Project and Dissertation

May 2025

Securing Communications Between Safety-Critical Industrial Control Systems

Rowan Edlington

Author's Note

This dissertation was completed between September 2024 and May 2025 as part of a degree apprenticeship with EDF, contributing towards a Cyber Security Technical Professional Integrated Degree with the University of the West of England (UWE) Bristol and Gloucestershire College. While undertaken during my employment at EDF and with relevance to the nuclear industry, all views expressed and work conducted are solely my own and do not represent the views or positions of EDF or any of its affiliates.

Abstract

This project addresses the challenge of securing communications between Industrial Control Systems (ICS) at Électricité de France (EDF) Energy's upcoming nuclear power plants (NPP) – Hinkley Point C (HPC) and Sizewell C (SZC). Given the safety-critical nature of these systems, ensuring the integrity, availability, and resilience of ICS communications is crucial. The project aims to evaluate and recommend a secure, suitable solution capable of protecting real-time operational data flows against modern cyber threats, in compliance with both the United Kingdom's (UK) regulatory frameworks and international standards.

Adopting a systems engineering approach, the project employs the V-lifecycle model to guide requirement derivation, technology selection, and validation. Detailed analysis was conducted on three candidate technologies: a data diode, an industrial firewall, and a hardware encryption appliance. Derived requirements prioritised low-latency, protocol compatibility with IEC104, cyber resilience, and long-term maintainability. Based on weighted scoring using engineering methods, Blueskytec's ICSProtect encryption device was selected for further evaluation.

Testing was carried out in a simulated ICS environment, using ICS equipment, and emulated IEC104 traffic. Functional tests confirmed reliable bidirectional communication and protocol adherence, while latency and throughput metrics remained within operational tolerances. Non-functional assessments demonstrated the device's suitability for long-term deployment, with strong key management based on a one-time pad system. Cybersecurity testing revealed strong resistance to traffic manipulation and exfiltration due to the ICSProtect's encryption and filtering mechanisms.

Despite some limitations – such as the use of non-native IEC104 hardware and limited analysis tools – the project provides EDF with a technically verified solution capable of enhancing ICS security. The findings support the potential procurement and deployment of ICSProtect within nuclear power plants and lay the groundwork for further research into protocol interoperability, endpoint defence, and real-world resilience testing. This work contributes meaningfully to the protection of UK critical national infrastructure against evolving cyber threats.

Acknowledgements

This project has been a great challenge and a huge learning opportunity. I've thoroughly enjoyed the entire process. There are a few people I'm especially grateful for, as this project wouldn't have been as successful without them.

I would like to extend my gratitude to Dr. Andrew McCarthy for his excellent guidance and valuable advice throughout this project. Your expertise has been incredibly helpful, and I've really enjoyed our discussions.

I also want to thank Guido Villacis Rivas for being a fantastic manager and for the encouragement and support provided during the project. Additionally, I have received some amazing support from my colleagues, who have provided feedback and listened to my ideas.

I'm also grateful to Dr. Chris Mobley and the team at Blueskytec for generously sharing the information and resources that helped to make this project a success. I'm excited to be able to share Blueskytec with the academic world.

Lastly, to my partner Matthew, thank you for your endless support, patience, and for always being there to talk through ideas. Your encouragement means the world to me.

Table of Contents

Table of Figures

Table of Tables

Abbreviations

Acronym	Expansion
AES	Advanced Encryption Standard
AI	Artificial Intelligence
APCI	Application Process Control Interface
APDU	Application Protocol Data Unit
APT	Advanced Persistent Threat
ASCII	American Standard Code for Information Interchange
BEIS	Department for Business, Energy & Industrial Strategy
BST	Blueskytec
CIA	Confidentiality, Integrity, Availability
CBC	Cipher Block Chaining
CMAC	Cipher Message Authentication Code
CNI	Critical National Infrastructure
COTS	Commercial Off-The-Shelf
CT	Cyber Test
EDF	Électricité de France
ECB	Electronic Codebook
FIPS	Federal Information Processing Standards
FPGA	Field-Programmable Gate Array
FT	Functional Test
HMI	Human-Machine Interface
HPC	Hinkley Point C
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
ID	Identification
IEC	International Electrotechnical Commission
INCOSE	International Council on Systems Engineering
IP	Internet Protocol
IT	Information Technology
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
MAC	Media Access Control
MCDM	Multi-Criteria Decision Making
MITM	Man-In-The-Middle
NCSC	National Cyber Security Centre

NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
NT	Non-Functional Test
ONR	Office for Nuclear Regulation
OS	Official Sensitive
OT	Operational Technology
OTP	One-Time Pad
PLC	Programmable Logic Controller
PUF	Physically Unclonable Function
QC	Quality Control
RSA	Rivest-Shamir-Adleman
SIL	Safety Integrity Level
SL	Safety Level
SMART	Specific, Measurable, Achievable, Realistic, Timebound
SNI	Sensitive Nuclear Information
SOC	Security Operations Centre
SP	Special Publication
SSL	Secure Sockets Layer
ST	Safety Test
SyAPs	Security Assessment Principles
SZC	Sizewell C
TAG	Technical Assessment Guide
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UK	United Kingdom
USB	Universal Serial Bus
WSM	Weighted Sum Model

1 Introduction

EDF Energy, a United Kingdom (UK) energy company owned by Électricité de France (EDF), operates all nuclear power plants (NPP) in the UK and is expanding the nuclear fleet. EDF will be constructing two new NPPs: Hinkley Point C (HPC) and Sizewell C (SZC). This project addresses securing communications between Industrial Control Systems (ICS) for both HPC and SZC.

ICS are vital in safety-critical environments like NPPs, controlling key processes to ensure nuclear safety, especially in the event of failure (Karmakar; et al, 2023). These systems are prime targets for cyber attackers, making their security crucial.

As discussed in literature, the CIA Triad – confidentiality, integrity, and availability – serves as a foundational cyber-security framework. For NPPs, integrity and availability take precedence, ensuring data accuracy for reliable control signals, and maintaining system operations to prevent disruptions. Although confidentiality is important for preventing unauthorised system access, the primary focus is on operational functions.

In addition to CIA, other principles are essential for ICS. Safety ensures systems do not cause harm to people and the environment; reliability ensures consistent functionality; resilience allows recovery from disruptions; and maintainability emphasises efficient repairs and updates. These principles collectively improve ICS security.

All ICS in the NPPs are classified into security levels based on their nuclear safety significance and other contributing factors such as commercial impact. The highest level is reserved for safety systems, designed to prevent accidents (Karmakar et al., 2023). This hierarchical framework ensures resources are allocated proportionally to the potential impact of ICS compromise.

Many ICS are being developed for both HPC and SZC; this project focuses on two in particular. Each of the selected ICS performs a distinct function, and they operate at different security levels. The specific architecture of these two ICS will not be discussed in detail, to avoid any breach of UK Official Sensitive: Sensitive Nuclear Information (OS:SNI).

1.1 Project Aims and Objectives

The primary aim of this project is to develop a secure solution for facilitating communication between the two ICS. The two systems require secure communications to maintain real-time operational availability and data integrity. The systems are scheduled for development within the next year, and any selected product must undergo a procurement and qualification process before deployment.

1.1.1 Objectives

- Analyse the selected ICS using documentation and applicable standards to assess ICS architecture, compatibility and security needs to develop a set of requirements based on the needs of EDF.
- Compare at least three existing communication solutions by assessing their ability to meet the requirements. The level of compliance will demonstrate the suitability of each solution in providing an adequate level of security to the system. Select an appropriate solution based on this analysis.
- Evaluate the selected solution by testing its functionality and resilience to cyber-attacks in a simulated lab environment. Verify that the testing results meet the specified requirements, providing clear justifications to produce a thorough assessment of the solution's feasibility for deployment.
- Inform stakeholders at EDF of the evaluation results to support the decision-making process for product procurement within the next six months.

