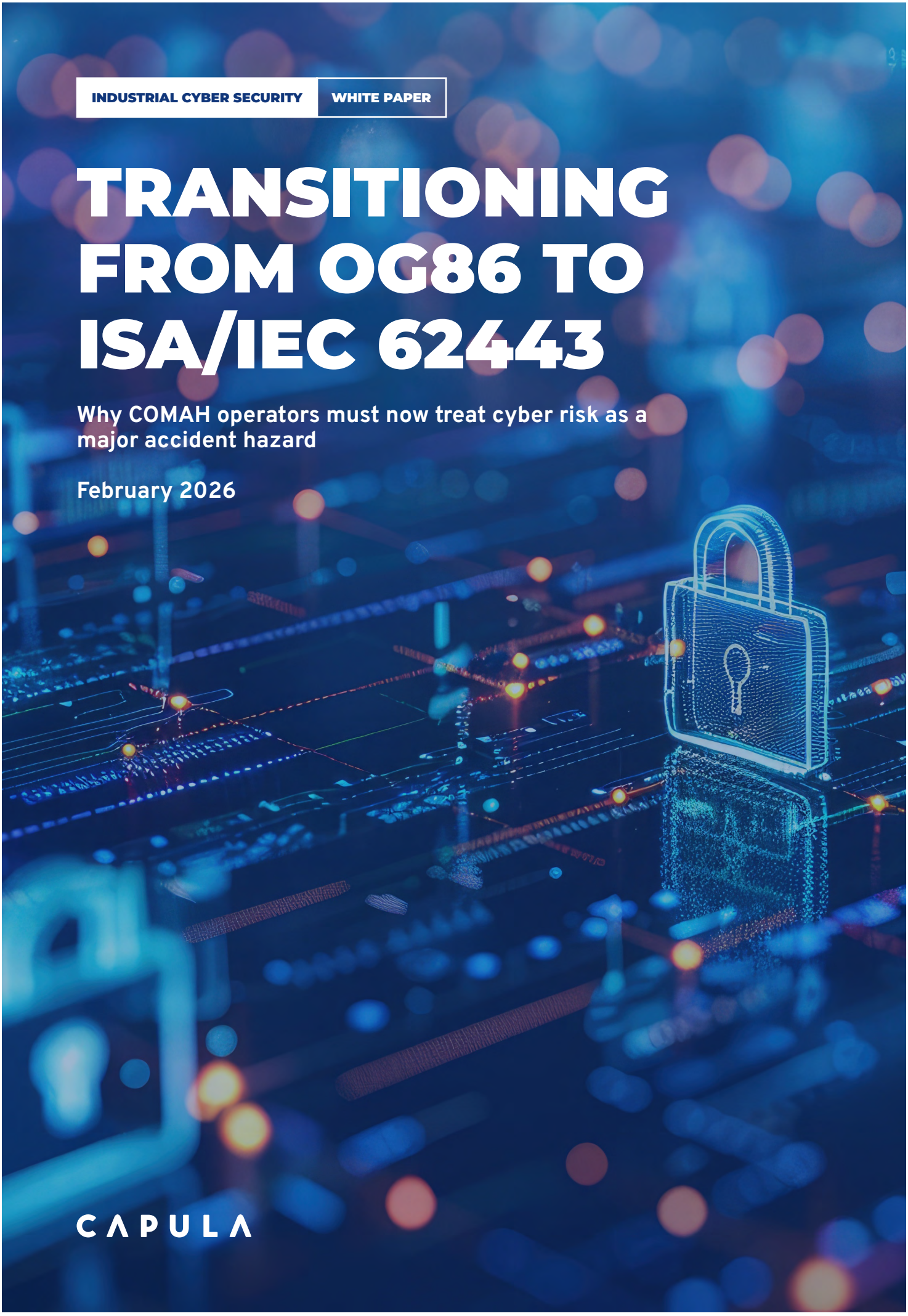
INDUSTRIAL CYBER SECURITY | WHITE PAPER

TRANSITIONING FROM OG86 TO ISA/IEC 62443

Why COMAH operators must now treat cyber risk as a major accident hazard

February 2026



CAPULA

TABLE OF CONTENTS

1. **Foreword** 3

2. **Introduction** 5

   Why cybersecurity is now a process safety issue; the shift away from OG86; why COMAH operators must adopt ISA/IEC 62443.

3. **Why OG86 Is No Longer Sufficient** 6

   Limitations of OG86, the evolving threat landscape, and HSE's rationale for transitioning to ISA/IEC 62443.

4. **What ISA/IEC 62443 Introduces** 7

   4.1 **Cyber Security Management System (62443-2-1)** 7
   Governance, risk management, competence, and assurance requirements.

   4.2 **Zones, Conduits & Security Levels (62443-3-2)** 7
   Hazard-linked zoning, boundary definition, and SL determination.

   4.3 **System Requirements (62443-3-3)** 7
   Hardening, access control, detection, monitoring and resilience capabilities.

   4.4 **Supplier Assurance & Secure Development (62443-2-4 / 4-1 / 4-2)** 7
   Vendor security, patching, secure design, and supply-chain expectations.

5. **Cyber as a Major Accident Hazard** 10

   5.1 **Academic Research on Cyber-Physical Failures** 10
   Why cyber must be considered an initiating event; collapse of BPCS/SIS independence assumptions.

   5.2 **Implications for COMAH Risk Assessment** 10
   How cyber-initiated failures impact LOPA, HAZOP and overall hazard analysis.

6. **Worked Example: Safety System Compromise (TRISIS-Inspired)** 11-14

   6.1 **Scenario Overview** 12
   Typical COMAH SIS/BPCS architecture and inherited vulnerabilities.

   6.2 **What TRISIS Demonstrated** 12
   Real-world safety system manipulation and operator deception.

   6.3 **Attack Stages (SIS Compromise Pathway)** 13
   Stage 1–5 breakdown of TRISIS-style compromise.

   6.4 **Why This Matters for UK COMAH** 14
   Typical UK legacy conditions and their regulatory significance.

   6.5 **Key Lessons for Duty-Holders** 14
   Why 62443 becomes the benchmark and how cyber links to MAH.

7. **What Good Looks Like: Practical Pathway for COMAH Operators** 15-19

   7.1 **Step 1 — Baseline Analysis** 16
   CAF maturity assessment, risk exposure, strategy and steering group formation.

   7.2 **Step 2 — Governance & CSMS** 17
   Accountability, competence, policies, supplier management.

