Simulating nuclear critical infrastructure for live cyber defence training: The Defence Cyber Marvel Nuclear Power Plant

By **Dr Richard Piggin** (Office for Nuclear Regulation) & **Captain Josef Yalvac** (Royal Signals)

SUMMARY

- Exercise DEFENCE CYBER MARVEL (DCM) is an annual competition, this year with the hub located in Singapore. Thirty-six teams, 29 countries and 2,500 personnel from Defence, Government agencies, industry partners, UK critical infrastructure operators and other nations, competed in a challenging real-world scenario defending a variety of systems. The range includes specialist systems, with technology used to operate critical infrastructure, which face increasing cyber risk. Specialist skills and realistic training opportunities for protecting CNI technology are limited. DCM developed a high-fidelity physical demonstrator to enhance hands-on training and increase awareness.
- The system uses industrial control systems technology, often referred to as Operational Technology (OT), commonly used for safety-related automation. It embodies components widely used in safety systems architectures. Similar safety-related control systems are used across Critical National Infrastructure, including transport, critical manufacturing, utilities, energy, and hazardous industrial processes.
- The paper discusses one approach the British Army Cyber Association takes to maximise future training opportunities. This includes specialist security functionality to provide control system protocol awareness, asset discovery, vulnerability prioritisation, anomaly detection, device behavioural analytics and threat hunting capability.

1. INTRODUCTION

DEFENCE CYBER MARVEL often referred to as DCM, has evolved into a UK tri-service Army led cyber exercise. Last year exercise hub was in South Korea, this year it was in Singapore, showcasing the deep cooperation between the UK and trusted partners like Singapore. The week-long exercise brought together more than 2,500 personnel from 70 different organisations, and 29 countries to form 36 teams, including representatives from UK Defence, Regular and Reserves, other UK Government departments including The National Crime Agency, The Department of Work and Pensions, The Cabinet Office and The Department of Business and Trade. This year's exercise tested participating nations' ability to coordinate responses in a realistic operational environment, with scenarios mirroring genuine cyber threats. [1]

DCM 2026 provided a platform to highlight the professional cyber development opportunities available across UK Defence. With personnel operating under a realistic, pressured environment containing traditional IT systems, as well as more complex industrial control systems, decision-making and technical skills can be transferred directly to operational settings, helping defend networks and disrupt daily attacks from UK adversaries.

The attackable systems within the range are varied and nuanced, ranging from physical replicas of Critical National Infrastructure to virtual traffic light systems during rush hour. Complemented by hybrid systems, which exist both virtually and physically, they provide a complex variety of attack surfaces for the participating teams. Blue Teams (BT) need to seize the initiative to quickly understand these systems, secure them and respond to evolving Red Team (RT) attacks. Meanwhile BTs will brief their in-scenario commanders on the impact to mission critical systems, their recovery and consequences should they fail. Any shortcomings will be physically represented, whether it's a crippled logistics network, a cascading national grid collapse or potentially HMS Wallace experiencing a catastrophic engine failure.

Operational Technology (OT) is often unrecognised, overlooked and taken for granted. Many OT components are hidden from view in electrical cabinets, alongside the process under control. You may notice the operator screen or an emergency stop and not consider the systems behind it. Did you see that air bridge as you boarded your most recent flight, and consider what drives that airport baggage carousel or that colossal theme park ride? Your next adrenalin filled launch is programmed by an OT engineer. Operational Technology moves physical stuff, including humans.

OT training is increasingly critical to Defence as modern military effectiveness as, unlike traditional IT, OT is not widely encountered in everyday MOD digital environments, creating a significant skills gap in our Service Personnel. Despite this, personnel are required to understand how to defend systems that behave differently to enterprise networks should the operational need arise.

This challenge is compounded by OT pervasive across the real world, yet it remains poorly understood outside specialist communities. As some adversaries have already demonstrated capability and intent to target OT systems. Defence must now look to rapidly build competence in identifying key vulnerabilities, interpreting system behaviour, and managing risk in environments where failure can have immediate and potentially catastrophic physical consequences.

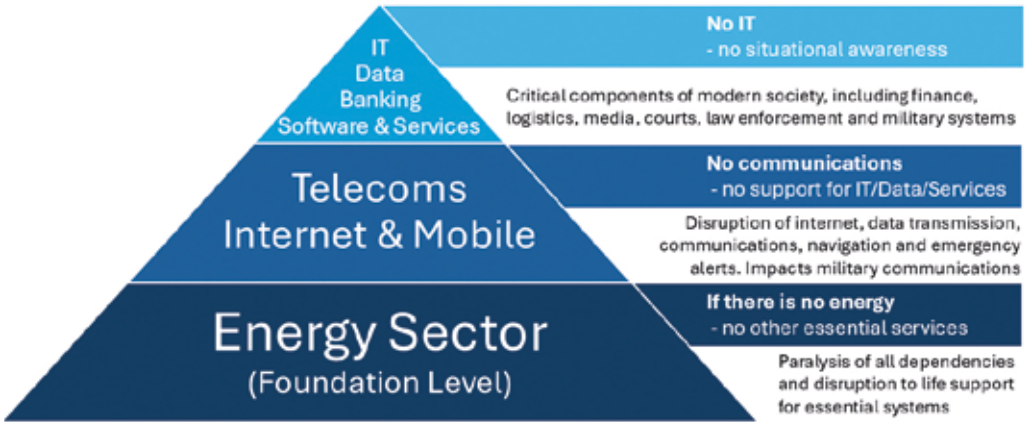

Figure 1. Targeting energy infrastructure can cause devasting consequences with cascading impacts
Source: After CERT-UA, War and Cyber: Three years of struggle and lessons for global security [2]

DCM looks to directly address this challenge through a mixture of tutelage, exposure to realistic OT environments and accelerating experiential learning. Critically, the OT environments provide a controlled means to develop understanding, build confidence and reduce the risks associated with deploying inadequately trained personnel into operational environments.

OT systems are in widespread use throughout critical infrastructure supporting the operation of our daily lives and they can be vulnerable. The Ukraine Government Computer Emergency Response Team (CERT-UA) recently reported the increasing targeting of energy infrastructure. CERT-UA's analysis highlighted potentially devasting consequences, with cascading loss of essential services that modern society relies upon (Figure 1).

WHAT IS OPERATIONAL TECHNOLOGY OR OT?

IT moves data. OT moves stuff, often found in essential services which support our daily lives. According to the UK National Cyber Strategy (2022), "Operational Technologies (OT) – combine hardware and software to monitor, control and automate physical processes, particularly in industrial sectors such as energy, manufacturing, water and transport." [14]

2. CHOOSING A CRITICAL INFRASTRUCTURE SCENARIO

The initial challenge was to how to bring a nuclear power plant (NPP) to the exercise, with the intent to engage participants, raise awareness of safety control systems and illustrate our reliance upon them in daily life. We choose to simulate a widely used pressurised water reactor (PWR) design, whilst providing visible interaction, tangible outputs and learning potential.

A PWR nuclear reactor has a primary loop that transfers heat to a secondary loop to produce steam for electricity generation. It uses ordinary (light) water as both a coolant and neutron moderator, operating under high pressure (typically 150-160 bar) to prevent the water from boiling.