1.2 Project Outline

This project adopts an engineering perspective focused on the high-security needs of safety-critical systems.

A comprehensive review of literature on ICS vulnerabilities, historical attacks, and relevant standards is included in Chapter 2, identifying potential solutions for securing ICS networks.

Chapter 3 discusses the V-lifecycle methodology, which informs the stages of this project.

Chapter 4 defines specific requirements that the final solution must meet, based on the literature review and EDF documentation. It then quantitatively analyses the three researched solutions: a data diode, an industrial firewall, and a hardware encryption device against these requirements.

Chapter 5 details the system architecture and network design of the chosen hardware encryption device from Blueskytec, including a testbed designed to simulate real-world conditions to assess solution effectiveness.

Chapter 6 outlines the integration of the solution into the simulated ICS environment.

In Chapter 7, the solution’s functionality and deployment suitability are verified against defined requirements. It concludes that the device is suitable for deployment, with additional controls like strong endpoint security.

Finally, Chapter 8 summarises this project's overall success, highlighting its strengths and limitations.

2 Literature Review

ICS are essential in modern industrial and safety-critical sectors, such as NPPs, where they monitor and control processes using a combination of hardware and software. These systems include sensors, actuators, Programmable Logic Controllers (PLC), and Human Machine Interfaces (HMI) to ensure efficient and safe operations (Cappelli, 2023). In NPPs, ICS are crucial in preventing accidents, predicting failures, and activating safety mechanisms (Karmakar et al., 2023). A typical NPP features around 10,000 sensors and 5,000 km of ICS cabling, making ICS one of the heaviest non-building NPP structures (Arinze et al., 2020). As ICS grow more complex and digitalised, they also face increased cyber threats (Arinze et al., 2020).

The key distinction between the security of ICS or operational technology (OT) and traditional information technology (IT) is their core objectives: IT prioritises privacy and financial concerns, while OT emphasises safety and resilience due to its interaction with physical processes (Conklin, 2016). Although some propose applying IT principles like the CIA triad to OT security (McLaughlin et al., 2016), this perspective fails to address the unique security needs of OT, where failures can have severe, potentially life-threatening consequences (Karmakar et al., 2023). In contrast, IT failures generally result in financial or data losses, which are less catastrophic.

Furthermore, IT principles often fall short for OT because IT systems have shorter lifecycles and are regularly updated, while OT components can remain operational for 15-20 years or more, lacking modern security measures (McLaughlin et al., 2016). However, this dismissive view of IT does neglect the developing landscape of converged IT/OT environments. As OT increasingly incorporates commercial off-the-shelf (COTS) hardware and software, it becomes more vulnerable to IT threats, making IT security practices, such as zero-trust architecture (Rose et al., 2020), relevant and potentially beneficial for enhancing OT security.

ICS face significant vulnerabilities, a fact proven by the Stuxnet worm, which marked a critical milestone in ICS security. In 2010, Stuxnet targeted Siemens control systems in an Iranian nuclear facility, demonstrating that cyberattacks could lead to catastrophic physical damage. This sophisticated malware spread via infected USB drives, infiltrating air-gapped systems to exploit zero-day vulnerabilities and sabotage gas centrifuges by manipulating their output frequency, resulting in substantial destruction. (Richardson, 2011)

The sophistication and stealth of Stuxnet is alarming; it infected numerous computers worldwide but activated its payload only on specific targets, showcasing advanced cyber capabilities. This incident illustrated how nation-states could weaponise code for strategic physical consequences without direct military conflict, setting a dangerous precedent for future ICS attacks. It revealed vulnerabilities in air-gapped networks, emphasising that cybersecurity for ICS can no longer be an afterthought. (Richardson, 2011)