   7.3 **Step 3 — Zones, Conduits & Architecture Mapping** 17
   Asset inventories, zoning, boundaries and conduit identification.

   7.4 **Step 4 — Cyber Risk Assessment Using a Safety Lens** 18
   Cyber as an initiating event; realistic attack pathway modelling; SL derivation.

   7.5 **Step 5 — Implementation Roadmap** 18
   Segmentation, identity controls, monitoring, detection and supplier uplift.

   7.6 **Traceability into the COMAH Safety Case** 19
   Linking hazards → SLs → controls; demonstrating lifecycle and evidence.

8. **Conclusion** 19

   The regulatory shift, why action is urgent, and how to achieve resilience.

FOREWORD

By Steven Lane, OT Cyber Security Lead

Cybersecurity in industrial environments has reached an inflection point. COMAH operators have long focused on process safety, improving management systems and asset integrity. However, increased digital connectivity and operational technology have created new cybersecurity risks in systems not originally designed for them. Recent incidents in chemicals, energy, and water sectors show that cyber-attacks on industrial controls can cause actual physical harm.

The HSE's decision to transition from Operational Guidance 86 (OG86) to the ISA/IEC 62443 series as its benchmark for enhanced cybersecurity at Tier 1 COMAH sites is a direct response to this reality. OG86 served its purpose well. It gave inspectors a consistent baseline and gave operators a starting point for basic cyber hygiene in safety-related control systems. However, it was not conceived as a formal standard, nor was it developed with consideration for the current threats encountered by operators. ISA/IEC 62443 provides what OG86 cannot: a structured, internationally recognised framework for governance, risk assessment, system hardening, and lifecycle assurance, all anchored to the specific demands of cyber-physical environments.

This transition is more than a change of reference document. It reflects a fundamental shift in how the regulator expects cyber risk to be treated. The TRISIS incident demonstrated beyond doubt that safety systems themselves can be targeted, manipulated, and disabled by determined adversaries. The long-standing assumption that the Basic Process Control System (BPCS) and the Safety Instrumented System (SIS) cannot fail simultaneously is an assumption that underpins much of classical process safety analysis. This is no longer defensible in a digitally connected plant. Cyber threats introduce credible mechanisms for common-cause failure that traditional hazard studies simply do not capture.

This paper sets out why the move to ISA/IEC 62443 is both necessary and urgent and offers a practical pathway for compliance and resilience. It examines how cyber threats should now be treated as initiating events within the COMAH safety case, and why governance, zone and conduit modelling, Security Level (SL) determination, and lifecycle traceability are essential components of a defensible cybersecurity programme. It includes a worked example, drawing on the TRISIS methodology, to illustrate how a single cyber compromise can defeat multiple protection layers simultaneously and what that means for major accident hazard management in a UK context.

My aim in writing this paper is to provide clarity. Clarity on what the regulatory transition means in practice. Clarity on what "good" looks like from both an engineering and an inspection perspective. Clarity on how duty-holders can build a credible, risk-based, evidence-driven approach to OT cybersecurity that protects people, assets, and the environment.

The message for industry is straightforward: cybersecurity is a process safety issue. The organisations that recognise this early, take ownership at board level, and embed ISA/IEC 62443 principles into their safety lifecycles will be best positioned to meet regulatory expectations and to operate safely in an increasingly hostile digital landscape. Those that delay risk being caught unprepared not just by the regulator, but by the threats themselves.

Steven Lane
OT Cyber Security Lead, Capula

Steven Lane

WHY COMAH OPERATORS MUST NOW TREAT CYBER RISK AS A MAJOR ACCIDENT HAZARD

INTRODUCTION

Industrial cybersecurity is now a key part of process safety and operational resilience. At Tier one COMAH sites, where failures can cause serious harm to people, the environment, and the economy, cyber threats are a central concern. Safety-critical systems are targets for attackers. Cyber attackers can disrupt operator visibility and push processes into unsafe conditions. Recent incidents in the chemicals, energy, and water sectors show that cyber-attacks on OT systems have real, physical impacts.

The Health and Safety Executive (HSE) has used OG86 since 2017 as its internal guidance for inspecting Industrial Automation and Control Systems (IACS), to assess cybersecurity. OG86 established essential cyber hygiene, but it was never designed for the threat landscape operators face today. It is not a standard, cannot deliver higher maturity levels, and lacks the depth needed for today's interdependent OT environments.

For this reason, the HSE will move from OG86 to ISA/IEC 62443 as the leading standard for Tier one COMAH sites, where enhanced cyber is needed, starting 1 April 2026. This change underscores the need for a clear, auditable, and internationally recognised approach to securing complex industrial systems and defending against determined attackers.

The main point is clear: cybersecurity is now a process safety issue, and COMAH operators must show that their OT systems are as secure as they are safe.

