INDUSTRIAL CONTROL SYSTEMS Community of Interest

Bringing together NCSC guidance, standards and CAF for Industrial Control Systems / Operational Technology environments

Aims of this guidance

This guidance is designed to help organisations with architectural considerations for securing their Industrial Control Systems (ICS)/Operational Technology (OT) environments and ultimately gain assurance on the cyber security maturity of their environments.

It has been designed to complement a range of NCSC generic architectural guidance, while focusing on the specific and unique aspects relating to ICS/OT, to support other ICS/OT focused guidance developed by the ICS COI. This article tries to bring together architecture design considerations from NCSC guidance, the Purdue Model, IEC62443 standards and NCSC's Cyber Assessment Framework CAF), all of which come into consideration by UK Critical National Infrastructure (CNI) Operators when they are securing their ICS/OT environments.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.*

Who is this guidance for?

If you are responsible for the cyber security of ICS/OT environments this article is designed to provide you with architectural insights to enhance the cyber security maturity of your environment.

Executive Summary

This document outlines a set of principles and metrics that can be applied to build a secure architecture for ICS/OT systems in Critical National Infrastructure (CNI) sectors, and other sectors who wish to use a best practice approach.

Introduction

ICS/OT systems are critical for the functioning of CNI sectors such as energy, water, transportation, finance and healthcare. With the increasing convergence of ICS/OT and Information Technology (IT) networks, these systems are exposed to new cyber threats, making robust security architectures essential for safeguarding them.

ICS/OT environments in the likes of factories, energy grids and water treatment plants have not traditionally been designed with cyber security in mind but with operational continuity. Often, cyber security is seen as a late-stage addition to the design mix at best or a retrograde addition at worst, inevitably leading to compromises and limitations in defence capability.

In recent years, there has been an increasing trend to transfer ownership of cyber security from ICS/OT operations departments to IT departments as organisations have become aware of the increasing number and sophistication of attacks in the ICS/OT domains. This transfer has not always gone smoothly - in many organisations, ICS/OT operations have been distrustful of IT departments and have often accused them of "not getting it" when it comes to service requirements. Likewise, many IT departments recognise the specialist knowledge ICS/OT Operation departments has but a wary of those who will compromise security every time in favour of service availability. Achieving balance and gaining benefit from close cooperation, knowledge and skills transfer usually achieves the best outcome for the business.

There is also a shift into the cyber security for ICS/OT environments to IT which is offshored which also causes some challenges as support and decisions are made thousands of miles away from the plant.

Design Solution

One of the key challenges in building reference architectures and 'gold standard' models for securing ICS/OT environments is the varying approaches, requirements and risk appetite across the different organisations and industry sectors that deploy and use ICS/OT. It is also true that many organisations are not truly aware just how much ICS/OT is in use in their organisations - a bank for example may not consider it is a user of ICS/OT, yet their data centres are critically dependent on cooling from Heating, Ventilation, and Air Conditioning (HVAC) systems, controlled by ICS/OT, elevators in their offices are moved by ICS/OT, personnel physical access, controlled by proximity or swipe badges, managed by its close cousin, the Internet of Things (IoT), video cameras monitoring buildings is also IoT, so there is a valid argument that in fact every organisation uses ICS/OT in their business in one form or another. The aim of this document is to build a set of guiding principles that can be applied in the context of each application of ICS/OT deployment and factor in the variables as highlighted above, allowing organisations to build a pro-active and considered approach to cyber risk management.

ICS/OT Cyber Security Principles

Secure systems are grounded in good design principles, and NCSC outlines cyber security principles, and ICS/OT design principles, which when followed can lead to better security outcomes for your organisation as a whole.

The following principles should be considered when building an ICS/OT architecture:

NCSC Cyber Security Principles:

- Establish the Context Before Designing a System
- Make Compromise Difficult
- Make Disruption Difficult
- Make Compromise Detection Easier
- Reduce the Impact of Compromise
- Good security culture
- Asset & network visibility

In addition, the following principles are deemed relevant when building an ICS/OT architecture:

- Establishing defensible networks**:** It's vital that attackers don't have the keys to the kingdom once they breach your perimeter. This is of particular importance if you employ new era techniques such as Zero Trust Networks (ZTN) or Privileged Access Management (PAM). These techniques tend to try to place all the keys to the kingdom in one place- and attacks such as the US treasury attack show the risks associated with this. Always consider what protection you would be left with if a control fails and where possible try to ensure a second, diverse mechanism exists. Design and implement segmented network

architectures to limit the spread of threats across ICS/OT environments. Employ layered defence mechanisms, such as firewalls, intrusion detection systems (IDS), and demilitarised zones (DMZs), to create zones of trust. Enforce strict access controls and least privilege principles for users and devices within critical network segments and regularly test and validate network defences to ensure resilience against evolving threats.

- **Detect and respond to threats:** While hardening against threats is always preferred, we must also accept that some may get through. Thus, having a good strategy for effective detection and response to threats is key. Ensure you have effective intrusion detection and if possible, prevention systems in play that are ICS/OT-specific. Incorporate anomaly detection tools to identify deviations from normal activities that may indicate threats. Leverage high-fidelity alerting systems to ensure that only actionable threats are escalated to incident responders, ensuring your teams are not overwhelmed. Reduce the Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) to ICS/OT-specific threats by deploying advanced analytics and automation. Integrate deception technologies such as honeypots to attract and analyse malicious activity, helping you build a database of behaviours to reduce false positives. Lastly, build comprehensive incident response playbooks tailored to ICS/OT environments, ensuring readiness for diverse scenarios.
- **Leverage information through integrated tooling:** Managing your cyber-exposure is the name of the game, and to do this effectively, you need to integrate your data sources so that threats can be modelled, detected, remediated and learned from. Prioritise solutions that integrate efficiently to reduce software sprawl and enhance operational efficacy. Establish centralised management and data sharing to ensure a unified security posture across both IT and ICS/OT domains. Facilitate integration of threat intelligence platforms to share context-rich data for informed decision-making.
- **Improve security posture through clear policies and procedures:** Policies help organisations develop the 'muscle memory' to ensure they practice cyber-hygiene and know how to quickly and effectively respond should an incident occur. Develop and enforce robust security policies tailored to the unique demands of ICS/OT environments. Clearly define roles and responsibilities for security management, ensuring alignment with broader organizational governance structures. Establish procedures for vulnerability management, patch deployment, and configuration control, considering ICS/OT system constraints. Conduct regular reviews and updates of policies to address emerging threats, regulatory changes, and technological advancements. Ensuring alignment with international standards and frameworks such as NIST, IEC 62443, and ISO 27001 will also help with audits and regulatory requirements.
- **Ability to respond and recover from an incident:** Given some ICS/OT environments are a challenging landscape, with poor patching, few maintenance windows, having to manage a range of vulnerable and probably legacy assets, compromise is quite possible. So being resilient with the ability to quickly respond and recover is critical.
- **Employ Formal Assurance**: This is mandatory for some applications, but it's value should not be restricted merely to cases where there are statutory or legal requirements. More companies are requiring cyber insurance from their supply chain which may provide some recompense after the event- but consider that good assurance could prevent the event occurring. Consider clauses requiring solutions providers of architecture to work to IEC