Stuxnet set the stage for modern ICS attacks, as evidenced by the 2016 CRASHOVERRIDE malware in Ukraine, which targeted a transmission substation using the insecure IEC-104 protocol. The IEC-104 protocol is especially susceptible to reverse engineering due to its lack of built-in security features like authentication and encryption, which also exposes it to cyber-attacks when transmitted over unsecured IP networks. Potential threats to IEC-104 include packet interception, altering transmitted data and injecting spoofed messages (Matoušek, 2017). CRASHOVERRIDE disrupted grid operations and highlighted adversaries' sophisticated knowledge of ICS. It demonstrates the need for integrated cybersecurity measures throughout the lifecycle of ICS, particularly when IEC-104 protocol is used. (Dragos, 2017)

The rise of Advanced Persistent Threats (APTs) poses a serious risk to the UK power grid and NPP, as evidenced by recent attacks on Ukraine's power grid. According to Dragos' 'Year in Review' report, nine APT groups targeted OT environments in 2024, with three capable of affecting physical operations. Alarmingly, 70% of OT vulnerabilities are deep within networks, making detection and remediation challenging. (Dragos, 2025)

No OT system can achieve complete visibility of vulnerabilities, rendering it impossible to prevent all intrusions. Even advanced frameworks like National Institute of Standards and Technology (NIST) or IEC62443 depend on reactive defences. Additionally, many OT systems rely on legacy components that have operated for 15-20 years without upgrades, creating a vulnerable long-term attack surface, particularly concerning for NPPs with ageing ICS not designed to withstand modern cyber threats. Despite improvements in defensive strategies, APTs use stealthy tactics like slow exfiltration to evade detection, as demonstrated by both Stuxnet and CRASHOVERRIDE, where intruders remained undetected for months. The evolution of such APTs illustrates that cyber warfare now poses as significant a threat as traditional military actions.

Protecting NPP ICS demands a specialised approach that goes beyond singular IT-focused frameworks. The UK mandates compliance with the NCSC Cyber Assessment Framework and the Minimum Cyber Security Standard, but their IT-centric focus is less effective for the complexities of OT environments.

The UK Government's former Department for Business, Energy & Industrial Strategy (BEIS) published a '2022 Civil Nuclear Cyber Security Strategy' report, which offers a relevant OT cyber framework by outlining governance structures and highlighting key risks such as ransomware and supply chain vulnerabilities, though it lacks detailed technical guidance.

The Office for Nuclear Regulation (ONR) provide guidance for regulatory judgements and recommendations through the Security Assessment Principles (SyAPs) and their Technical Assessment Guides (TAGs), which adopt a layered, defence-in-depth approach. 'SyDP5' mandates the inclusion of reliability, resilience, and fail-secure mechanisms to prevent unauthorised changes or disruptions, while 'SyDP7' stresses the importance of integrating security throughout the design, implementation, and operational stages of ICS (ONR, 2022). These are the key concerns of OT security and take precedence over IT principles.

Unlike generic IT standards like ISO27001, NIST Special Publication 800-82 (Stouffer et al., 2023) offers ICS-specific guidance. Stouffer et al. (2023) highlight the long lifespans of OT assets and the importance of investing in reliability and safety. They caution that legacy protocols lack built-in cryptographic protection. NIST recommends implementing defence-in-depth in alignment with the ONR, echoing the IEC62443 series known for its layered security model. Furthermore, the International Atomic Energy Agency (IAEA) Nuclear Security Series 42-G provides guidance on graded, layered security for nuclear contexts.

The key principles for protecting OT, outlined by these standards, are defence-in-depth, secure-by-design, and zero-trust. Defence-in-depth involves multiple protective layers to effectively mitigate risks (Bouhdada & Ayala, 2024). A graded approach ensures security measures correlate with the potential impact of attacks, optimising resource allocation (IAEA, 2021), in line with the hierarchical Safety Integrity Levels (SIL) of IEC61508 and Security Levels (SLs) of the ONR. Zero-trust principles, which reduce implicit trust in networks, are particularly crucial for ICS due to the significance of safety-critical systems (NIST, 2024). Secure-by-design emphasises integrating security from the beginning of system development and closely aligns with the ONR's SyDP7 (ONR, 2022). These principles will be considered throughout this project.