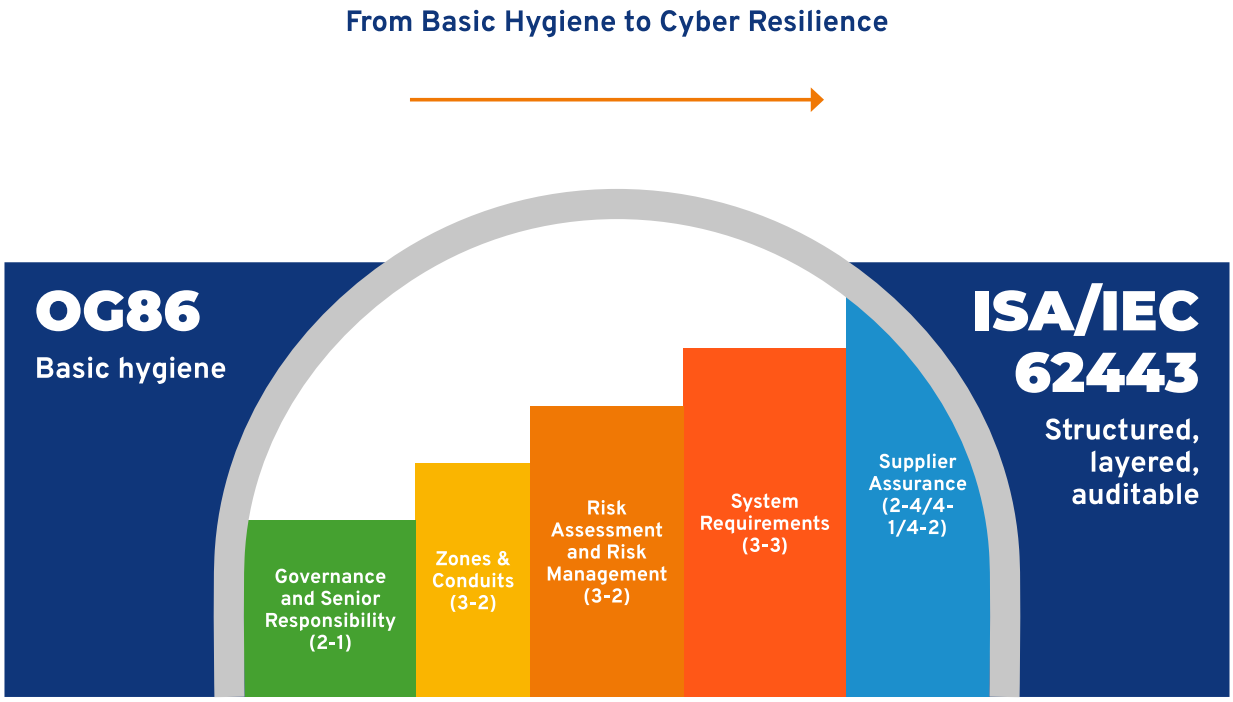


Figure 1: Comparison of OG86 and ISA/IEC 62443 Approaches.

WHY THE HSE IS MOVING TO ISA/IEC 62443

When the HSE began inspecting cybersecurity on COMAH sites about 10 years ago, there was little OT-specific guidance available. OG86 was created to fill that need. It combined parts of the NCSC CAF Basic Profile with the HSE's practical engineering steps for basic cyber hygiene in safety-related control systems. For its original purpose, OG86 works well. It provides sites with a starting point and it has helped inspectors use a consistent benchmark during early inspections. However, OG86 was never meant to be a formal standard. It was the HSE's internal view of good practice, written by engineers for engineers.

The challenge now is that things have changed. Cyber threats that once seemed unlikely are now common and target the technologies COMAH sites depend on. Attackers can move through shared networks, switch between systems, and affect both Basic Process Control System (BPCS) and Safety Instrumented System (SIS) functions. These risks are real, not just theoretical.

Many major hazard sites still rely on outdated ideas, such as believing network segregation alone is sufficient protection. Many sites have made little progress in managing cybersecurity throughout the system's lifecycle, even after years of regulatory focus.

Given these changes, the HSE has decided that OG86 can only provide a basic level of cyber maturity. It covers the basics but lacks the depth, structure, and lifecycle focus needed for today's OT environments and threats. OG86 also does not support the NCSC's Enhanced Profile CAF, which is now the UK's standard for resilience in high-risk settings. The HSE has made it clear that moving from OG86 to ISA/IEC 62443 is a shift from basic hygiene to real resilience. Organisations must be able to detect, respond, and recover. These are not optional extras. They are essential for any site where failure could cause harm beyond the site itself.

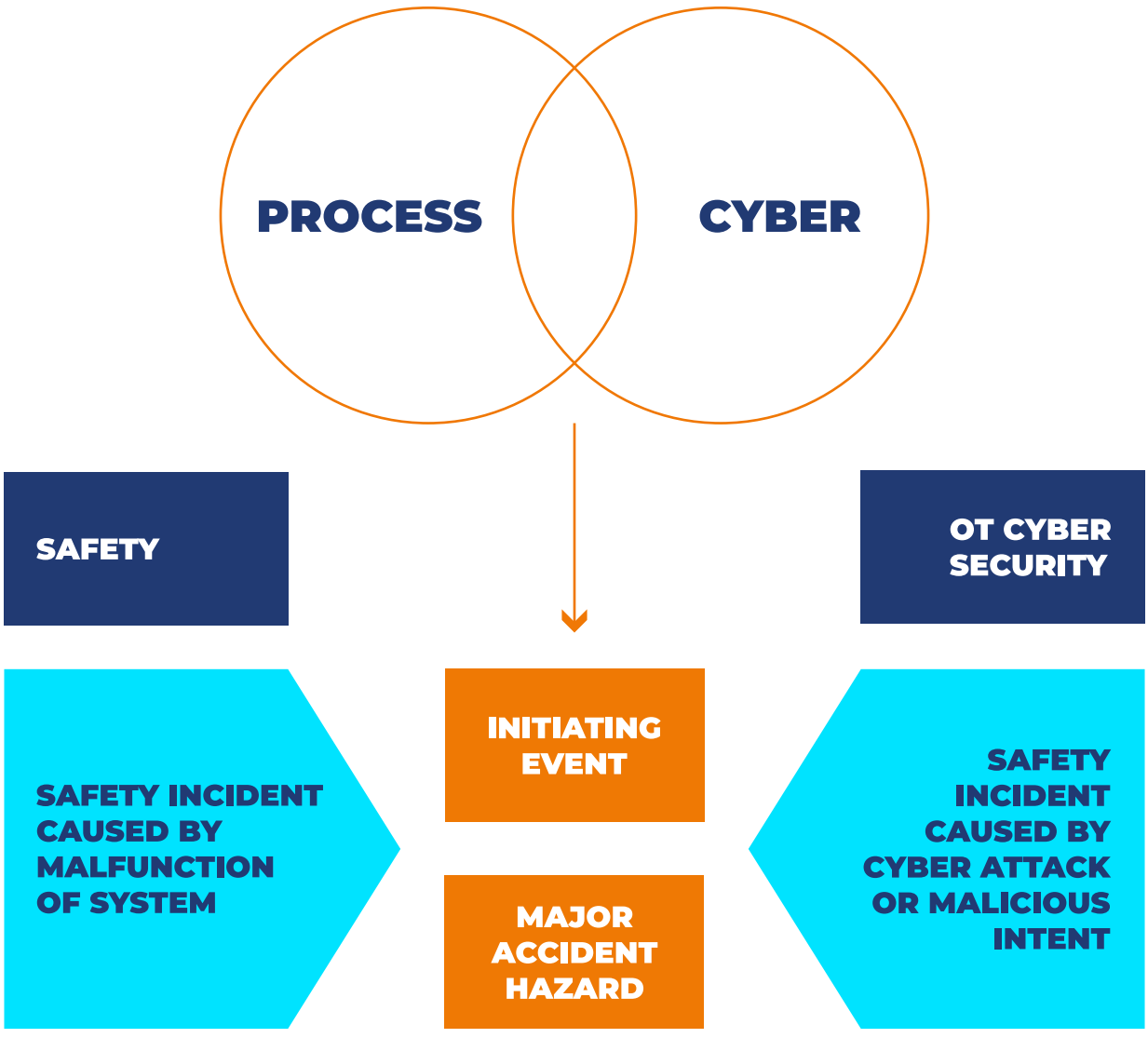


Figure 2: Cyber–Process Safety Interaction Diagram.