62443. Then jointly or independently employ a third-party conformity assessment body who is recognised to a standard such as ISO/IEC 17065/ UKAS.

Avoiding pitfalls

When designing security architectures, there are some common pitfalls organisations make that can compromise security. NCSC refer to these as "Anti-patterns". Avoiding the following Anti-Patterns identified by NCSC is essential for creating secure and resilient ICS/OT environments.

- Anti-pattern 1: 'Browse-up' for Administration
- Anti-pattern 2: Management Bypass
- Anti-pattern 3: Back-to-Back Firewalls
- Anti-Pattern 4: Building An 'On-Prem' Solution In The Cloud
- Anti-pattern 5: Uncontrolled and Unobserved Third-Party Access
- Anti-pattern 6: The Un-patchable System

ICS/OT Architecture Frameworks and Security Models

Reference models serve as conceptual frameworks that outline the components, layers, and functionalities essential for securing industrial systems and networks. These models provide a structured approach to designing, implementing, and managing secure ICS/OT environments, enabling organisations to systematically address complex security challenges. By leveraging reference models, stakeholders can ensure a consistent and comprehensive approach to cybersecurity across different sectors and technologies.

Models are typically designed to align with established cybersecurity standards and best practices, such as IEC 62443, NIST guidelines, and the NCSC's advice. This alignment ensures that the models incorporate a comprehensive set of security controls and measures that are widely recognized and respected in the industry.

While reference models provide a general framework for ICS/OT security, they also offer the flexibility to be tailored for different sectors. Such sector-specific models take into account the unique operational processes, technologies, and risk profiles of each domain, enabling more effective and relevant security strategies.

Reference models can incorporate risk management processes and resilience strategies into their frameworks. This includes mechanisms for identifying and assessing risks, implementing protective measures, detecting and responding to incidents, and recovering from disruptions.

Lastly, reference models are central in enhancing collaboration and communication among system operators, vendors, regulators, and cybersecurity professionals. By providing a common language and understanding of security principles and practices, models facilitate more effective cooperation and coordination in addressing cybersecurity challenges.

Purdue Model

The **Purdue Enterprise Reference Architecture (PERA)**—commonly known as the **Purdue Model**—was developed in the 1990s by The Purdue University Consortium for Integrated Manufacturing Systems, led by Theodore J. Williams, a professor at Purdue University.

Although the Purdue model is not a true Cyber Security model, it is useful as an architectural framework to guide the design and organisation of ICS/OT environments and their cybersecurity measures. The Purdue Model provides a hierarchical blueprint that categorises the elements of industrial control and information systems into distinct layers, from physical processes to enterprise-level planning and scheduling.