To protect the integrity of critical ICS in NPPs, systems at different SLs are typically isolated. When communication is needed, it is strictly controlled and typically unidirectional. A data diode is a hardware device that enforces one-way communication, allowing information to flow only from a higher to a lower SL system, preventing lateral movement and unauthorised access to higher SL systems (Kumar et al., 2023).

Kumar et al. (2023) propose implementing data diodes to secure critical systems from external interference, meeting reliability standards. The system can incorporate redundant diodes to maintain communication during failures, aligning with defence-in-depth principles. In TAG51, the ONR (2025) highlights redundancy as a key element of achieving resilience. Widely used in high-risk environments like NPPs, data diodes support layered security for safety and reliability, making them a viable option for this project.

Alternatively, firewalls facilitate controlled bidirectional communication between networks based on set rules (Siemens, 2020). The effectiveness of a firewall is reliant configuration and regular maintenance to keep them up to date. Outdated rules and poor setups can create vulnerabilities, exposing networks to threats like backdoor exploits, malware, and denial-of-service attacks. As a result, their suitability for this project may be limited.

According to Siemens (2020), while firewalls are important, data diodes are becoming standard in protecting critical infrastructure, especially where cybersecurity risks are intolerable. This project could consider combining data diodes with firewalls to enhance overall network security and reduce attack risks, while ensuring necessary operational connectivity.

Firewalls and data diodes have been established components in network security for an extended period, and their implementation is widely recognised as a best practice within the industry. However, due to the evolving complexity of ICS networks and the increasing sophistication of APTs, there is a need to adopt more advanced technological solutions.

Blueskytec (BST) offers a hardware-based encryption solution for securing ICS in critical infrastructure. This device establishes a secure communication line using a One-Time-Pad (OTP) for key management and Twofish for data encryption. Unlike firewalls and data diodes that enforce communication boundaries, BST provide hardware-level encryption, ensuring data integrity without relying on software or configuration management (Mobley, 2022), consequently decreasing the attack surface significantly. However, BST's approach is unverified in NPPs, making it a less documented solution. Therefore, testing and verification in NPP environments is needed to prove its applicability.

Encryption is often avoided in OT systems due to concerns about data validity, potential corruption, and added latency. OTPs, while being theoretically unbreakable (Easttom, 2016), are generally discouraged due to practical challenges, such as secure distribution and key management. However, BST avoids key distribution issues by pre-placing OTPs in hardware.

Carlson *et al.* (2022) argue that contrary to OT, cryptographic standards change frequently, resulting in outdated cryptographic protocols when safety-critical systems do eventually receive firmware updates. Although BST devices do not require firmware updates, the cryptographic protocols are fixed, which could be problematic in an evolving cyber world.

While IEC62443 and NIST SP 800-82 suggest applying cryptography to OT data in transit, protocols like IEC104 simply do not have the capabilities in-built. Using BST would allow this functionality. However, NIST SP 800-82 suggests using a Federal Information Processing Standards (FIPS) certified algorithm, which Twofish is not.

Despite this, Schneier et al. (2000) assert that Twofish "far surpasses" other FIPS algorithms. Though this claim lacks authoritative backing, they argue that Twofish's security stems from its advanced design, which features a 16-round Feistel structure, key-dependent substitution-boxes, a complex key schedule, and matrices for strong diffusion. These elements, along with pre-computed key material and modular arithmetic, solidify high resistance to differential, linear, and related-key cryptanalysis. Consequently, no successful cryptanalytic attacks against the full Twofish cipher have been demonstrated in practice. Furthermore, Ghosh (2020) finds Twofish to outperform AES and Blowfish in terms of time and throughput, making it suitable for low-latency safety-critical environments.