WHAT 62443 INTRODUCES THAT OG86 CANNOT PROVIDE

ISA/IEC 62443 provides structure and detail that fit the needs of cyber-physical systems in high-hazard settings. Some parts are essential for COMAH operators:

A formal Cyber Security Management System (62443-2-1)

OG86 covers management-system ideas, but 62443 spells them out clearly. It requires governance, risk management, asset ownership, organisational competence, and assurance activities to be set up, maintained, and proven. This matches the functional safety lifecycle and helps include them in COMAH safety reports.

Hazard-linked zoning, conduits, and Security Level (SL) determination (62443-3-2)

Rather than relying on segmentation or 'air gaps,' 62443 requires a straightforward engineering process that connects hazards, threat scenarios, system boundaries, and needed Security Levels. This allows for realistic modelling of cyber common-cause failures, which traditional safety methods miss. A cyber incident can affect 'everything, everywhere, all at once' because equipment failure probabilities do not limit attackers.

Prescriptive system requirements (62443-3-3)

OG86 sets out expectations, but 62443 turns them into precise technical requirements. These cover access control, system hardening, communication integrity, monitoring, detection, and recovery. This supports the CAF Enhanced Profile's focus on resilience, especially detection and response, which OG86 does not fully include.

Supplier assurance and secure development (62443-2-4, 4-1, 4-2)

Modern control systems need proof that vendors provide secure components, keep up with patching, and design with security in mind. OG86 does not cover this well. The HSE now expects sites to show supply-chain assurance that matches these standards.

Figure 3: Linking hazards to cyber risk, Security Levels, controls, and evidence.

This may be the most critical change. Sites need to show the whole process:

Figure 4: The five lifecycle questions required for 62443 traceability.

This matches the functional safety lifecycle and helps fit with COMAH safety case logic. OG86 does not require this full traceability, but 62443 does.

WHY THIS ALIGNMENT MATTERS FOR COMAH OPERATORS

The HSE's position is cybersecurity is a process safety issue. If a cyber-attack can disable a Safety Instrumented Function, manipulate the Basic Process Control Systems (BPCS), or interfere with alarms, then it can initiate or escalate a Major Accident Hazard (MAH). As such, cyber threats must be explicitly considered in COMAH safety reports, with a lifecycle-based demonstration in the same style as functional safety.

This shift also reflects the reality that in many ways OG86 could be reaching the end of its useful life. It has served its purpose, but industry has matured, threats have intensified, and regulators such as Health and Safety Executive (HSE), the Office for Nuclear Regulation (ONR), and the Environment Agency (EA) must rely on established international standards rather than maintaining a bespoke internal guide.

By embracing 62443, operators gain:

- a structured, defensible approach to cyber risk
- clear linkage between cyber threats and process hazards
- a scalable way to evidence proportionality
- an approach that aligns with CAF Enhanced requirements
- An internationally recognised framework that supports auditability and resilience

Most importantly, they gain a common language with the regulator, and international industry as a whole, removing ambiguity and clarifying what "good" looks like.

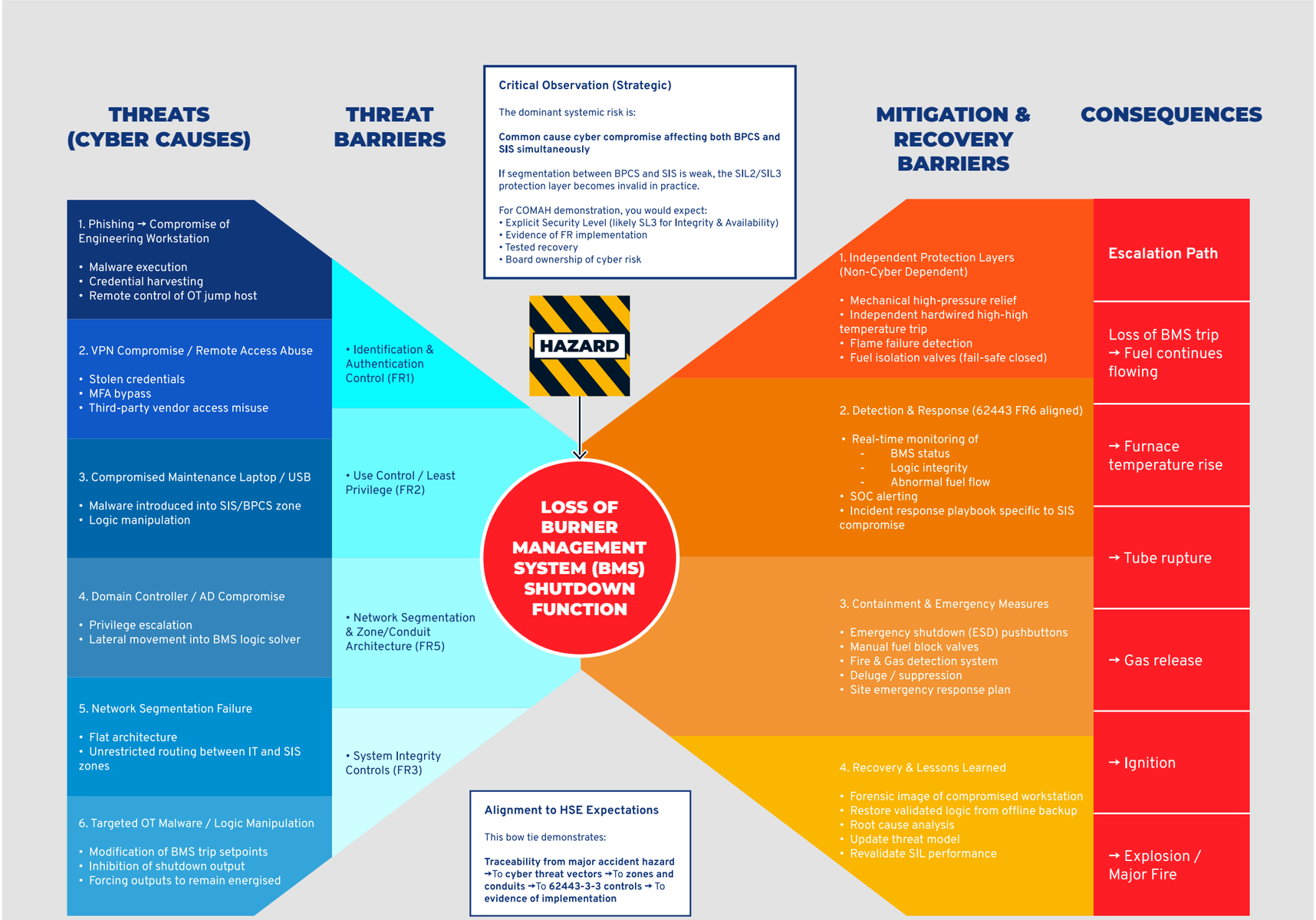


Figure 5: TRISIS-Inspired Cyber Attack Stages on Safety Instrumented Systems.

