging a capable partner with industrialised processes, regulatory compliance capabilities and commercial offerings, and insights to drive high quality of service.

By working in a shared partnership that clearly delineates roles and responsibilities, it is easier for the customer to manage and direct resources, and control and mitigate delivery risk.

Model	Description	Internal	Shared	External
		Own service design Own service responsibility Costs distributed across organisation		Contractually agreed service scope Contractually agreed service levels Contractually agreed service costs
Self-managed/ in-house	Solution owned wholly by the customer, with vendor(s) only providing detailed support on an as-needed basis			
Managed Service	Solution owned by the customer or the vendor with shared customer-vendor responsibility for operations and support; good optionality in asset ownership and capital investment			
Outsourcing	Full handover of solution and activities to a service provider, managed by a performance-driven commercial model; some optionality in asset ownership and capital investment			
As-a-Service	A 'subscription-based' delivery and commercial model, where the customer consumes a vendor's standardised service and pays only for consumption; moves spend from CAPEX to OPEX			



## Partnering for your organisational success

Using the new opportunities of open, integrated IT-OT systems while also managing the accompanying challenges requires capabilities and partnerships that can 'bridge the gap'. Frequentis has been delivering comprehensive solutions for a safer world for decades. These include managed services that remove the difficulties set out in this paper and enable simplified, trusted, and seamless services for customers.

By bringing together our global capabilities and experience in services management, maintenance solutions, technical operation solutions, lifecycle services solutions, along with our enabling services and our partner network, Frequentis proactively simplifies, modernises and supports your safety-critical communications systems.

For more information regarding our service catalogue, please visit:

<https://www.frequentis.com/modern-managed-services>

### FREQUENTIS AG

Innovationsstraße 1  
1100 Vienna, Austria  
Tel: +43-1-811 50-0  
[www.frequentis.com](http://www.frequentis.com)

The information contained in this publication is for general information purposes only. The technical specifications and requirements are correct at the time of publication. Frequentis accepts no liability for any error or omission. Typing and printing errors reserved. The information in this publication may not be used without the express written permission of the copyright holder.