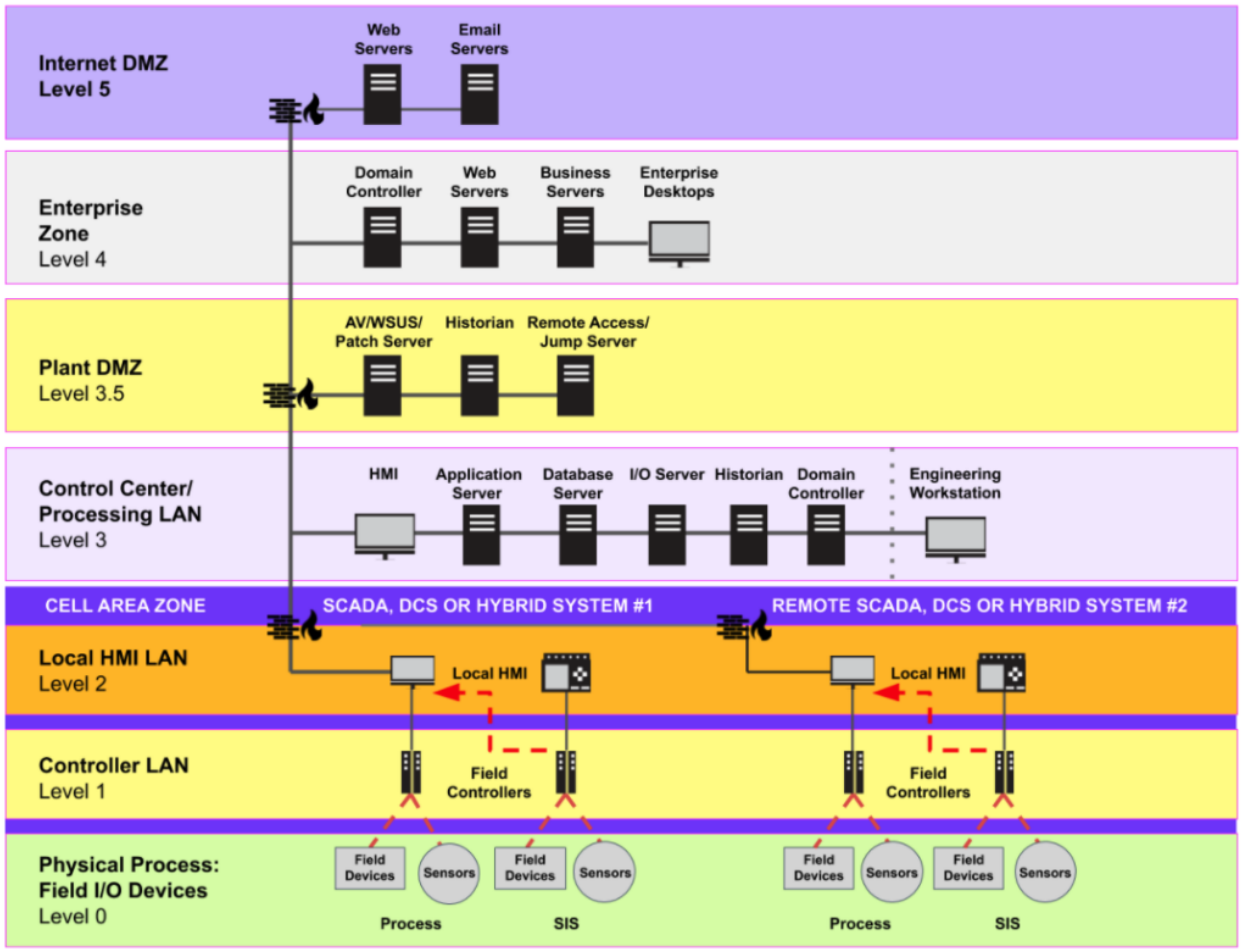

Figure 1- Purdue Model

The Purdue Model divides industrial networks into several levels, starting from Level 0, which represents the physical process, up to Level 5, which is the enterprise level. These levels are:

- **Level 0: Physical Process** - The actual process occurs in level 0. The devices in this level are also known as Equipment Under Control (EUC). We can find sensors, actuators, pumps, motors and valves in level 0, facilitating movement, heating, mixing, etc

- **Level 1: Basic Control** - All controlling equipment are present in level 1. The devices and systems present in this level provide automated control of a process. Devices found in level 1 include PLCs, PIDs, etc.

- **Level 2:** Area Supervisory Control - Systems that provide supervisory control, data acquisition, and visualisation tools for managing the process control level

- **Level 3: Site Operations** - Systems responsible for production scheduling, batch management, and operational-level optimisation. This level bridges the gap between plant control and business systems

- **Level 4: Enterprise Management** - The business and enterprise systems that do not directly interact with the production process, focusing on tasks like inventory management, order processing, and financial planning

- **Level 5: Enterprise Planning and Logistics** - The highest level, focusing on interactions outside the organisation, including sales, distribution, and supply chain management

The Purdue Model remains useful today as it helps architects categorise functional elements in network systems, their likely risk exposure, typical security requirements and likely incident impact.

The Purdue Model is foundational in understanding and securing industrial control systems for several reasons:

- **Segregation and Defence in Depth:** By defining distinct layers within an industrial environment, the Purdue Model facilitates the implementation of layered security measures. This segregation helps in applying appropriate security controls tailored to each layer, enhancing the overall security posture through a defence-in-depth strategy.
- **Communication and Data Flow Control:** The model outlines how data should flow between different levels, which is crucial for implementing secure communication protocols and controlling access to sensitive information and systems. It aids in the design of network segmentation strategies, reducing the attack surface and containing potential breaches.
- **Risk Management:** Understanding the functions and interactions of different levels allows organisations to perform more accurate risk assessments. Identifying critical assets and their connections within the architecture helps prioritise security efforts and resource allocation.
- **Compliance and Best Practices:** The Purdue Model aligns well with industry standards such as IEC 62443, providing a structured approach to compliance. Its widespread

recognition and adoption make it a valuable reference point for developing policies, procedures, and technical measures that meet or exceed regulatory requirements.

The Purdue Model applies best to traditional ICS/OT network systems that are designed to operate hierarchically. Its clear delineation of industrial network layers helps organisations design, secure, and manage their control systems effectively. It is of less value in guiding the design of modern "Industry 4.0" environments that make extensive use of IIoT and Cloud, elements and publisher/subscriber concepts.

For these environments, the IEC 62443 zones and conduits model provides a better fit for managing risk exposure, definition of security level and corresponding security controls.

IEC 62443

IEC 62443 is a series of international standards for Industrial Automation and Control Systems (IACS) cybersecurity. It provides a framework to address security vulnerabilities in industrial control systems across various sectors including manufacturing, power generation, and critical infrastructure.

Key features include: A risk-based approach to security, definition of four security levels (SL1-SL4) for increasing security capability, guidance for both technical and organizational security measures and requirements for secure development lifecycle for control system products.

The standard consists of several parts organised into four main categories detailed in the image below:

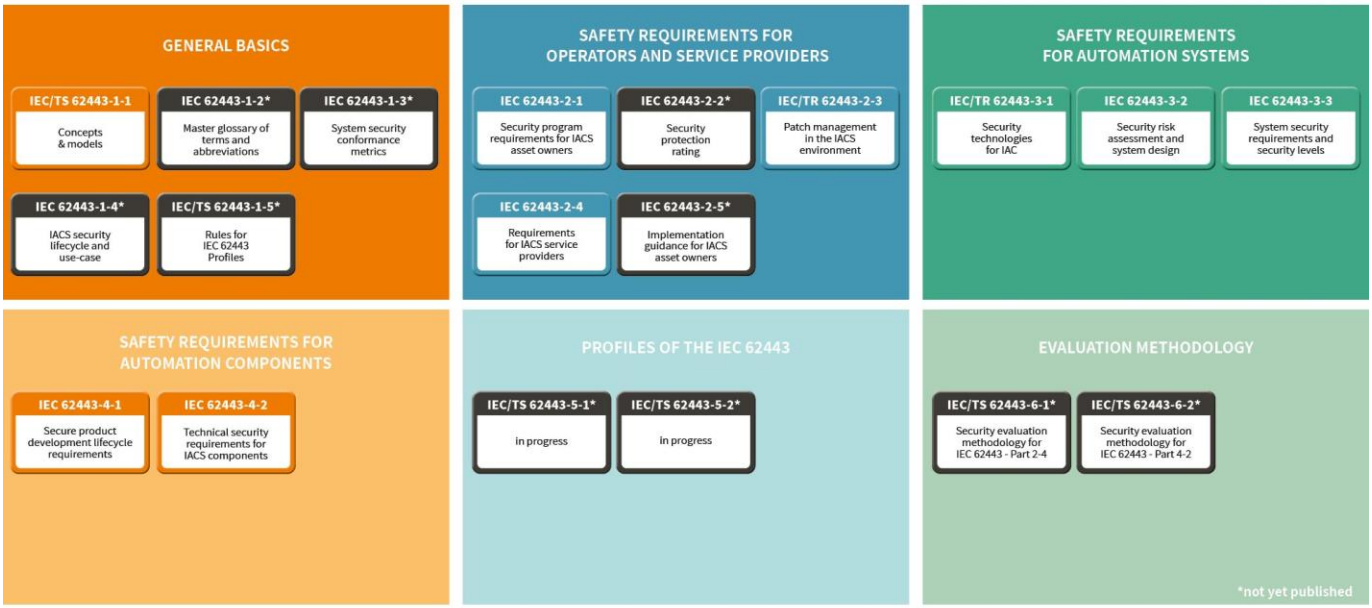

Figure 2 - IEC62443 categories

IEC 62443 has become the globally recognised standard for industrial cybersecurity, helping organisations establish systematic protection against cyber threats in operational technology environments.