CYBER AS AN INITIATING EVENT IN PROCESS SAFETY

Research mainly by academia establishes that cyber threats are a credible initiating event for major process safety incidents. Cyber threats are not just an IT or data-security concern. As operational technology and digital connectivity have increased, cyber-attacks have shown the ability to manipulate process conditions, suppress alarms, interfere with control logic, and directly compromise safety systems. Studies show that traditional hazard and risk analysis techniques underestimate risk when cyber-initiated failures are excluded, especially in highly automated, networked industrial environments.

For decades, process safety practice has relied on the assumption that the BPCS and the SIS are independent layers of protection and cannot fail at the same time. While this holds for random hardware failures, academic research shows it is no longer valid with cyber threats. Modern industrial architectures often include data exchange, shared engineering workstations, trusted communications, and indirect dependencies between BPCS and SIS. These connections create cyber-enabled common-cause and common-mode failure pathways, allowing a single attack to disable or degrade both systems at once.

Research extending Layer of Protection Analysis (LOPA) to include cyber risk shows that once cyber-attack is treated as an initiating event, traditional independence assumptions collapse and risk outcomes change significantly. In cyber scenarios, the BPCS can no longer be credited as an independent protection layer, and sometimes the SIS itself cannot be assumed to function on demand. This leads to higher residual risk than predicted by classical LOPA and often requires additional safeguards, such as independent Safety Instrumented Functions, architectural hardening, or reliance on inherently non-hackable mechanical protections.

Complementary research on cyber-physical HAZOP reinforces this conclusion, showing that cyber-attacks often act as indirect causes that exploit vulnerabilities in the information domain to trigger unsafe control actions in the physical domain. These attack pathways are not captured by traditional deviation-based hazard studies, confirming that cyber risk must be explicitly integrated into process safety analysis rather than managed as a separate security issue.

THE UNIFIED MESSAGE FROM ACADEMIC RESEARCH

The unified conclusion from current academic research is clear and consistent. The long-standing assumption that BPCS and SIS cannot fail simultaneously is no longer defensible in modern, digitally connected process plants. Cyber threats introduce credible mechanisms for simultaneous failure that invalidate traditional process safety assumptions. As a result, cyber risk must be treated as an initiating event within hazard and risk analyses, and safety and security can no longer be designed, assessed, or governed in isolation. Organisations that do not adapt their process safety frameworks risk underestimating major accident hazards in today's OT environments

WORKED EXAMPLE: SAFETY SYSTEM COMPROMISE INSPIRED BY TRISIS

WORKED EXAMPLE:
SAFETY SYSTEM COMPROMISE INSPIRED BY TRISIS

The TRISIS/TRITON cyber incident remains one of the most instructive real-world demonstrations of how a determined attacker can target safety systems directly. The event occurred on a petrochemical site in the Middle East. It showed that compromising a Safety Instrumented System (SIS) is not theoretical: it has happened. It nearly resulted in a catastrophic process event.

Drawing on lessons observed from the TRISIS incident, it is possible to model how similar techniques could apply to UK COMAH sites if equivalent architectural weaknesses exist.

Scenario Overview

A high-hazard facility relies on a SIL2 or SIL3 SIS to prevent loss of containment, thermal runaway, or mechanical overstress. The SIS logic solver is connected to the BPCS through an engineering workstation and a shared OT network segment, allowing operators to view diagnostics and status.

This architecture is typical of many legacy UK COMAH installations.

What TRISIS Demonstrated

The real-world attackers behind TRISIS were able to:

- Access the engineering workstation used to configure the SIS.
- Upload modified SIS logic designed to disable or manipulate safety functions.
- Preserve the appearance of normal operation to operators.
- Target the final elements: shutdown valves and interlocks essential for preventing a major accident.

Most importantly, the attack aimed to turn off or corrupt the very safety functions designed to prevent catastrophic consequences.

TRISIS-INSPIRED EXAMPLE:
FURNACE SHUTDOWN PROTECTION DEFEAT

Hazard Pathway (Process Safety View)

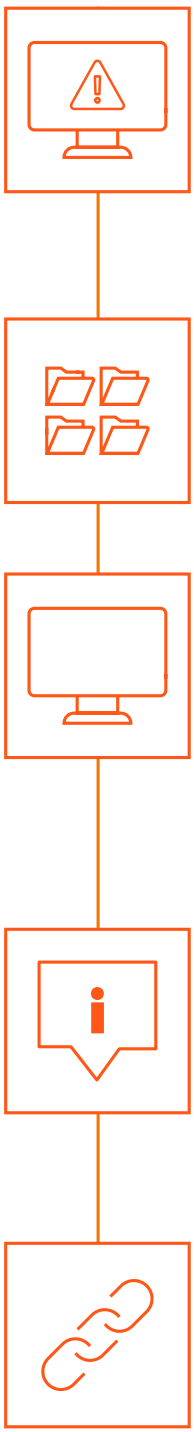
A HAZOP identifies the scenario:
“Loss of burner management shutdown → uncontrolled furnace temperature rise → tube rupture → fire or explosion.”

LOPA allocates:

- A SIL2 burner trip Safety Instrumented Function (SIF), implemented in the SIS.
- A BPCS temperature control loop as the primary control.
- Operator intervention based on high-temperature alarms.

Under traditional assumptions, these layers are independent.

CYBER ATTACK PATHWAY (BASED ON THE TRISIS METHODOLOGY)



Stage 1 — Compromise of the Engineering Workstation

The attacker gains access through:

- A remote-access pathway not protected by Multi Factor Authentication (MFA)
- A vendor maintenance connection
- A compromised corporate account

This mirrors the initial foothold used in TRISIS.