The pressurised water reactor (PWR) is simulated using a programmable safety controller, a safety version of a programmable logic controller (PLC) used in industrial automation. Safety controller provides additional redundancy and self-checking for safety applications and resilient operation in the event of faults. Status information display and operator interaction are enabled using an operator panel, known as a human machine interface (HMI). The safety programmable controller inputs provide systems monitoring and control rod position. Controller outputs drive a 3D printed reactor, moving the control rods to determine the reactor output, and shutdown the reactor in the event of an incident. A high pitch audible alarm and flashing red lights would indicate an anomaly, irritating and tangible enough for Blue Team defenders and suitably noticeable for Red Team kudos.

The use of a safety system introduces specialist OT with resilient safety functionality, designed to protect people, the environment, and systems used with hazardous processes. The concept of safety critical functions is used across a wide range of industrial sectors, including manufacturing and safety-related automation. Consider turning the London Eye, or any complex motion ride, moving a bridge or train signalling, points and shunting. Larger schemes such as petrochemical plants use redundant safety instrumented systems (SIS) and nuclear reactors have diverse safety systems, combining both programmable and non-programmable hardwired logic.

The control system hardware used are the basic building blocks of 'automation Lego'; all being bespoke in their programming and their implementation for process automation, but all using commercial off the shelf (COTS) modular components. Similar safety systems and process automation are used for numerous applications, including transport (road, rail, ship control, port and airport infrastructure), the built environment, critical manufacturing, utilities, energy, and hazardous industrial processes. Industrial automation is also used in a variety of other applications, often where people are near or operating automation, or 'in machines', including tunnels, leisure park rides, ski lifts, cable cars and funicular railways.

2.1. System design and overview

Earlier DCM systems introduced Operational Technology to participants and illustrated CNI threats to exercise visitors. The Railway Control System Demonstrator provided an accessible CNI model rail system, operated by a rail safety system, with specialist OT cyber security protection, in a robust air portable package (Figure 2). The DCM Nuclear Power Plant (NNP) simulator benefited from

the rail systems design approach and lessons learnt. These included implementing a more sophisticated control system and offering an increased network attack surface, with real-time automation protocol exposure. The design benefited from increased robustness and visual appeal, whilst reducing weight for carriage by air in hold baggage. Our approach enabled design innovation with risk mitigation to address to critical component lead times and ensure delivery within a short duration prior to the exercise.

Figure 2 "The trainset" rail control demonstrator with safety-controlled points and signal interlocking.
Image credit: Rob Young

The system is mounted in two transportable hard cases with the following principal components:

- A programmable safety controller, often referred to as safety programable logic controller (PLC) or safety PLC. This runs the simulation and safety programable logic used to control the process;
- Safety Input/Output (I/O) or remote I/O with industrial Ethernet connectivity to support additional inputs and outputs (sensors/actuators) for PLC process control. This also increases the Red Team attack opportunity to manipulate the process, and the necessity for Blue Team defence;
- Human Machine Interface (HMI), or Operator Panel which is also connected via industrial Ethernet to enable operator spoofing, by sending false information or malicious commands;
- 3D model reactor operated with remote safety inputs and outputs with moveable control rods and LEDs indicate to operational status (blue normal; visualising Cherenkov radiation , red for anomaly, and that really bad day in the Blue Team office. Green shows a successful shutdown with rods fully down).
- Environmental hardened industrial network infrastructure.

These components are shown in Figure 3.

Control system programming is performed using IEC 61131-3 PLC programming languages, with ladder logic and safety functions. This combination limits the variability of coding, reducing the likelihood of programming errors in safety applications (Figure 4). The graphical function blocks can encapsulate pre-defined code written in other PLC languages, specific safety functions are certified and not editable to further reduce safety programming

OT AND IT HAVE DIFFERENT SECURITY REQUIREMENTS

OT

- Limited data capacity and computing;
- Safety operations are critical;
- High availability and integrity are vital. Confidentiality is less stringent;
- Critical operations/systems at network edge with humans at the centre;
- Long life (often decades) resulting in legacy, unsupported infrastructure;
- Essential equipment and operations remotely deployed at network edge;
- Heterogenous OT assets, from differing vendors and different asset types, includes IT assets used to support OT functions;
- Slow response to threats, rapid patching might be impossible due to incurring system outages.

IT

- High data capacity and computing power;
- Few safety critical operations;
- Confidentiality and integrity are vital while availability is important;
- Critical operation and systems are at the network centre, with human users at the edge;
- Continuous equipment upgrades with short life cycles;
- Essential equipment and operations concentrated at network centre;
- Homogenous IT assets and limited asset types;
- Rapid response to threats, patching forced reboots are acceptable.

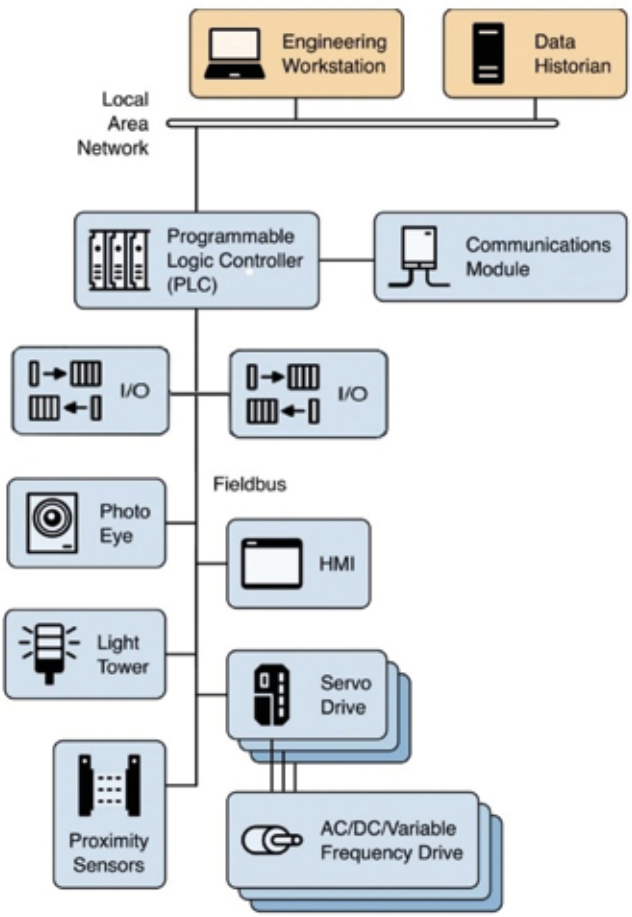

Figure 3 An example control system implementation
Source: After NIST 800-82r3 Guide to Operational Technology Security [3]

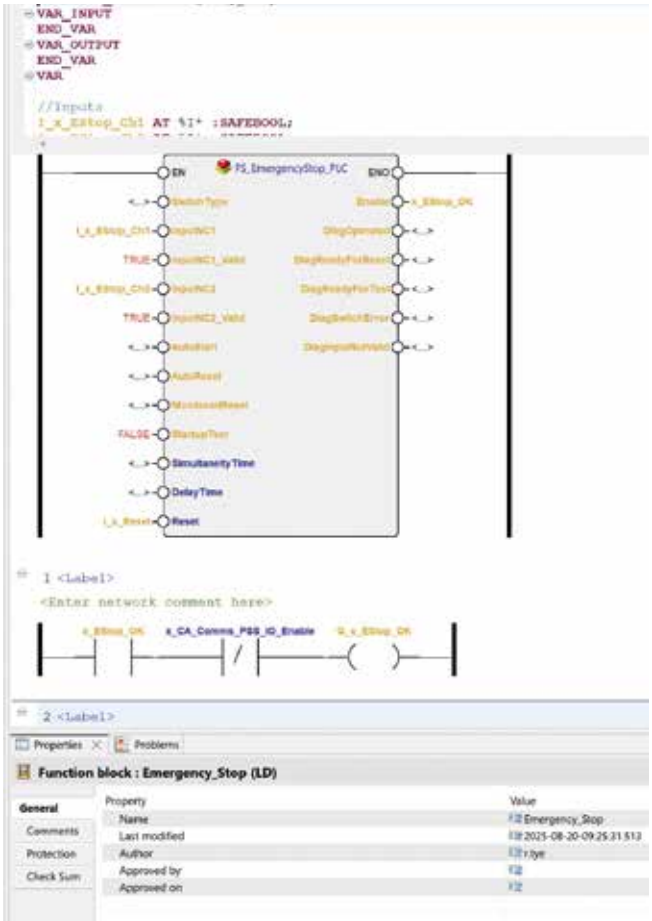

Figure 4 Safety program logic showing emergency stop function block with a 'rung' of ladder logic enabling code