General Concepts (IEC 62443-1-X Series)

Provides the foundational framework for the entire standard, establishing consistent terminology, models, and methodologies that apply across all aspects of industrial control system security. This category creates a common language and conceptual basis that enables stakeholders to communicate effectively about security concerns, ensuring that everyone from manufacturers to end users can align their understanding of threats, vulnerabilities, and security requirements.

Section Documents:

- **IEC 62443-1-1**: Establishes core terminology, concepts, and models for the entire standard
- **IEC 62443-1-2**: Master glossary of terms and abbreviations
- **IEC 62443-1-3**: System security compliance metrics
- **IEC 62443-1-4**: IACS security lifecycle and use cases

Policies & Procedures (IEC 62443-2-X Series)

Focuses on the operational and organisational aspects of security, targeting asset owners and those responsible for implementing and maintaining secure industrial environments. This category outlines requirements for establishing comprehensive security programs, including governance structures, risk assessment methodologies, incident response protocols, and patch management processes, essentially providing the blueprint for how organisations should manage security throughout the lifecycle of their industrial automation and control systems.

Section Documents:

- **IEC 62443-2-1**: Requirements for an IACS security management system, including risk assessment, security policy, and organisational structure
- **IEC 62443-2-2**: Guidance on how to implement specific requirements from 2-1
- **IEC 62443-2-3**: Patch management requirements in the IACS environment
- **IEC 62443-2-4**: Requirements for service providers who integrate and maintain IACS systems

System Requirements (IEC 62443-3-X Series)

Addresses the technical security requirements at the system level, providing guidance on how to design and implement secure industrial control architectures. This category introduces the concept of security zones and conduits for network segmentation, defines the seven fundamental

requirements (FRs) for secure systems, and establishes the framework for the four security levels (SL1-SL4) that allow organisations to implement security controls proportional to the assessed risk, creating a systematic approach to securing entire industrial control systems against cyber threats

Section Documents:

- **IEC 62443-3-1**: Security technologies for IACS
- **IEC 62443-3-2**: Security risk assessment and system design for IACS
- **IEC 62443-3-3**: Detailed technical system security requirements and security levels

Component Requirements (IEC 62443-4-X Series)

Drills down to the individual component level, specifying security requirements for products used within industrial automation and control systems. This category establishes requirements for secure product development lifecycles that manufacturers should follow and defines specific technical security capabilities that components must possess to achieve different security levels, ensuring that security is built into the fundamental building blocks of industrial systems rather than added as an afterthought.

Section Documents:

- **IEC 62443-4-1**: Requirements for secure product development lifecycle for IACS products
- **IEC 62443-4-2**: Technical requirements for IACS components (control systems, applications, host devices, and embedded devices)

Each category addresses different stakeholders in the industrial ecosystem: general users, asset owners, system integrators, and product suppliers, respectively.

Component Requirements (IEC 62443-6-X Series)

The IEC 62443-6-X series does not define component requirements. These specifications are technical reports that establish an evaluation methodology to assess conformance with other standards in the series. The actual requirements for components in industrial automation and control systems (IACS) are specified in the IEC 62443-4-2 or IEC 62443 2-4 standard.

Section Documents:

- **IEC 62443-6-1**: Specifies the evaluation methodology to determine if an IACS service provider conforms with the requirements found in IEC 62443-2-4.
- **IEC 62443-6-2**: Specifies the evaluation methodology to determine if an IACS component meets the technical requirements of IEC 62443-4-2.

IEC 62443 Security Levels (SL1-SL4)

Security Levels (SL) in IEC 62443 define graduated levels of security capability designed to protect against attackers with different levels of motivation, resources, and skills. Each level builds upon the previous one, establishing increasingly robust security measures:

Figure 3 - IEC62443 SL Levels

SL1 - Basic Protection: Provides protection against casual or coincidental violations. It defends against attackers with low resources, generic skills, and low motivation, typically using simple means with little effort. SL1 implements basic security measures such as password authentication, minimal network segmentation, and essential security policies. This level is suitable for environments where security breaches would have limited impact.

SL2 - Intermediate Protection: Designed to defend against intentional violations using simple means with moderate resources, IACS-specific skills, and moderate motivation. SL2 implements stronger access controls, enhanced network segmentation, event logging, and basic encryption. This level addresses environments where security breaches could cause moderate operational or safety impacts but is insufficient for critical infrastructure protection.

SL3 - Advanced Protection: Provides defence against sophisticated attacks from highly motivated and well-funded adversaries possessing IACS-specific knowledge. SL3 implements robust authentication (often multi-factor), comprehensive network segmentation with deep packet inspection, sophisticated logging and monitoring, strong encryption, and formal security governance. This level is appropriate for critical systems where breaches could cause significant operational, financial, or safety impacts.

SL4 - Maximum Protection: The highest level of protection, designed to prevent sophisticated attacks from nation-states or highly motivated, well-resourced threat actors with extensive IACS-

specific expertise. SL4 implements state-of-the-art security controls with redundant protection mechanisms, real-time monitoring and response capabilities, rigorous change management, and extremely restricted connectivity. Hardware security modules might be required, and security is designed in from the beginning. This level is reserved for the most critical national infrastructure where breaches could cause catastrophic impacts.

Each security level can be specified differently across the three aspects:

- Target SL (SL-T): The desired security level based on risk assessment
- Capability SL (SL-C): The inherent security capability of a component or system
- Achieved SL (SL-A): The actual security level implemented after considering constraints

This framework allows organizations to make appropriate security investments proportional to their risk profile and system criticality.