The literature highlights that while data diodes provide effective one-way communication and network isolation, they do not ensure data integrity and cannot prevent unauthorised access or tampering. Firewalls, although flexible, depend on proper configuration and management, making them susceptible to misconfigurations and failing to guarantee the confidentiality and integrity of plaintext data transfers. Conversely, while encryption is a more robust solution, it is often overlooked in OT environments for less intrusive security measures. This study will further explore the suitability of these three products for NPPs, providing insights into the feasibility of using emerging advanced technologies to secure communications within safety-critical ICS.

3 Methodology

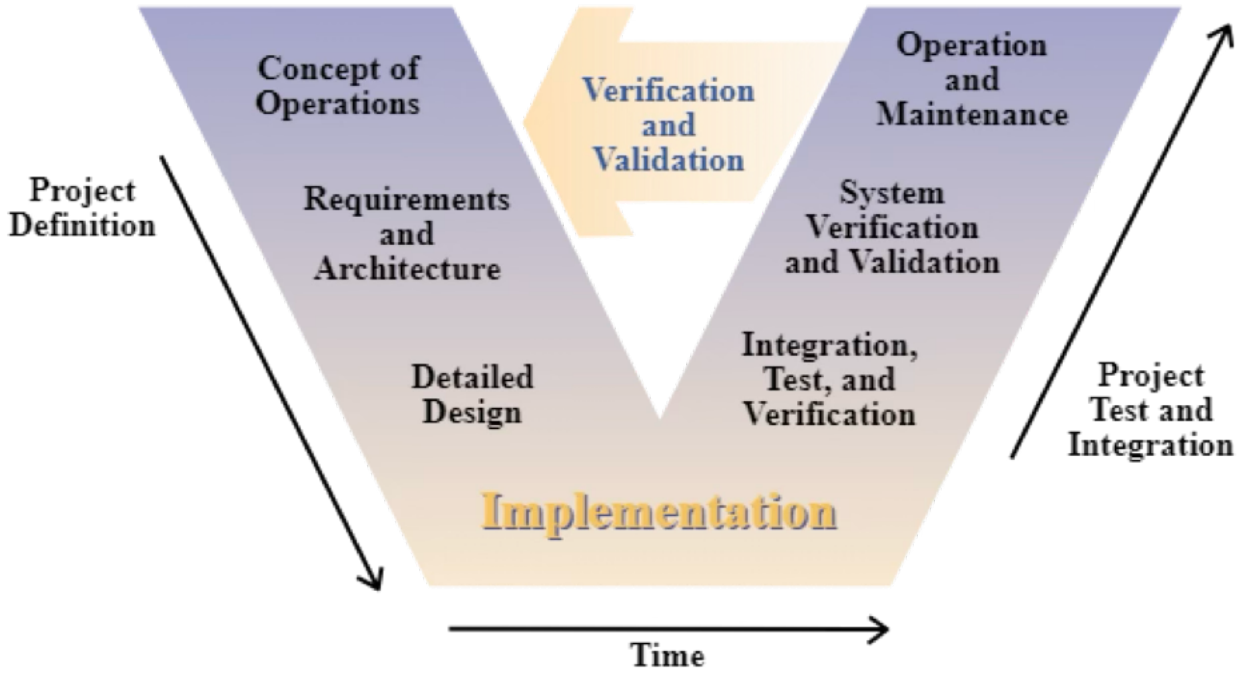

Figure 1 V-Life cycle Model (Anon, 2005)

This project adopts the V-Model lifecycle, a structured approach to systems engineering that is widely used across EDF engineering functions, promoting consistent development and validation processes. The V-Model aligns with the IEC15288 standard, which defines systems engineering as a transdisciplinary approach facilitating the development, use, and retirement of engineered systems (IEC, 2023). This standard recommends lifecycle models like the V-Model to ensure quality throughout all stages (INCOSE, 2023). This framework is particularly suitable for developing complex systems like the ICS in nuclear environments, where security, safety, and regulatory compliance are essential.

While alternative models such as Waterfall and Agile were considered, they present significant drawbacks. The Waterfall model, with its linear structure and emphasis on documentation (Balaji & Murugaiyan, 2012), lacks the necessary validation for complex projects. Testing only starts post-development, risking undetected deviations from requirements at earlier phases, which is unacceptable for safety-critical systems.