Stage 2 — Reconnaissance of SIS Logic

From the engineering workstation, the attacker:

- Retrieves the current SIS logic
- Identifies the burner trip SIF
- Identifies memory locations and function block structures

Stage 3 — Modification of Safety Logic

The attacker uploads modified logic that:

- Extends the trip delay
- Raises the shutdown threshold
- Reduces voting from 2oo3 to 1oo3 or bypasses a channel entirely
- Corrupts the final element command path

This is structurally identical to the behaviour seen in TRISIS.

Stage 4 — Manipulation of Operator Visibility

The attacker ensures:

- The HMI continues to show healthy SIS status
- Trip conditions are hidden or suppressed
- Change logs appear normal

This prevents the operator from seeing that protection has been disabled.

Stage 5 — Loss of Independence of Protection Layers

When the furnace overheats:

- The BPCS loop fails to maintain control under off-normal conditions (e.g. fouled heat exchangers, drift, poor combustion conditions).
- The operator alarm does not reflect the corrupted SIS status.
- The SIL2 SIF does not actuate because the logic has been modified.

A single cyber compromise has disabled all three layers simultaneously which is a direct parallel to the TRISIS event.

Figure 6: Cyber Attack Pathway.

WHY THIS MATTERS FOR UK COMAH

The core insight from TRISIS, when translated into a UK setting, is that safety systems are now a legitimate and demonstrated target for hostile actors.

Typical assessments of sites in the UK identify common legacy conditions that could permit similar compromise:

- Engineering workstations without Multifactor Authentication (MFA) or Role Based Access Controls (RBAC)
- Flat networks not adequately segregating BPCS/SIS
- Outdated firmware on logic controllers
- Lack of application whitelisting
- Infrequent or unverified logic backup comparisons
- Vendor connections not governed properly within the governance framework of a Cyber Security Management System (CSMS)

These conditions create a credible pathway for a TRISIS-style attack.

KEY LESSON FOR DUTY-HOLDERS

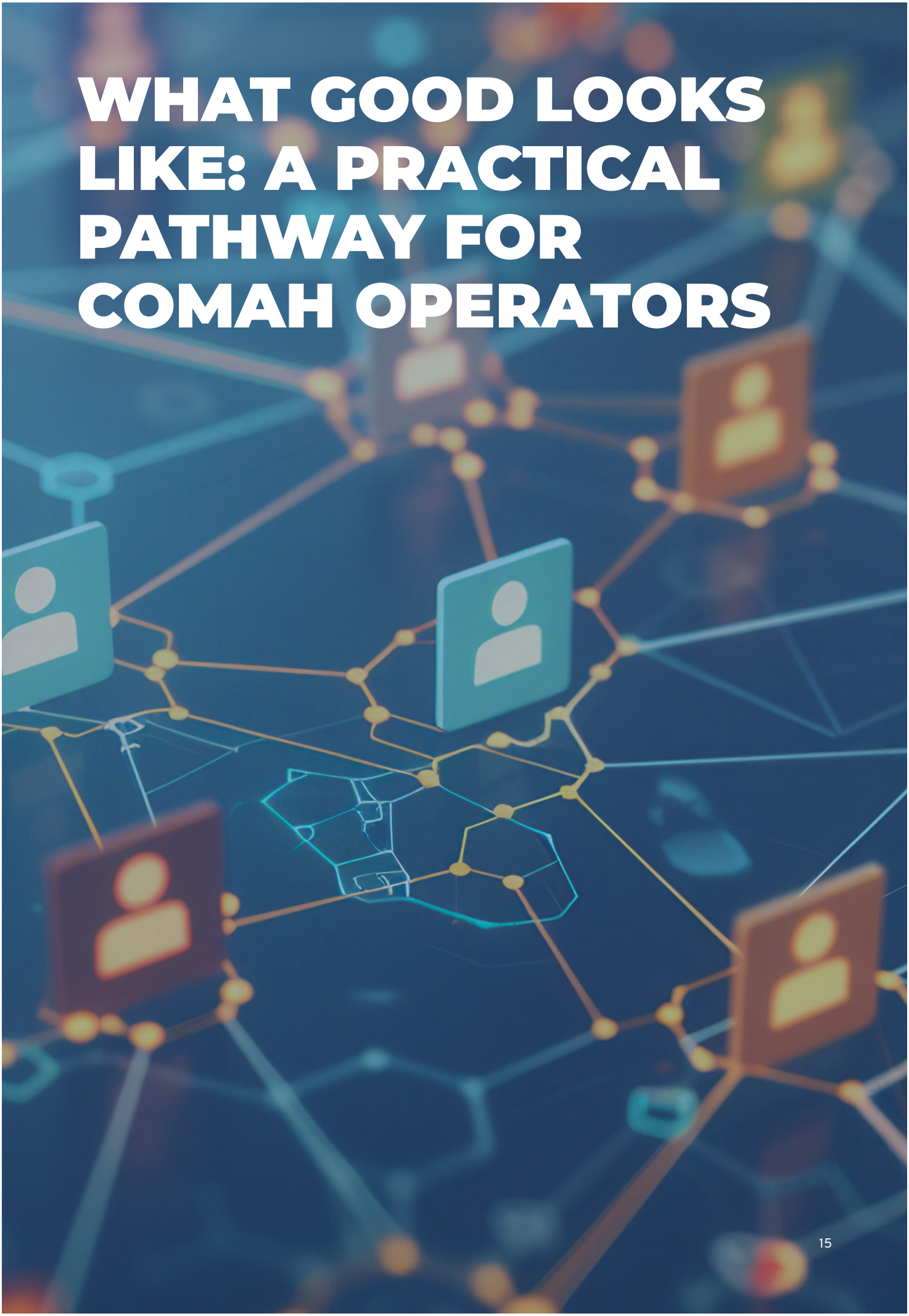
From a COMAH perspective, the TRISIS incident is the most unmistakable evidence that a cyber threat can directly disable the SIL-rated protections that underpin a major accident safety case.

This is precisely why:

- ISA/IEC 62443 now forms the regulatory benchmark
- Security Levels must align with SIL requirements
- BPCS–SIS independence must be validated
- Cyber must be treated as a MAH initiating event

This worked example demonstrates how a real-world cyber-attack translates directly into a UK context and why safety and cyber analysis must be unified.

WHAT GOOD LOOKS LIKE: A PRACTICAL PATHWAY FOR COMAH OPERATORS



WHAT GOOD LOOKS LIKE: A PRACTICAL PATHWAY FOR COMAH OPERATORS

For many COMAH operators, the April deadline has now passed and for some this may feel uncomfortably late. However, the HSE has been clear that organisations cannot wait for an inspection to take action. Cyber risk must now be treated with the same seriousness as any other MAH. The HSE's message is that cyber resilience must be built in, managed, and evidenced as part of the safety lifecycle and no longer an optional add-on.