Zone and Conduit Model

The Zone and Conduit model is a fundamental security architecture concept within IEC 62443, specifically detailed in the IEC 62443-3-3 standard. This model provides a structured approach to network segmentation and defence-in-depth for industrial control systems.

Zones

A **zone** is defined as a grouping of logical or physical assets that share common security requirements. Zones are established based on:

- **Criticality**: Systems with similar importance to operations
- **Functional requirements**: Systems serving similar purposes
- **Security requirements**: Assets requiring similar protection levels
- **Physical/logical location**: Naturally grouped assets

Common zone types include:

- **Enterprise zone**: Business systems, office IT
- **Operations zone**: Manufacturing operations management systems
- **Control zone**: Process control systems (DCS, SCADA)
- **Safety zone**: Safety instrumented systems
- **Field zone**: Field devices, I/O, sensors, and actuators

Each zone is assigned a specific Security Level (SL) based on risk assessment, determining the security controls required.

Conduits

A **conduit** represents the communication pathway between zones or the communication channel within a zone. Conduits:

- Control and protect the flow of information between zones
- Implement security controls such as firewalls, data diodes, or gateways
- Are assigned their own Security Levels based on risk assessment
- Often represent the primary attack vectors and therefore require particular attention

Implementation Principles

Key principles of the Zone and Conduit model include: **Defence-in-depth**: Multiple layers of protection make attacks more difficult, **Least privilege**: Only necessary communication is permitted between zones, **Default deny**: All communication is blocked unless explicitly allowed, **Monitoring and control**: All traffic through conduits is monitored for security events and **Risk-based segmentation**: More critical zones receive higher protection levels

Zone And Conduit Model Benefits

- **Scalable security**: Can be applied to systems of any size or complexity
- **Systematic approach**: Provides a methodical framework for security design
- **Reduced attack surface**: Limits the impact of compromises to specific zones
- **Tailored security**: Allows security controls to be matched to specific risks
- **Simplified compliance**: Maps clearly to regulatory requirements

The Zone and Conduit model helps organisations implement practical industrial cybersecurity by breaking down complex environments into manageable segments with defined protection requirements, creating a structured approach to securing industrial control systems against increasingly sophisticated threats.

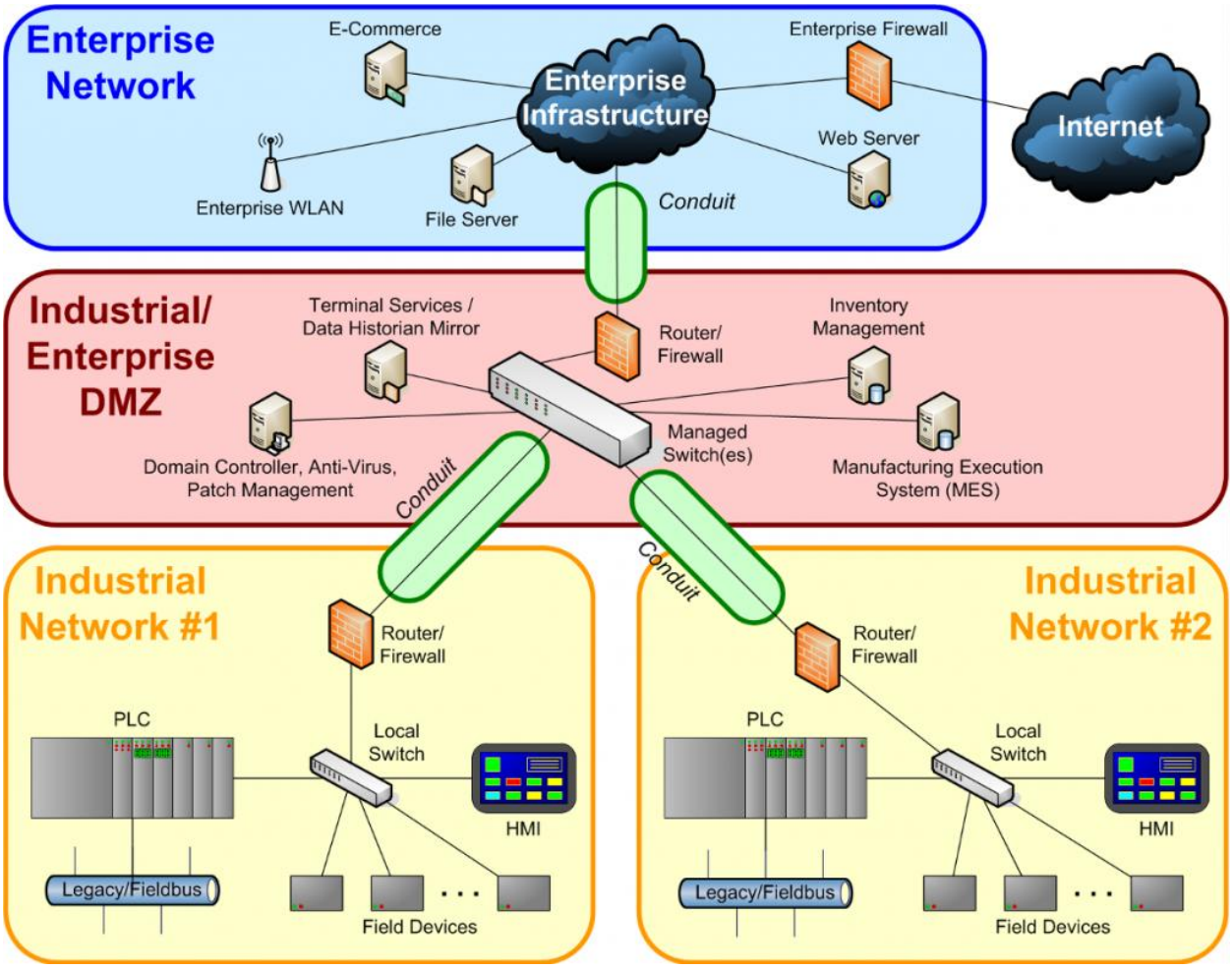

Figure 4 - IEC62443 - Zone and Conduit model

Cyber Assessment Framework (CAF) and Mapping to ICS/OT Security

The CAF provides a structured approach for assessing and improving cybersecurity for key UK stakeholders, such as Operators of Essential Services (OES) under the UK's NIS Regulations, Critical National Infrastructure (CNI) sectors such as energy, water, healthcare, and transportation, Public-sector bodies, including local councils and NHS organisations, and Suppliers and partners supporting regulated entities.