Agile offers incremental delivery (Rubio, 2022) and adaptability but often sacrifices comprehensive documentation and traceability in favour of speed (Stephen & Oriaku, 2014). This can lead to insufficient validation of system outputs against requirements, compromising regulatory and safety compliance. The V-Model mitigates these risks by linking development with validation stages, ensuring continuous checks against requirements and confirming that the system achieves its intended purpose.

3.1 Concept of Operations

The concept of operations, which evaluates the feasibility and rationale for developing a system, has already been performed as part of this dissertation. The customer has defined the problem, which has been introduced and discussed in the Aims and Objectives.

3.2 Requirements Analysis

The requirements analysis stage focuses on defining and deriving the functional and non-functional requirements of the solution. These requirements will include both system performance and security specifications. The objective is to thoroughly define the parameters that the solution must meet, particularly with regard to nuclear safety and cybersecurity.

Multiple products will be assessed against the set requirements to select the most suitable solution for this project. A product will be selected based on its initial suitability against the requirements.

3.3 Solution Design

The design stage involves discussing the design and architecture of the selected product to understand its functionality and security features.

A solution network design will be produced for the testing environment to ensure that the solution can be tested in a realistic, representative environment. It cannot be implemented directly into the actual ICS due to previously discussed information sensitivity concerns.

3.4 Implementation

In this phase, the solution is implemented into a test network environment. The focus is on integrating this solution into the designed simulation network and ensuring functionality.

3.5 Testing

Integration and testing are critical in the V-Model lifecycle. This stage ensures that the system components work together as intended and that the system meets the defined requirements. The tests will be based on the requirements. The selected solution will undergo rigorous testing to validate its effectiveness in a safety critical and real-time environment.

3.5.1 Verification and Validation

The verification phase ensures that the system not only meets the design specifications but also satisfies the operational requirements in real-world conditions. It also checks the alignment with security and safety standards. This stage will involve conducting validation tests on the solution to confirm that it upholds the nuclear safety classification standards and supports secure communication between the ICS.

3.6 Operations and Maintenance

Once verification and validation are completed successfully, the selected solution can be deployed into the operational ICS. While this stage will not be explicitly covered in this project, recommendations for future deployment considerations will be provided based on the results of the testing.

4 Requirements Analysis

4.1 Requirement Analysis Process

The requirements derivation process adhered to the INCOSE (2023) 'Systems Engineering Handbook' for a traceable approach, aligning requirements with quality characteristics (QCs). As defined by IEC15288 (2023), a QC is a characteristic of a product, process, or system that ensures the system meets specific goals and maintains high quality throughout its lifecycle (INCOSE, 2023). The most relevant QCs were chosen to guide this project, as in Table 1.

QC Approach	Approach Aims	Requirements Category
Logistics Engineering	System support for the entire lifecycle.	Non-Functional
Reliability, Availability, Maintainability Engineering	System performance with minimal failure, operational when needed, and restored to a functional state after failure.	Functional
System Safety Engineering	Reduces the likelihood and level of harm to people, assets and the wider environment.	Safety
System Security Engineering	Identifies, protects from, detects, responds to, and recovers from disruptive events, including cyber.	Security

Table 1 Quality Characteristics (INCOSE, 2023)

Requirements are detailed statements of what a system must achieve, broken down into actionable, measurable tasks. SMART criteria (Doran, 1981) ensure clarity, measurability, and verifiability (Mannion and Keepence, 2004). Requirements will use MUST and SHOULD as specified by Bradner (1997).

This project defined requirements by analysing customer documentation, relevant ICS literature and regulatory requirements such as the SyAPs (ONR, 2022). Functional requirements were derived by assessing system capabilities against operational conditions, while non-functional requirements were based on environmental and lifecycle constraints. Safety and cybersecurity requirements were derived according to relevant standards and historical attacks.