Figure 5 Nuclear Power Plant simulator
Image credit: Rob Young

errors (see the Emergency Stop function block shown in Figure 4). Ladder diagram, one of the original graphical languages, and still the most widely used is likened to electrical schematics, representing rungs of relay logic. When rung logic conditions are met, the output on the rung is triggered.

*Cherenkov radiation is the blue light emitted when a charged particle passes through a transparent dielectric medium such as water faster than the speed of light. It's named after the Noble Prize winner scientist Pavel Cherenkov. The International Atomic Energy Agency (IAEA) uses Cherenkov radiation measurement to verify the presence, activity and integrity of spent fuel in storage ponds.

The safety-related programmable logic running on the safety simulates the PWR, enables operator interaction via HMI panel and emergency stop button. The reactor control rods, LEDs and PWR system are monitored and enabled via the remote inputs/outputs, connected to the safety controller by industrial ethernet (Figure 5). Configured HMI operator panel screens are shown in Figure 6 and Figure 7.

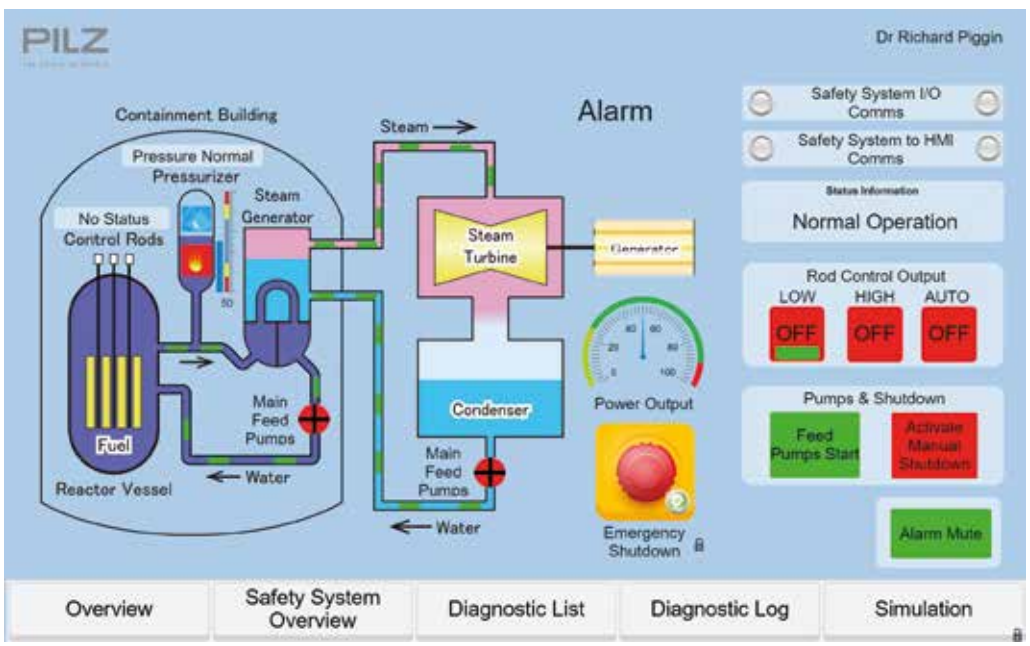

Figure 6 Operator Panel configuration in HMI display configuration software

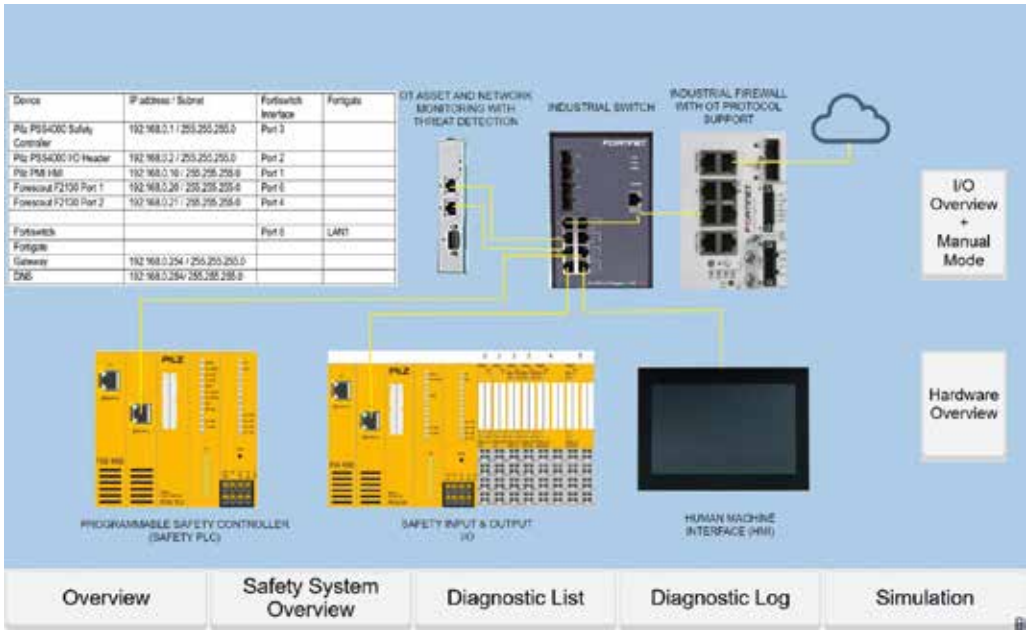

Figure 7 System architecture with security capabilities,
Image from the Operator Panel (HMI) display configuration software

The components are interconnected via an industrial managed network switch, using the Industrial Ethernet protocol Modbus TCP. Chosen for its vulnerability and simplicity. This enables users to appreciate widely adopted industrial networking, which is inherently insecure, and will remain in place for many years, as installed industrial equipment lifetimes are often measured in decades (Figure 7). Long lifecycles lead to widespread OT system vulnerabilities. Forescout Research Vedere Labs Threat RoundUp 2025 report revealed attacks against OT protocols have increased by 84% year on year. [4]

WHAT ARE THE OPERATIONAL TECHNOLOGY CHALLENGES?

A cyber attack targeting OT, leading to a prolonged loss of the electricity grid, loss of logistic capabilities, or platforms, could have severe consequences, including the potential for loss of life. As such, a cyber-attack could have comparable effects to a physical attack.

Cost reduction and improved efficiency drive adoption of digital solutions, but security is often overlooked. There is a shortage of experienced personnel with converged IT/OT security expertise. OT is found in complex environments, with overlapping green and brownfield technologies which can lead to complex integration, visibility and vulnerability issues. Increasing connectivity potentially expands the attack surface, where OT systems were formerly isolated.