The reference architecture aligns with the CAF's four objectives:

- **CAF Objective A: Managing Security Risk:** ICS/OT systems should be designed with a comprehensive risk management process, identifying, assessing, and mitigating risks throughout the system lifecycle.
- **CAF Objective B: Protecting Against Cyber Attack**: Implementing protective controls that prevent cyber-attacks from succeeding, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and secure access controls.
- **CAF Objective C: Detecting Cyber Security Events:** The architecture must include mechanisms for real-time detection of cybersecurity events, supported by continuous monitoring and alerting systems.
- **CAF Objective D: Minimising the Impact of Cyber Security Incidents**: Systems should be designed to ensure resilience and quick recovery from cyber incidents, minimising their impact on operations.

Organisations can apply the CAF through self-assessment, to internally evaluate their cyber posture, and Regulatory assessment, submitting to evaluations by regulators or qualified third parties.

Design Summary

We have reviewed some key architectural frameworks: Purdue, IEC 62443, CAF. One take away is that all of them are useful. Borrow from each approach concepts that are useful, effective and efficient. Strive for prompt progress, not perfection as the ultimate security system that takes a year to implement is, not secure for a year.

We've listed below a series of imagined case studies, showing how organisations can apply the key NCSC principles and avoid pitfalls in doing so.

Case Studies

Energy Corp

Energy Corp is a large energy company responsible for generating and distributing electricity to millions of customers. Given the critical nature of its services, the company must ensure that its ICS/OT systems are secure, resilient, and capable of withstanding cyber threats.

It is important to note that there a range of additional IEC related standards specific to the energy sector. The IEC 62351 series was developed specifically for data and communications security within smart grids and power system management. It is designed to secure the communication protocols used for monitoring and controlling electrical infrastructure.

IEC 62351 complements IEC 62443 by focusing on securing protocol-level traffic. Key aspects include:

- **Encrypted communications:** Secures protocols like Manufacturing Message Specification (MMS), Generic Object-Oriented System Event (GOOSE), and Distributed Network Protocol 3 (DNP3).
- **Authentication:** Ensures the integrity and authenticity of messages to prevent injection or replay attacks.
- **Role-based access control:** Manages access to information infrastructure.

The IEC 61850 standard defines the communication protocols for intelligent electronic devices (IEDs) in electrical substations to enable interoperability. While IEC 61850 itself does not mandate security, the IEC 62351 series adds the necessary cybersecurity protections, such as authentication and digital signatures, to its protocols. In combination with the system-level protections from IEC 62443, these standards help create a secure environment for digital substations.

Applying NCSC Principles

Establish context	Energy Corp conducted a comprehensive risk assessment to understand the threat landscape, business needs, and regulatory requirements. They identified key assets, such as SCADA systems and power grid controllers, and addressed any gaps in current security measures.
Making compromise difficult	The company implemented strong authentication mechanisms, network segmentation, and encrypted communications across all ICS/OT systems. Least privilege principles were enforced to limit access to critical systems.
Making disruption difficult	Redundancy and fault-tolerant designs were incorporated into critical systems to ensure continuous availability. Backup power supplies and disaster recovery plans were also established to minimise downtime.

Making detection easier	Energy Corp deployed an advanced monitoring system that includes real-time anomaly detection and continuous logging. The system was designed to provide visibility into all critical operations, with alerts configured for immediate incident response.
Reducing the impact of compromise	Segmentation of the ICS/OT network ensured that any compromise was contained within a limited scope. The incident response plan was tailored to quickly isolate affected systems and restore normal operations with minimal disruption.

Avoiding Security Architecture Anti-Patterns

'Browse-up' for Administration	**Description:** Allowing administrators to use the same environment for both browsing the Internet and performing administrative tasks can lead to the exposure of critical systems to Internet-borne threats. **Mitigation:** Energy Corp prohibited the use of administrative accounts for browsing or non-essential tasks, ensuring that administrative actions were conducted in a dedicated, secure environment.
Management Bypass	**Description**: This Anti-Pattern involves creating alternative management routes that bypass security controls, which can be exploited by attackers to gain unauthorised access to critical systems. **Mitigation**: Energy Corp selected a privilege access management vendor to implement secure, controlled remote access and mediated privilege escalation and logging. Firewall rules were tightened to permit only PAM channels for management.
Back-to-Back Firewalls	**Description**: The practice of placing two firewalls from different vendors back-to-back under the assumption that it provides added security can lead to misconfigurations and reduced performance without a significant security gain. **Mitigation**: Instead of using back-to-back firewalls, Energy Corp focused on a layered defence strategy, combining properly configured firewalls with IDS/IPS and segmented networks.

Building an 'On-Prem' Solution in the Cloud	**Description**: Replicating on-premises security architecture in the cloud without considering cloud-specific threats and capabilities can lead to ineffective security controls and gaps. **Mitigation**: Energy Corp had specific substation requirements: 1) Security services must operate locally in the event of an interruption of cloud access (which can happen during a power cut. 2) Substations themselves must never be connected to cloud services. 3) Information destined for SAS applications can only be transmitted from the IT domain. By implementing a suitable hybrid cloud/on-prem architecture Energy Corp gained the benefits of cloud-based analytics without compromising operational security.
Uncontrolled and Unobserved Third-Party Access	**Description**: Allowing third-party vendors to access critical systems without sufficient oversight can lead to security breaches, as these access points are often less controlled and monitored. **Mitigation**: Substations were inspected for third-party modems and communications devices, and these were either removed or exceptions made where necessary. All third parties were required to use the PAM, with defined third party-tagged accounts.
The Un-patchable System	**Description**: Systems that cannot be patched due to operational constraints, compatibility issues, or other reasons are vulnerable to exploitation over time as new vulnerabilities are discovered. **Mitigation**: Energy Corp implemented a system to monitor for end-of-life and created a proactive maintenance program for advance replacement of these systems. For systems within spec, architectural changes were made to ensure systems could be taken off line and patched without interruption of customer service. Energy Corp also implemented an attack path analysis tool to identify methods of access to critical resources and the means to reduce their exposure.