With that in mind, the following pathway sets out what "good" looks like in practice. It reflects what inspectors might expect to see, what the standards require, and what is achievable for most duty-holders without over-engineering the solution.

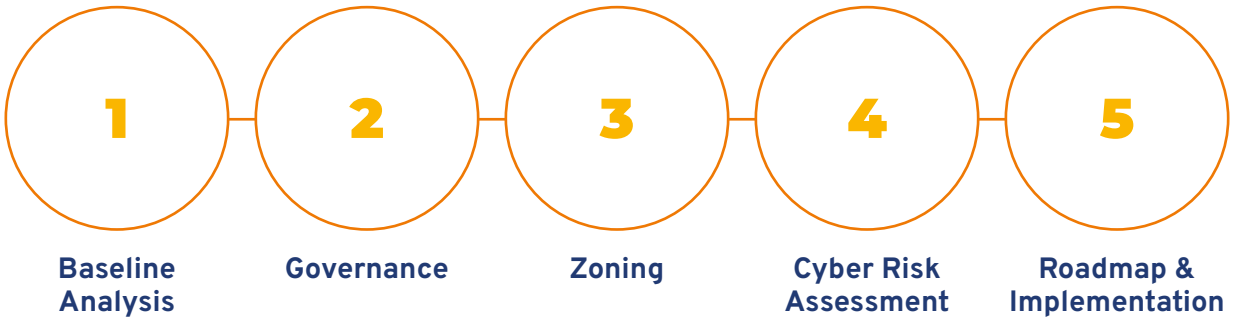


Figure 7: A Practical Pathway For COMAH Operators.

1. Start with a Baseline Analysis and Set the Direction

For most COMAH operators, whether Tier 1 or Tier 2, the first meaningful step is to undertake a health check against the NCSC Cyber Assessment Framework. This is where you understand your current exposure, identify gaps, and assess whether your organisation is truly positioned to meet expectations. The HSE's own guidance underlines that you cannot manage what you have not first understood.

A good baseline includes:

- A CAF maturity assessment across governance, risk, architecture, monitoring, and response.
- A review of how OT, cyber and process safety teams currently interact (or do not interact).
- Identification of immediate risks, legacy vulnerabilities, and areas requiring urgent remedial work.
- Clarify senior stakeholder engagement, preferably at board level, by creating a steering group. Set up a funding discussion urgently, and discuss the issue of risk reduction. Investment in cyber will be required to lower risk, manage the potential of MAH and avoid potential HSE sanctions
- The steering group will be required to set a mandate. Whilst ownership of cyber risk must sit at the board, decisions on who is accountable day-to-day, and how decisions will be made must be documented and agreed in a charter document. Barriers between OT, Safety and Cyber need to be broken down as collaboration is key to success.
- The steering group will establish the strategy that will take the site to 2026 and beyond. Very often this in captured in an OT cyber security charter as described in NIST SP800-83[1]

Once this strategic foundation is in place, the next natural step is to embed these decisions into a formal Cyber Security Management System (CSMS).

2. Establish Effective Governance with a Cyber Security Management System (CSMS)

A strong baseline appears not with firewalls or network diagrams, but with governance. The HSE's published material suggests that unless cyber considerations are embedded within the existing safety management system, subsequent technical controls are unlikely to be effective.

In practical terms, this means:

- Defining who is accountable and establishing an effective cyber operating model.
- Knowing what systems you operate.
- Managing competence, suppliers, and change.
- Aligning policies and procedures with the principles of the IEC 62443-2-1 standard (Security for industrial automation and control systems – Part 2 1: Security program requirements for IACS asset owners) and the NCSC CAF.

For many organisations, this is where the fundamental cultural shift happens. It is the point at which cyber stops being "something IT do" and becomes part of the same discipline that manages functional safety, maintenance, and operational integrity.