Air gaps, with no presumed connectivity can provide false optimism, even without network or wireless connectivity. System updates on digital media could provide a high latency low bandwidth connection. A trusted privileged access (engineering) workstation used to program OT could be a viable attack pathway, compromised by browsing the internet, using office applications or checking email. Remote and third-party access used for system commissioning, monitoring and maintaining systems can also afford unintentional internet exposure and access.

According to the Vedere Labs report, Modbus TCP accounted for 57% of OT attacks, followed by EtherNet/IP at 22%. Both are open industrial networking technologies and are widely used by OT vendors and third parties for connectivity for controller networking, programming, configuration and fieldbus (industrial automation networking) process sensors and actuators. Other protocols included BACNet, a building management protocol and STEP7, a Siemens proprietary protocol. Attacks against building automation protocols had increased by 37%. These include Heating, Ventilation, and Air Conditioning, security systems and data centres.

This illustrates the necessity to monitor traffic to and from OT assets. This is now equally, if not more critical than monitoring just IT traffic. Forescout's research shows attackers are continuously probing assets for weaknesses, and many organisations remain blind to the threats as they lack visibility into their OT environments (Figure 9).

3. SECURING OPERATIONAL TECHNOLOGY WITH CYBER-PHYSICAL SECURITY

"IT moves data, OT moves stuff": OT or cyber-physical security protects networked control systems, where the imperative is to prevent unwanted physical actions and consequences. [5] Cyber-physical security is critical with increased connectivity and more sophisticated automation will continue to expose wider attack surfaces.

Unsophisticated attackers may gain access to OT, and apply ransomware or interfere with systems, but they rarely invest to understand the process. This is illustrated with a security advisory issued by the UK, US agencies and partners encouraging increased protection of OT systems against Russian aligned hacktivists targeting Critical National Infrastructure. The alert warns of heightened threat to OT systems from the creation of nuisance effects. [6]

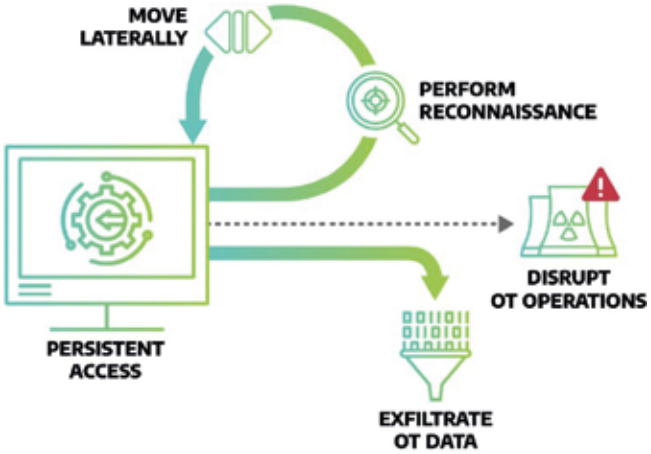

Figure 8 Nation state attacks involve persistent access for espionage
Source: Threats & Risk to the United Kingdom's Civil Nuclear Sector, Dragos and ONR 2025 [7]

Sophisticated actors behave like engineers, seeking to understand the process under control, developing attack strategies to create defined outcomes. Advanced attacks target the physics of the industrial process, such as motion, temperature, level, flow, pressure, time/rate and process analytics. This requires knowledge of the system, its OT components and the automation process to derive potential effects (Figure 8). OT risk management should consider the worst case consequence of system compromise, the loss of critical functions and their recovery.

Stuxnet, discovered in 2010, targeted Siemens WinCC Supervisory Control and Data Acquisition (SCADA) engineering software and PLCs used to enrich uranium in Iran's nuclear programme. Stuxnet 'jumped' the perceived air gap isolating enrichment cascades, compromising engineering workstations (often Windows laptops) used to program and configure enrichment systems, initially with a compromised USB flash drive. Early versions of Stuxnet exfiltrated OT information, before executing the attack. Stuxnet deceived personnel, over-pressurised and varied the rotor speed of centrifuges, successfully destroying thousands. Ralph Langer's definitive analysis 'To Kill a Centrifuge' provides insight into the sophisticated and first of its kind cyber physical attack with cognitive and kinetic effects, along with its subsequent impact on control systems security. [8]

Tier one adversaries, highly capable, well resourced nation state/state sponsored groups, have demonstrated their willingness to target safety systems designed to prevent and mitigate process hazards. Reckless nation state campaigns feature in US Department of Justice indictments and UK Government exposure of historic malign activity. This includes malware designed to target a petro-chemical plant's safety systems, resulting in two emergency shutdowns. [9]. See Boxouts. Dr Piggin discusses these, and other incidents in 'Enhancing Civil Nuclear Cyber Security' in Nuclear Future Journal Volume 20.1. [10]

Safety risk assessments with their identified potential hazards may become adversary outcomes, turning security threats into safety hazards. Triggering a safety system to operate as intended, and safely shutdown a process, will cause a nuisance 'trip', and lost productivity. There is potential for harm too, where the safest course of action might be to continue to operate. False information or status sent to operators either to disguise unauthorised changes or to initiate inappropriate actions may cause premature shutdown, damage, loss of functionality and risk to life.

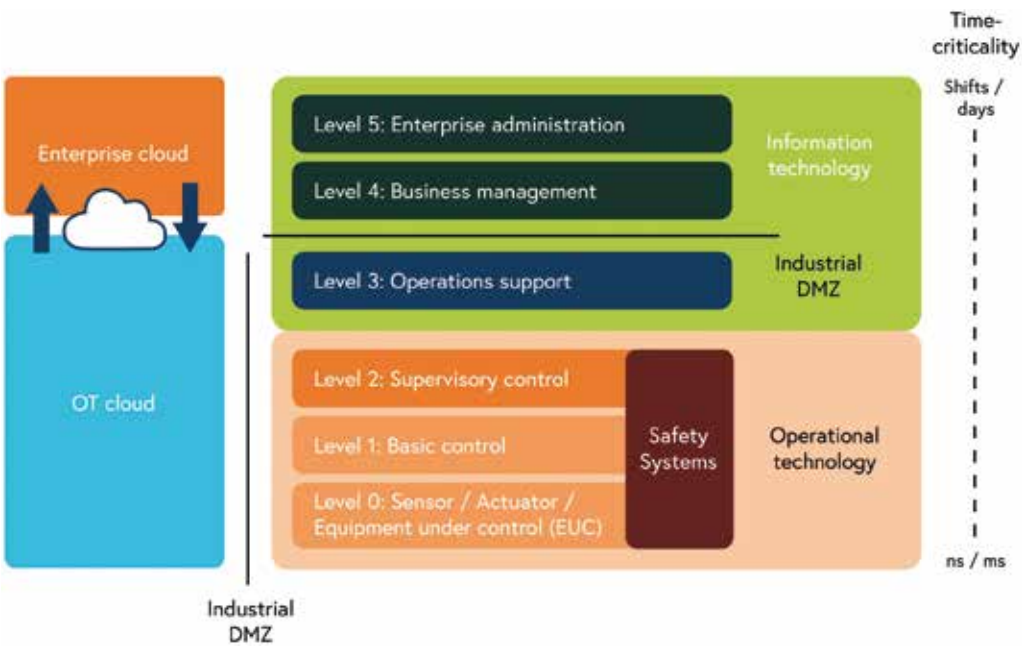

Figure 9 OT architecture hierarchy with ISA-95 standard levels used in manufacturing and security/
Source: R Piggin for IET Code of Practice for Cyber Security and Safety.
Reproduced with permission of the IET [11]