Aligning with CAF Objectives

Managing Security Risk	Energy Corp continuously assessed and managed security risks through regular audits and updates to its security policies.
Protecting Against Cyber Attack	The architecture included multiple layers of protection, including firewalls, encrypted communications, and secure access controls, to defend against potential cyber-attacks.
Detecting Cyber Security Events	Advanced monitoring systems provided real-time detection of cybersecurity events, enabling a swift response to any incidents.

Minimising the Impact of Cyber Security Incidents	The company's robust incident response plans ensured that any cyber incidents were quickly contained and resolved, minimizing their impact on production.

Chem Corp

Chem Corp is a global chemical manufacturer producing a wide range of industrial chemicals, including hazardous materials. The company's ICS/OT systems manage critical processes such as chemical synthesis, storage, and distribution. Given the nature of its operations, Chem Corp must ensure that its ICS/OT systems are secure, not only to protect its business but also to prevent environmental and safety hazards.

It is important to note that for the chemical sector, the Health and Safety Executive (HSE) , utilise OG86 as operational guidance that outlines the minimum requirements for cyber security in Industrial Automation and Control Systems (IACS) for major accident hazard sites and essential services. It is considered a benchmark for managing cyber risks in ICS/OT environments to prevent health and safety incidents and major accidents, and is aligned closely with NCSC's CAF.

Applying NCSC Principles

Establish context	Chem Corp conducted a risk assessment to understand the specific threats facing its ICS/OT systems, including sabotage, theft of intellectual property, and environmental hazards. The company engaged with stakeholders from safety, IT, and production departments to ensure that all perspectives were considered in the security design.
Making compromise difficult	To secure its ICS/OT systems, Chem Corp implemented a range of controls, including strong authentication, role-based access control (RBAC), and encrypted communications. The company also deployed physical security measures, such as secure access to critical control rooms and surveillance systems, to prevent unauthorized physical access.
Making disruption difficult	Redundancy and fault-tolerant designs were incorporated into critical systems, such as chemical reactors and storage facilities, to ensure continuous operation. Chem Corp also developed comprehensive disaster recovery plans, including backup systems and emergency shutdown procedures, to minimize the impact of any disruption.
Making detection easier	Chem Corp deployed real-time monitoring tools with a focus on detecting anomalies in process control systems. Any deviations from expected process parameters, such as reagent mix, pH, temperature or pressure changes, were flagged for immediate investigation. The company also upgraded automated safety systems that could trigger alarms or shutdowns in the event of a detected compromise.

Reducing the impact of compromise	By segmenting its ICS/OT network and isolating hazardous processes, Chem Corp ensured that any compromise would be contained and managed without risking widespread impact. The company's incident response plan was designed to prioritize the safety of personnel and the environment, with rapid containment and recovery procedures in place.

Avoiding Security Architecture Anti-Patterns

'Browse-up' for Administration	**Description**: Allowing administrators to use the same environment for both browsing the internet and performing administrative tasks can lead to the exposure of critical systems to internet-borne threats. **Mitigation**: Chem Corp ensured that administrative actions were performed in secure, isolated environments, with no browsing or other non-essential activities allowed on administrative accounts.
Management Bypass	**Description**: This Anti-Pattern involves creating alternative management routes that bypass security controls, which can be exploited by attackers to gain unauthorized access to critical systems. **Mitigation**: All management interfaces were integrated into the overall security architecture and secured with multi-factor authentication, reducing the likelihood of any bypass of security controls.
Back-to-Back Firewalls	**Description**: The practice of placing two firewalls from different vendors back-to-back under the assumption that it provides added security can lead to misconfigurations and reduced performance without a significant security gain. **Mitigation**: Chem Corp implemented a layered security approach rather than relying on back-to-back firewalls, using network segmentation and IDS/IPS to enhance security. They did consider back-to-back firewalls for segregation of duties between the IT and ICS/OT teams, however in this case, decided not to implement.
Building an 'On-Prem' Solution in the Cloud	**Description**: Replicating on-premises security architecture in the cloud without considering cloud-specific threats and capabilities can lead to ineffective security controls and gaps. **Mitigation**: The company adopted cloud-native security practices for its cloud deployments, ensuring that security controls were optimized for the cloud environment.

Uncontrolled and Unobserved Third-Party Access	**Description**: Allowing third-party vendors to access critical systems without sufficient oversight can lead to security breaches, as these access points are often less controlled and monitored. **Mitigation**: Third-party access was tightly controlled, with comprehensive logging and monitoring to ensure that all activities were observed and secured.
The Un-patchable System	**Description**: Systems that cannot be patched due to operational constraints, compatibility issues, or other reasons are vulnerable to exploitation over time as new vulnerabilities are discovered. **Mitigation**: Chem Corp designed their architecture for frequent updates and patches, using network isolation and other controls to protect systems that could not be patched.

Aligning with CAF Objectives

Managing Security Risk	Chem Corp continuously managed security risks through regular audits, risk assessments, and updates to security policies. They also upgraded their asset discovery and VM system to a full exposure management system that included their "asset risk traffic light system" which highlighted assets at high risk of leading to service failure, loss of life or environmental accidents.
Protecting Against Cyber Attack	The architecture included multiple layers of protection, such as firewalls, secure access controls, and physical security measures, to defend against potential cyber-attacks. All data was brought into their exposure management system giving managers a top-down view across all security domains.
Detecting Cyber Security Events	Real-time exposure management tools provided early detection of cybersecurity events, allowing for swift responses to any incidents.
Minimising the Impact of Cyber Security Incidents	The company’s incident response plans ensured that any cyber incidents were quickly contained, minimising their impact on safety and production.

Water Corp

Water Corp is a regional water utility company responsible for the supply and treatment of water for residential, commercial, and industrial use. The company's ICS/OT systems manage critical processes such as water purification, distribution, and wastewater treatment. Given the essential nature of its services, Water Corp must ensure the security and resilience of its ICS/OT systems to prevent disruptions that could affect public health and safety.

Water Corp had additional challenges due to budgeting priorities, chronic under-investment in security staff and poor maintenance of its estate.