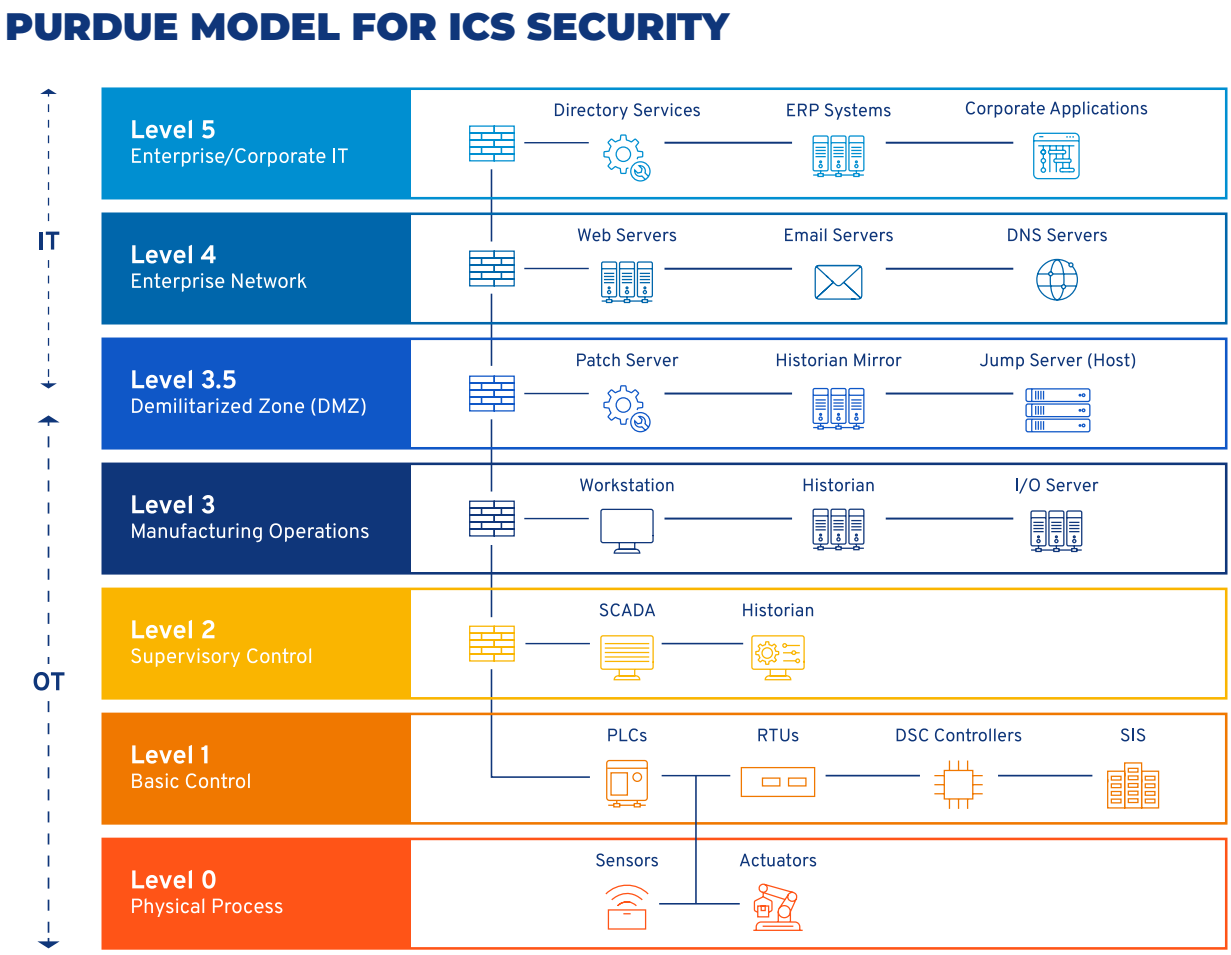


Figure 8: OT Network Zoning Model for COMAH Sites.

3. Map Your OT Environment Properly: Zones, Conduits, Boundaries

Once the CSMS foundations are in place, operators need a clear picture of what they are defending. HSE OG86 guidance and 62443-3-2 (Part 3 2: Security risk assessment for system design) are explicit. Duty-holders must define where the control system begins and ends and understand how data moves through it.

This step is inherently practical:

- Document every control, safety, electrical, and supporting system.
- Group assets into logical zones based on criticality.
- Identify conduits between zones and any connection to the corporate network, vendors, or remote access paths.
- Understand which zones really carry major hazard consequences.

One clear message from inspectors in a recent presentation was that many sites misunderstand their own architectures. Several inspections reported assumptions such as “we are air-gapped” that turned out to be false once the drawings were verified on site.

A robust zoning model becomes the backbone for everything else such as risk assessment, security level determination, and implementation planning.

4. Assess Cyber Risk Through a Safety Lens, Not an IT Lens

For COMAH tier one sites, the HSE’s transition from OG86’s basic expectations to a more prescriptive, risk-based model based on 62443 is precisely because cyber incidents now have the potential to affect every protective layer simultaneously.

This means risk assessment must now:

- Consider cyber as an initiating event.
- Reflect credible attack pathways (e.g., TRISIS-style SIS modification, BPCS compromise, OT lateral movement).
- Integrate threat-informed judgement—especially in high-consequence zones such as SIS and critical BPCS.

62443 provides a structured method to assign target Security Levels (typically SL2–SL3 for COMAH sites), but the HSE expects this to be linked explicitly to hazard scenarios. For example, if a cyber incident could remove a SIL2 protection layer and simultaneously affect alarms, interlocks, and operator interfaces, the risk assessment must reflect that reality.

Modelling cyber risk using bow-tie analysis is an effective way of combining both safety and cyber initiating events.

5. Build a Realistic, Prioritised Implementation Roadmap

Once SLs are defined, the organisation needs a clear plan that moves from “what” to “how.” It was made clear at a presentation given by the HSE that inspectors are not expecting perfection, but they are expecting evidence of progress, prioritisation, and justification.

A strong roadmap typically includes:

- Network segmentation aligned to your zone model.
- Identity and access controls, including MFA for all remote access and privileged operations.
- Monitoring and anomaly detection, scaled to the site’s threat exposure.
- Tested and rehearsed incident response and recovery.
- Supplier assurance upgrades (which are often the most neglected area).

The HSE specifically calls out the need to detect, respond, and recover, which are capabilities that OG86 does not cover and which many operators still lack. This is where IEC 62443-3-3 (system security requirements and security levels) and IEC 62443-2-4 (service provider security requirements) begin to bite, and where most organisations will spend their main effort over the next 24–36 months.

DEMONSTRATE TRACEABILITY INTO THE COMAH SAFETY CASE

Everything above ultimately needs to reconcile with the COMAH Safety Report. HSE's inspectors are likely to want to see a clear, auditable chain that links hazards to SL assignments and then to implemented controls.

This means:

- Showing how cyber threats were considered when analysing major accident hazards.
- Demonstrating how safety functions (SIS, BPCS, interlocks) remain dependable under cyber duress.
- Evidencing testing, monitoring, updates, and change control.
- Showing the lifecycle approach in action, not simply described on paper.

The bar is not theoretical perfection. It is demonstrable, systematic, risk-based control of cyber-physical hazards.

PUTTING IT ALL TOGETHER

This is not an academic exercise. It is reasonable to assume this broadly reflects what HSE inspectors may look for from April 2026 onwards, and it aligns with a lifecycle-based approach that should be achievable for most COMAH operators.

In short:

- Establish your baseline.
- Build governance and operating model.
- Understand your architecture.
- Assess your risk based on realistic cyber-physical scenarios.
- Prioritise your controls.
- Provide evidence and traceability.

This is the pathway to a defensible position during inspection and, more importantly, the path to resilient, safe operations in a world where cyber incidents can now "affect everything, everywhere, all at once."

CONCLUSION

The shift from OG86 to ISA/IEC 62443 is not regulatory rebranding. OG86 will remain and will still be used by HSE where basic cyber hygiene is needed. The transition for enhanced cyber requirements for Tier 1 COMAH is a recognition that industrial cyber threats can now trigger significant accident hazards with real-world consequences. For all COMAH operators, cybersecurity is now inseparable from process safety. The responsible to have a safe system is sits firmly with the duty-holder and in order to have a safe system cyber must have been considered.

Organisations that act now by assessing their current environment, embedding cyber into process safety, and adopting the 62443 lifecycle are likely to meet HSE expectations and strengthen resilience against the cyber-physical threats faced by modern industrial operations.

For operators who have yet to begin this journey, the message is do not delay. Start your journey now and at least baseline your organisation.

Book Your OT Baseline Assessment

CAPULA

capula.com

Orion House,
Stone Business Park,
Staffordshire ST15 0LT

Get in touch:
Tel: +44 (0)1785 827000
Email: contactus@capula.com

Follow us on LinkedIn