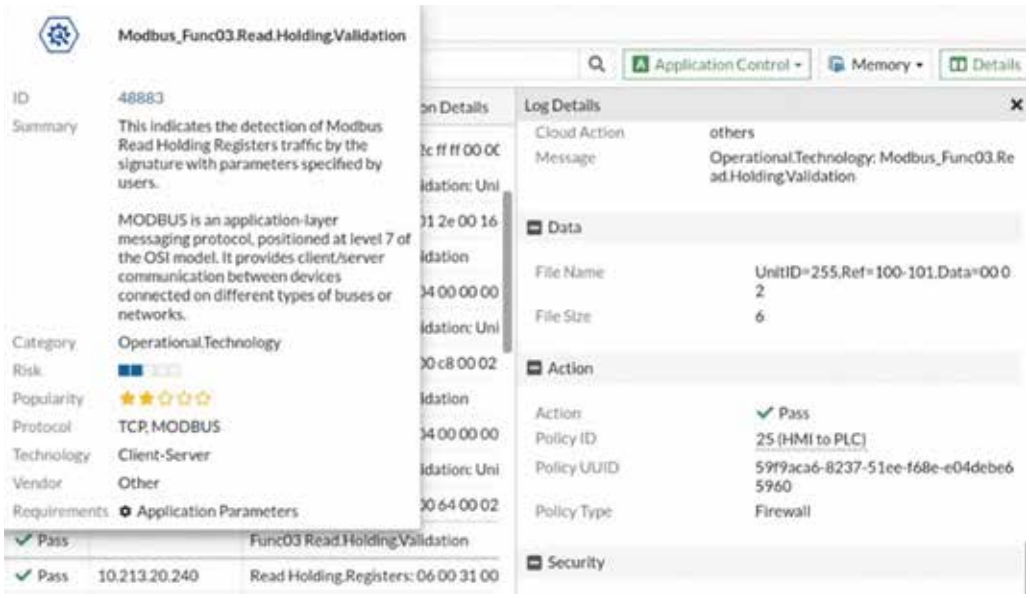

Figure 10 Understanding OT protocols and unusual activity with Fortinet

The networking convergence of IT and OT has bridged functionally distinct silos. Critical business systems run the business and control systems automate real-time physical processes that enable the business to run. IT focuses on agility with frequent software patching, often with confidentiality foremost. Whilst OT environments demand high availability with integrity, in a reliable and stable environment, with safety paramount.

The merging of IT and OT environments to achieve data driven optimisation in the industry 4 paradigm, often known the fourth industrial revolution, increases the potential for OT systems exposure from threats traversing the IT/OT boundary (Figure 9). Conversely, enterprise IT environments can be exposed by third party supply chain partners directly connecting to OT for condition monitoring and maintenance. Increasing architecture complexity can provide additional attack paths or bypass the protection, including perceived air gaps.

3.1. Enhancing capability and training value: Adding industrial security

The nuclear simulator also incorporates industrial network security components specifically designed to protect OT. Project partner Forescout provided eyeInspect, an OT asset intelligence, threat detection and monitoring platform with industrial protocol recognition, behavioural analytics and anomaly detection. We

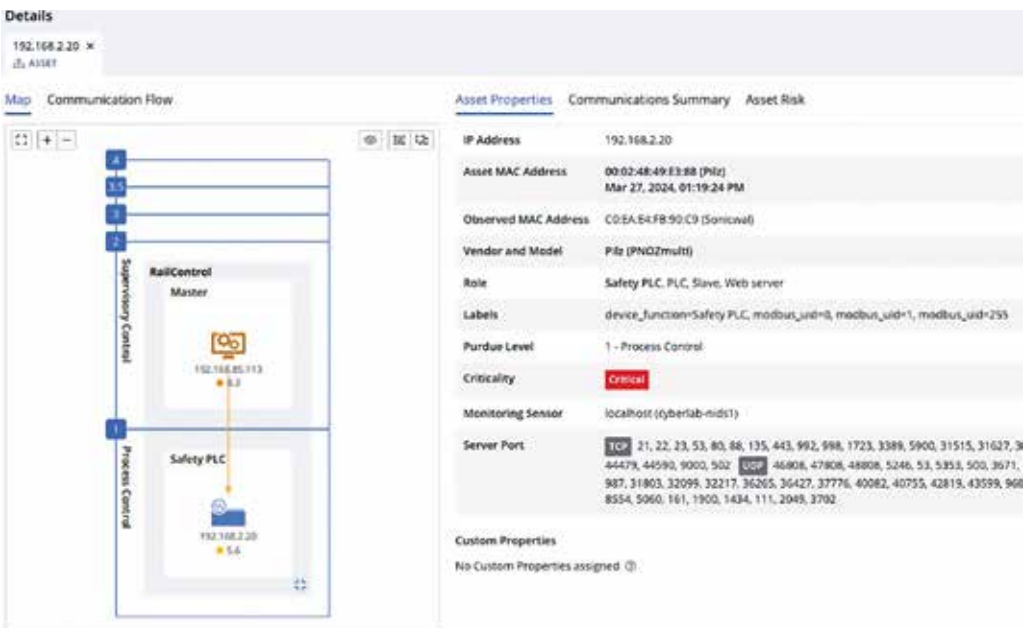

Figure 11 Understanding OT protocols and unusual activity in a control systems environment with Forescout

choose to use Fortinet for both network connectivity and an OT capable firewall, which enhances OT device and protocol protection.

OT traffic is made visible by integrating Fortinet's FortiGuard Operational Technology (OT) Security Services with a FortiGate Next Generation Firewall (NGFW) (Figure 10). FortiGuard OT Security Services continuously update signatures to identify and police most of the common OT protocols. OT functionality provides additional vulnerability protection for applications and devices from major control systems manufacturers. Updated signatures and vulnerability protection data enable a FortiGate to detect attempted exploits of known vulnerabilities. Since many OT devices run without patches, having the ability to identify exploits and protect against them with 'virtual patching' is valuable where patching is problematic, and cannot be performed. Often this make require scheduled outage, due to loss of system availability or patches may not be available, which is a challenge for unsupported legacy OT.

Additional security measures can be configured via the integrated Fortinet FortiGate and FortiSwitch, which will enable transparent security configuration with Fortinet security fabric support across both devices. This enables control system segmentation from external networks (Figure 9).

Forescout's cybersecurity platform provides visibility into all connected assets (OT, IoT and IT), continuously monitoring risk, exposure and security compliance and offers automated response and remediation capabilities.

Forescout's OT solution, eyeInspect passively monitors network traffic via a FortiSwitch mirror port. Using Deep Packet Inspection and anomaly detection eyeInspect analyses industrial protocol commands, parameters and their values. It validates network communication for compliance with the protocol specification and alerts to malformed traffic, which can indicate a zero-day or known cybersecurity exploit or failing devices. It extracts asset details from the network traffic, alerts weak security posture and critical process operations, whilst tracking process values for further customized use cases (Figure 11).

With these insights and remediation suggestions Blue Teams could mitigate security risks before they are exploited. Should anything evade defences, Forescout's rich contextual alert information, analytics dashboards and packet capture of the suspicious events supports effective root cause analysis.