Applying NCSC Principles

Establish context	Water Corp engaged the services of a managed security services provider to help with a risk assessment and help provide a managed service to help them meet current CAF and future CS&R requirements. The highly distributed nature of Water Corp, with hundreds of water course sluice gate controllers, dams, grey and potable water systems made the task especially challenging. The MSSP drafted a two-year plan based on NCSC principles to increase cyber-security resilience in Water Corp.
Making compromise difficult	The company implemented a cloud-first strategy, minimising local hardware requirements and decreasing time to value. All major systems were retrofitted with multi-factor authentication access controls. Water Corp enhanced it's network segmentation, in larger treatment plants and data centres. Least privilege principles were implemented for service operators with monitoring carried out by the MSSP.
Making disruption difficult	Redundancy and fault-tolerant designs for critical systems were reviewed and upgrades planned where possible. Disaster recovery plans were reviewed and tested through table-top exercises led by the MSSP.
Making detection easier	Water Corp outsourced all detection to their chosen MSSP, with regular reports provided to the CSO. The MSSP service was tailored to provide visibility into all critical operations, with alerts configured for immediate incident response.
Reducing the impact of compromise	Segmentation of the ICS/OT network ensured that any compromise was contained within a limited scope in larger environments. The incident response plan was tailored to quickly isolate affected systems and restore normal operations with minimal disruption.

Avoiding Security Architecture Anti-Patterns

'Browse-up' for Administration	**Description**: Allowing administrators to use the same environment for both browsing the internet and performing administrative tasks can lead to the exposure of critical systems to internet-borne threats. **Mitigation**: Water Corp enforced strict policies that separated administrative tasks from regular user activities. Dedicated environments were used for administrative work and browsing or non-essential activities were prohibited on administrative accounts.
Management Bypass	**Description**: This Anti-Pattern involves creating alternative management routes that bypass security controls, which can be exploited by attackers to gain unauthorised access to critical systems. **Mitigation**: All management interfaces were secured and integrated into the overall security architecture. No out-of-band management paths were left unsecured, ensuring that security controls could not be bypassed.
Back-to-Back Firewalls	**Description**: The practice of placing two firewalls from different vendors back-to-back under the assumption that it provides added security can lead to misconfigurations and reduced performance without a significant security gain. **Mitigation**: Instead of relying on back-to-back firewalls, Water Corp employed a layered security strategy, incorporating network segmentation, intrusion detection/prevention systems (IDS/IPS), and secure access controls to enhance security without the complexity and potential pitfalls of dual firewalls.
Building an 'On-Prem' Solution in the Cloud	**Description**: Replicating on-premises security architecture in the cloud without considering cloud-specific threats and capabilities can lead to ineffective security controls and gaps. **Mitigation**: The MSSP implemented a service was primarily cloud-based with the stipulation for local security capability in the larger sites.
Uncontrolled and Unobserved Third-Party Access	**Description**: Allowing third-party vendors to access critical systems without sufficient oversight can lead to security breaches, as these access points are often less controlled and monitored. **Mitigation**: The company implemented strict controls over third-party access to its systems. All third-party activities were tightly monitored and logged by the MSSP, with access restricted to only the necessary systems and functions. Continuous observation ensured that all vendor activities were secure and compliant, with the solution that was implemented providing both a pre authorisation requirement for access and then time limiting that access.

The Un-patchable System	**Description**: Systems that cannot be patched due to operational constraints, compatibility issues, or other reasons are vulnerable to exploitation over time as new vulnerabilities are discovered. **Mitigation**: Water Corp has a legacy of end of sale equipment that it did not have the funds to replace quickly. Instead, it relied on continuous attack path analysis by the MSSP and compensating controls such as network isolation, enhanced monitoring, and additional layers of access control to mitigate risks associated with these systems.

Aligning with CAF Objectives

Managing Security Risk	Water Corp engaged the MSSP to twice-yearly review of the cyber risk register and provide a prioritised report on exposures and mitigations.
Protecting Against Cyber Attack	The company's architecture included next generation firewalls with embedded IPS, encrypted communications wherever possible, and strong physical security measures.
Detecting Cyber Security Events	Water Corp deployed advanced monitoring and detection systems across its ICS/OT environment and managed by the MSSP. These systems provided real-time alerts for any suspicious activity, enabling the security team to quickly respond to potential threats.
Minimising the Impact of Cyber Security Incidents	Water Corp incident response plans were regularly tested and refined to ensure rapid containment and recovery in the event of a cyber incident. These plans prioritised the protection of public health and safety, ensuring that any disruptions were minimised and that essential services could be quickly restored.

Conclusion

The protection of ICS/OT systems in CNI sectors is paramount due to the increasing cyber threats and the potential consequences of disruptions. This document has outlined a comprehensive reference architecture for ICS/OT security, guided by the principles of the UK's NCSC, the avoidance of common Security Architecture Anti-Patterns, and alignment with the Cyber Assessment Framework.

Through three detailed case studies—Energy Corp in the energy sector, Chem Corp in chemical production, and Water Corp in water utilities—we have demonstrated how these principles and frameworks can be effectively applied in diverse real-world environments. Each organisation faced unique challenges, but by adhering to the NCSC's five security principles, avoiding critical Anti-Patterns, and aligning with the four CAF objectives, they were able to design and implement robust ICS/OT security architectures.

By following the guidance provided in this document, other organisations can similarly enhance their ICS/OT security posture, safeguarding their critical systems against an evolving threat landscape. Regular reviews, updates, and adherence to these best practices will be essential in maintaining and strengthening ICS/OT security in the face of new and emerging challenges.

References:

- https://www.ncsc.gov.uk/static-assets/documents/cyber-assessment-framework-v3.2.pdf
- https://www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-caf-collection
- https://www.ncsc.gov.uk/collection/cyber-security-design-principles
- https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles
- https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

Statement of support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, and whilst ICS-COI members have exercised reasonable care in compiling the guidance, they provide no warranty as to its accuracy, completeness, or suitability for any particular purpose.

To the fullest extent permitted by law, neither the ICS-COI or its members accept any liability for any loss, damage, cost, or expense arising directly or indirectly from the use of and / or reliance on, this document. Users of this guidance are advised to exercise their own judgement and consider taking independent professional advice.

Any reference to commercial products, services, or entities by name or otherwise, does not constitute or imply endorsement, recommendation or preference by the ICS-COI. The views and opinions expressed in this document shall not be used for advertising or product endorsement purposes.

Document Details

This document is version 1.0 and was published on 17/10/2025. It will be reviewed every 18 months.