The industrial network infrastructure and threat detection platforms provide the opportunity for users to understand and develop their industrial networking, security and monitoring awareness. Tables 1 & 2 highlight the differing IT and OT (ICS) impacts according to the MITRE 'ATT&CK' framework. Note the physical nature of OT impacts and potential to influence operator decision making. The MITRE ATT&CK® knowledgebase catalogues adversary tactics and techniques, from initial access through to impact in IT and OT environments.

The nuclear system can be used to demonstrate these real-world impacts in a flexible and realistic manner using representative control systems components and system architecture. Importantly, users will experience state-of-the-art, applied industrial automation control, as opposed to low fidelity virtual systems, which lack the hardware and network elements that automation engineers interact with, and which are now increasingly targeted by sophisticated adversaries and criminals.

MITRE ATT&CK® Enterprise Impact
Account Access Removal
Data Destruction
Data Encryption for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Resource Hijacking
Service Stop
System Shutdown/Reboot

Table 1. MITRE ATT&CK® Enterprise Impact
Source: https://attack.mitre.org/matrices/enterprise/

MITRE ATT&CK® ICS [OT] Impact
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information

Table 2. MITRE ATT&CK® ICS [OT] Impact
Source: https://attack.mitre.org/matrices/ics/

CYBER ATTACKS HAVE ALREADY TARGETED HAZARDOUS PROCESSES

The Triton (also known as Trisis or Hatman) malware specifically targeted Schneider Electric's Triconex Safety Instrumented System (SIS) in 2017, with the intent to manipulate industrial control systems in Middle Eastern petrochemical plants. Safety systems are used to protect systems and provide emergency shutdown of hazardous processes. Industrial safety systems run independently from the main control system to monitor and prevent potentially dangerous conditions. The malware was designed to compromise the system and manipulate the controller to override the safety system and cause a failure that could lead to a dangerous physical incident. [15, 17, 18, 19, 20]

Lessons identified included the segmentation/isolation of critical systems, network monitoring and the necessity to protect engineering workstations used to program and make configuration changes to control systems. In addition to the OT systems themselves, engineering workstations are also regarded as the 'Crown Jewels', which an organisation would seek to protect due to the opportunity they present to the adversary. Clearly defined accountability/responsibility for specific domains or environments to ensure control measure implementation and validation were also identified. [17]

TEN YEARS SINCE THE UKRAINE POWER GRID ATTACKS

On the 23 December 2015, Ukrainian media reported that a cyber-attack had left half of homes and 1.4 million people in the country's Ivano-Frankivsk region without electricity. Although services were restored within hours, this was largely due to manual intervention rather than by recovering automation systems. The initial incident was not isolated, and multiple electricity companies had been affected. The control centre systems (SCADA) were accessed remotely via compromised VPN credentials, and the intended functionality was used to open circuit breakers at 50 substations, causing outages across three electricity distribution network operators. The second phase of the campaign sought to delay restoration, corrupting firmware, destroying workstations, and severing communications. [21, 22]

The following year, in December 2016, a modular framework was used to purposely attack electrical transmissions stations, using recently installed substation controllers and protection relays. The development in modular malware demonstrated deep knowledge of grid control systems and network protocols, with a range of exploits (malware development) to target various equipment. The framework was a tool, developed not for one system, but with the capability to address multiple targets, rapidly. [23] Dragos and Office for Nuclear Regulation research "Threats and Risks to the UK Civil Nuclear Sector", highlights artificial intelligence use in the analysis of exfiltrated OT data for targeting. [7]

Time stamp	Priority	Text	Diagnostic ID
2009-01-01-01:53:54.487	Error	No valid input signal is detected	C-0009-0002
2009-01-01-01:53:54.487	Error	No valid input signal is detected	C-0009-0002
2009-01-01-01:53:54.487	Error	No valid input signal is detected	C-0009-0002
2009-01-01-01:53:54.487	Error	No valid input signal is detected	C-0009-0002
2009-01-01-01:53:54.487	Error	No valid input signal is detected	C-0009-0002
2009-01-01-01:53:54.487	Status information	Output energized	C-0009-0001
2009-01-01-01:53:54.487	Status information	Output energized	C-0009-0001
2009-01-01-01:53:54.487	Status information	Output energized	C-0009-0001
2009-01-01-01:53:54.487	Status information	Output energized	C-0009-0001
2009-01-01-01:48:14.488	Warning	The system is in state Ready for Reintegration (waiting for automatic Reintegration)	C-0009-0005
2009-01-01-01:48:14.488	Status information	Output energized	C-0009-0001
2009-01-01-01:48:14.488	Status information	Output energized	C-0009-0001
2009-01-01-01:48:14.488	Status information	Output energized	C-0009-0001
2009-01-01-01:48:14.488	Status information	Output energized	C-0009-0001
2009-01-01-01:48:14.487	Error	The "Reintegrate" bit is missing. All FS outputs on the PSS u2 system are in a safe state.	S-0100-0243
2009-01-01-01:47:44.468	Warning	The system is in state Ready for Reintegration (waiting for automatic Reintegration)	C-0009-0005
2009-01-01-01:47:44.467	Error	The "Reintegrate" bit is missing. All FS outputs on the PSS u2 system are in a safe state.	S-0100-0243
2009-01-01-01:47:43.623	Error	The configured FS output module is missing on slot 3. All FS outputs on the PSS u2 sy...	S-0200-0010
2009-01-01-01:47:39.653	Status information	An electronic module was inserted on slot 3.	S-9000-0056
2009-01-01-01:47:36.488	Status information	Output energized	C-0009-0001
2009-01-01-01:47:36.488	Status information	Output energized	C-0009-0001
2009-01-01-01:47:36.488	Status information	Output energized	C-0009-0001
2009-01-01-01:47:36.488	Status information	Output energized	C-0009-0001
2009-01-01-01:47:36.483	Error	The configured FS output module is missing on slot 3. All FS outputs on the PSS u2 sy...	S-0200-0010
2009-01-01-01:47:36.483	Status information	An electronic module was removed on slot 3.	S-9000-0057
2009-01-01-01:46:26.419	Status information	Download of device project was successful: The device project has been started. Chec...	S-9000-0021
2009-01-01-01:46:26.418	Status information	Download of device project was successful: The device project has been started. Chec...	S-9000-0021
2009-01-01-01:43:22.588	Warning	The system is in state Ready for Reintegration (waiting for automatic Reintegration)	C-0009-0005
2009-01-01-01:43:22.588	Status information	Output energized	C-0009-0001
2009-01-01-01:43:22.588	Status information	Output energized	C-0009-0001
2009-01-01-01:43:22.588	Status information	Output energized	C-0009-0001
2009-01-01-01:43:22.588	Status information	Output energized	C-0009-0001
2009-01-01-01:43:22.587	Error	The "Reintegrate" bit is missing. All FS outputs on the PSS u2 system are in a safe state.	S-0100-0243
2009-01-01-01:42:52.568	Warning	The system is in state Ready for Reintegration (waiting for automatic Reintegration)	C-0009-0005
2009-01-01-01:42:52.567	Error	The "Reintegrate" bit is missing. All FS outputs on the PSS u2 system are in a safe state.	S-0100-0243
2009-01-01-01:42:51.623	Error	The configured FS output module is missing on slot 3. All FS outputs on the PSS u2 sy...	S-0200-0010
2009-01-01-01:42:47.653	Status information	An electronic module was inserted on slot 3.	S-9000-0056

Figure 12 The engineering perspective: Safety PLC diagnostic logs and alerts.
Source: Pilz Automation Technology

3.2. Technical skills development and training

The Nuclear Simulator supports skills development by enabling further expansion of the learning environment and use during and post DCM 2026. The networking infrastructure supports future SCADA implementation, commonly used for remote control and visualisation, broadening the potential attack surface and affording Blue Team experience in implementing, monitoring and securing remote SCADA access. Large and geographical dispersed systems such as pipelines, rail and water use SCADA to centrally to monitor and control operations. The Simulator provides an environment where personnel can experience configuring, programming and diagnostics with a safety system controlling a physical process (Figure 4 and Figure 12).

Personnel will understand the fundamentals of safety-related control systems and how they are designed to provide fault-tolerant safe operation, with their programming design and redundant architecture. Users will also appreciate how safety systems could be susceptible to attack and the potential consequences. An insight into engineering diagnostics will also highlight their utility and limitations when personnel are confronted with malicious cyber events that may appear as misleading system faults or remain hidden.

Users will also gain an insight into industrial automation protocols and OT device vulnerabilities. Exposure of the industrial protocols via an OT capable network switch and firewall facilitates industrial protocols inspection for anomalous behaviour, traffic monitoring and threat detection. The system architecture is specifically designed to provide the means for the Red Team to employ various techniques to create impact scenarios illustrated in the MITRE ATT&CK® ICS shown in Table 2.

The OT security functionality with machine learning provides control system protocol awareness, asset discovery, vulnerability discovery, anomaly detection, and device behavioural analytics. This enables personnel to develop specialist OT threat hunting capability, with state-of-the-art tools. This specialised OT technical capability is still emerging, with skills scarce across industrial sectors and CNI.

4. CONCLUDING REMARKS

The Nuclear Power Plant Simulator exceeded expectations, adding a compelling OT representation to DCM. It gave Red Teams a challenging target to attack, while helping participants understand safety systems and visualise an Operational Technology process and its potential risks.

In addition to its training value, the NPP captured the interest of visitors and participants. As planning begins for next year's DCM, Special Systems remain central to the exercise's success, offering clear real-world relevance, lasting training value and demonstrable impact.

Together with the Rail Control System, the Nuclear Power Plant Simulator is expanding access to realistic OT training and creating opportunities for further research between DCM exercises. The cyber threat to OT is broad and complex, making it essential that UK Government has a shared understanding of OT risk. This knowledge is needed to protect critical assets beyond traditionally recognised Critical National Infrastructure and to safeguard the services that underpin daily life. DCM and this work are helping to develop the skills and knowledge needed to keep the trains running, the water clean and the energy flowing.

DESTRUCTIVE ATTACK TARGETS POLISH OT SYSTEMS ACROSS ENERGY SECTOR AND COMBINED HEAT AND POWER

In July 2026, the UK and European Union attributed an attack on Poland's energy grid to Russia's FSB Centre 16. The UK Government stated the reckless attack failed but could have caused 500,000 citizens to lose electricity in the depths of winter. The coordinated attacks were directed at more than 30 wind and solar farms, a manufacturing company and a large, combined heat and power plant.

Both IT systems and operational technology was affected. The Polish CERT report noted this was rarely observed and represented a significant escalation compared to previous incidents. The attacks targeted the grid substation connection points between wind, solar generation and the electricity distribution system. Internet exposed Virtual Private Network connections and compromised credentials were likely used to gain access. Custom destructive malware targeted Remote Terminal Units (RTUs) used for remote control and substation protection. The wiper malware corrupted controller firmware, causing substations to lose communication with the electricity distribution system operator, preventing remote operation. [24, 25, 26]

ONGOING ACTIVITY TARGETING INTERNET EXPOSED OPERATIONAL TECHNOLOGY USED IN CRITICAL INFRASTRUCTURE

In August 2026 the National Cyber Security Centre (NCSC) published a news article on disruptive cyber activity and the risk to internet-exposed OT. NCSC reported increased targeting of operational technology systems across multiple sectors globally, including in the UK. A range of threat actors had undertaken this activity, which had resulted in some limited real-world disruption. NCSC urged organisations that use, deploy or maintain OT systems that they treat this development seriously and review their security posture accordingly. [27]

In July, a small UK generator had suffered a four day outage as a result of Iranian affiliated activity according to The Telegraph and BBC. Department for Energy Security and Net Zero (DESNZ) confirmed the incident had impacted a small scale power generator, with no risk to the wider grid. This first reported cyber-related power outage in the UK coincided with Iranian affiliated exploitation of operational technology across US critical infrastructure sectors. [28, 29]

Earlier in March, NCSC issued an alert concerning the conflict in the Middle East and heightened cyber risk. This followed prior advisories regarding Iranian cyber actors exploiting Operational Technology in multiple critical infrastructure sectors. In April, the US Cybersecurity and Infrastructure Security Agency (CISA) published an advisory regarding ongoing cyber exploitation of internet-connected operational technology by Iranian-affiliated advanced persistent threat (APT) actors. [30, 31]

The CISA advisory provided guidance on detecting malicious code changes in Rockwell Automation controller programs and targeting of other programmable logic controllers (PLCs) from other leading manufacturers, including Scheider Electric and Siemens. These actions disrupted PLCs across several U.S. critical infrastructure sectors through malicious project file interactions and manipulation of data on human machine interface (HMI) and supervisory control and data acquisition (SCADA) displays, resulting in operational disruption and financial loss.

A joint advisory published by the US, Canada, Israel and the UK highlighted an earlier Iranian Government's Islamic Revolutionary Guard Corps affiliated campaign targeting operational technology. The actors supplanted existing ladder logic program files with their own, renamed devices likely to delay owner access, reset software versions to older versions, disabled upload and download functions, and changed the default port numbers. The deeper device access obtained enabled local network level access which could permit additional, more profound cyber-physical effects on processes and equipment. The advisory noted that the National Cyber Security Centre had observed the targeting of PLC devices in the United Kingdom, posing an ongoing risk to UK organisations that use operational technology. [32]

ACKNOWLEDGEMENT

The authors wish to extend their gratitude to Pilz and Forescout for their generous and timely support.

DR RICHARD PIGGIN ENGD CENG MIET CHCSP MCIIS MBCS

Richard is a Nuclear Security Inspector with ONR. He is also a recent Pinkerton Prize winner for best technical paper in the Nuclear Future Journal. He is a Chartered Engineer and recently became a Chartered Cyber Security Professional. Richard has an Engineering Doctorate from the University of Warwick (industrial networking), and a Cyberspace Operations PgDip from Cranfield University. He was a co-instigator/contributor to the IET Code of Practice: Cyber Security and Safety. www.researchgate.net/profile/Richard-Piggin/publications

CAPTAIN JOSEF YALVAC BSC(HONS) CMGR CMI IMI IENG RSIGNALS

Captain Yalvac joined the Army 10 years ago, originally as a Communications Systems Engineer. Following commissioning and desiring to reawaken his practical technical skills he joined the Army Cyber Association and attended his first Defence Cyber Marvel, appointed as the Special Systems Lead. His educational background is in Systems Engineering and Management. He recently gained his Chartership in management from CMI.

ACRONYMS

APT	Advanced Persistent Threat A well-resourced, highly skilled group, frequently backed by a nation-state, which executes prolonged, targeted cyber intrusions to remain undetected and has the capability to cause significant harm.
CERT	Computer Emergency Response Team Cyber security professionals tasked with cyber incident detection, response, prevention, and reporting.
CISA	Cybersecurity and Infrastructure Security Agency United States cyber security and infrastructure protection agency.
CNI	Critical National Infrastructure Essential national assets, services and systems whose loss or disruption would have a major impact on security, economy, health or safety.
DCM	Defence Cyber Marvel A series of UK-led international cyber exercises, currently in its fifth year.
DCS	Distributed Control System Industrial automation system where control is decentralised across equipment. Commonly used in large and complex processes such as chemicals, refining and power generation.
DMZ	Demilitarized Zone A network segment that acts as a buffer between two networks, restricting and controlling traffic flow.
DESNZ	Department for Energy Security and Net Zero UK government department responsible for energy security, protecting billpayers and achieving net-zero goals.
HMI	Human Machine Interface Operator display and interaction system used to monitor and control industrial processes.
I/O	Inputs/Outputs Connections for sensors and actuators. Often connected to a safety PLC via an industrial Ethernet network using a safety protocol.
ICS	Industrial Control Systems Systems used to monitor and control industrial processes; often used interchangeably with Operational Technology (OT).
IET	Institution of Engineering and Technology Professional engineering institution based in the UK.
IT	Information Technology Systems and infrastructure used for business computing, communications and data management.
NCSC	National Cyber Security Centre UK authority providing cyber security guidance, incident response and threat intelligence.
NGFW	Next Generation Firewall Security appliance that processes network traffic and applies advanced inspection rules. It analyses traffic origin, destination, connection legitimacy and content to identify and block threats hidden within normal-looking traffic.
NIST	National Institute of Standards and Technology US organisation that develops technical standards, frameworks and cyber security guidance.
NPP	Nuclear Power Plant Facility that generates electricity using nuclear fission.
ONR	Office for Nuclear Regulation Independent UK regulator responsible for nuclear safety, security and safeguards.
OT	Operational Technology Hardware and software used to monitor and control physical industrial processes; often synonymous with ICS.
PLC	Programmable Logic Controller Industrial controller used to automate and control processes. Typically programmed using industrial languages such as ladder logic and safety function block diagrams.
RTU	Remote Terminal Unit Special-purpose operational technology used to connect and control field equipment from a SCADA system in a control centre.
PWR	Pressurised Water Reactor The most common nuclear reactor type worldwide. Uses ordinary water as both coolant and neutron moderator, operating at high pressure (typically 150-160 bar) to prevent boiling. Heat is transferred from a primary circuit to a secondary steam cycle for electricity generation.
SCADA	Supervisory Control and Data Acquisition System used for centralised monitoring, control and data analytics of distributed assets such as water networks, wind farms, petrochemical facilities and railways.
SIS	Safety Instrumented System Independent protection system that detects unsafe process conditions and automatically returns the process to a safe state. Typically used alongside a DCS to reduce the consequences of hazardous events to an acceptable level.
VPN	Virtual Private Network Technology that provides secure connectivity between devices located in physically separate locations.

REFERENCES

[1] HM Government, UK to lead multinational cyber defence exercise from Singapore, 2026 https://www.gov.uk/government/news/uk-to-lead-multinational-cyber-defence-exercise-from-singapore

[2] CERT-UA, War and Cyber: Three years of struggle and lessons for global security, 2025 https://cip.gov.ua/services/cm/api/attachment/download?id=69131

[3] NIST, NIST SP 800-82r3 Guide to Operational Technology (OT) Security, 2023 https://doi.org/10.6028/NIST.SP.800-82r3

[4] Forescout, 2025 Threat roundup 2025, 2026 https://www.forescout.com/resources/2025-threat-roundup/

[5] NCSC, Cyber Security Body Of Knowledge (CyBOK), 2021 https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf

[6] Heightened threat of state-aligned groups against western critical national infrastructure https://www.ncsc.gov.uk/news/heightened-threat-of-state-aligned-groups, 2023

[7] Threats & Risks to the United Kingdom's Civil Nuclear Sector, 2025 https://www.onr.org.uk/media/qt0jmzfw/dragos_wp_emergingrisksonr_final.pdf

[8] Ralph Langer, To Kill a Centrifuge, 2013 https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[9] HM Government, UK exposes Russian spy agency behind cyber incidents, 2022 https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents

[10] Richard Piggin, Enhancing Civil Nuclear Cyber Security, Nuclear Future Journal, 2024 https://www.researchgate.net/publication/378309998_Enhancing_Civil_Nuclear_Cyber_Security

[11] IET, Cyber security and safety code of practice, 2020 https://www.ncsc.gov.uk/news/code-of-practice-cyber-security-and-safety-in-engineering

[12] MITRE, MITREATT&CK ® Enterprise Impact https://attack.mitre.org/matrices/enterprise/

[13] MITRE, MITRE ATT&CK ® ICS Impact https://attack.mitre.org/matrices/ics/

[14] HM Government, National Cyber Strategy 2022, 2022 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[15] MIT, Triton is the world's most murderous malware, and it's spreading, 2019 https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[16] Wired, Unprecedented Malware Targets Industrial Safety Systems in the Middle East, 2017 https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/

[17] Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware, 2017 https://hub.dragos.com/hubfs/116-Whitepapers/TRISIS-01.pdf

[18] Wired, Menacing Malware Shows the Dangers of Industrial System Sabotage, 2018 https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/

[19] US Department of Justice, United States v. Gladkikh, 1:21-cr-00442 2021 https://www.justice.gov/d9/press-releases/attachments/2022/03/24/dc_gladkikh_0.pdf

[20] US Department of Justice, Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide, 2022 https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historicalhacking-campaigns-targeting-critical

[21] Richard Piggin, Cyber security trends: What should keep CEOs awake at night, International Journal of Critical Infrastructure Protection, 2016 https://doi.org/10.1016/j.ijcip.2016.02.001

[22] Richard Piggin, Comment: Are you ready for the increasing focus on cyber-risk, 2016 https://eandt.theiet.org/2016/04/18/comment-are-you-ready-increasing-focus-cyber-risk

[23] Dragos, Ten Years After Ukraine's Power Grid Cyberattack, 2026 https://www.dragos.com/blog/ukraine-power-grid-cyberattack-crashoverride-10-year-lessons

[24] HM Government, UK and EU strike Russian cyber networks with new sanctions, 2026 https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

[25] European Union, Cyber / Russia: Statement by the High Representative on behalf of the European Union denouncing Russia's malicious cyber ecosystem targeting the EU, its member states and international partners, 2026 https://www.consilium.europa.eu/en/press/press-releases/2026/07/13/cyber-russia-statement-by-the-high-representative-on-behalf-of-the-european-union-denouncing-russia-s-malicious-cyber-ecosystem-targeting-the-eu-its-member-states-and-international-partners

[26] CERT.PL Energy Sector Incident Report - 29 December 2025, 2025 https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025

[27] NCSC, Disruptive cyber activity highlights risk from internet-exposed systems and edge devices, 2026 https://www.ncsc.gov.uk/news/disruptive-cyber-activity-highlights-risk-from-internet-exposed-systems-and-edge-devices

[28] The Telegraph, Iranan hackers shutdown UK power plant, 2026 https://www.telegraph.co.uk/news/2026/08/22/iranian-hackers-shut-down-uk-power-plant/

[29] BBC, Iran-linked hackers behind cyber attack that shut down power plant, reports say, 2026 https://www.bbc.co.uk/news/articles/ce9793g34yvo

[30] NCSC, Alert: NCSC advises UK organisations to take action following conflict in the Middle East, 2006 https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east

[31] CISA, Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure, 2026 https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

[32] CISA, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities, 2024 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a