When selecting a product, regulatory and contractual considerations must also be addressed. The budget should cover initial costs and ongoing maintenance, including replacement parts, software updates, and security patches. Confirmed regulatory compliance with the ONR’s safety and security standards and a qualification process are necessary for successful tender. However, cost and contractual considerations are outside the scope of this project.

4.2 Requirements Derivation

The following requirements have been defined and derived into single, atomic statements.

4.2.1 Functional Requirements

F01: The product MUST support the IEC 104 protocol for all communications.
The existing systems use the IEC-104 protocol for communications. IEC-104 may not be compatible with all products.

- **F01-1**: The product MUST be compatible with the IEC104 communication stack.

F02: The product MUST facilitate bidirectional communication between the two systems at all times.
Bidirectional communication is essential for sending control commands and receiving communication feedback in real-time. Without this, the two ICS would lose the ability to synchronise, resulting in delays or failures in safety-critical tasks.

- **F02-1**: The product MUST support send operations.
- **F02-2**: The product MUST support receive operations.

F03: The product MUST achieve a communication latency below 250µs during normal operations.
Low latency is crucial in safety-critical applications to ensure timely execution of commands and responses. Excessive delays could jeopardise safety or system performance.

- **F03-1**: The product MUST minimise data transmission times to achieve a latency below 250µs during normal operations.

F04: The product MUST handle at least 800 updates per second during normal operations.
The ability to process high message volumes ensures the system remains functional during peak demand, without losing or delaying critical data. 800 updates per second was specified in customer documentation as 20% higher than the expected maximum of realistic system operations required.

- **F04-1**: The product MUST have capacity to transmit 800 updates per second without failure.

4.2.2 Non-Functional Requirements

N01: The product MUST integrate with the existing ICS without altering the current design.
Maintaining current system functionality ensures the new product does not disrupt operations or require costly redesign. This is critical in NPPs where operational stability is essential.

- **N01-1**: The product MUST be interoperable with ICS connected devices.
- **N01-2**: The deployment of the product MUST not require reconfiguration or modification of existing system's hardware or software.

N02: The product SHOULD be supported in operations for 60 years.
NPPs require long-term operational support to avoid frequent replacements or interruptions. NPPs are intended for 60 years of operation without modification of the design, with planned outages for maintenance purposes occurring every 18 months.

- **N02-1**: The product SHOULD not require regular maintenance outside of a planned 18-month NPP operational period.
- **N02-2**: The product SHOULD not require replacement within 60 years.

N03: The product SHOULD withstand environmental conditions within the NPP.
Harsh environmental conditions necessitate durable designs to prevent equipment failure.

- **N03-1**: The product MUST comply with a temperature tolerance of +4ºC to +55ºC at all times.
- **N03-2**: The product MUST comply with a humidity tolerance of 40% to 60% at all times.

4.2.3 Safety Requirements

S01: The product MUST deal with faults safely.
Fail-safe operation prevents faults from escalating into hazardous conditions, ensuring the safety of systems and personnel. Faults are interruptions to normal operation, such as communication failures or power disruptions.

- **S01-1**: The product MUST include fault detection mechanisms.
- **S01-2**: The product SHOULD correct the fault if possible.
- **S01-3**: The product MUST enter a safe operational state when the fault cannot be corrected.
- **S01-4**: The product MUST resume normal operation when a fault has been resolved.

4.2.4 Cyber Security Requirements

C01: The product SHOULD support good industrial cyber practices.
Good industrial cyber principles such as secure-by-design, zero trust and defence-in-depth support the overall security of the system and compliance with standards and regulations.

- **C01-1**: The product SHOULD demonstrate that it adheres to secure-by-design principles.
- **C01-2**: The product SHOULD be able to support defence in depth principles.
- **C01-3**: The product SHOULD support zero-trust principles.

C02: The product MUST ensure communication confidentiality at all times.
Confidentiality protects sensitive operational data from unauthorised access.

- **C02-1**: The product MUST ensure communication confidentiality at all times.

C03: The product MUST preserve the integrity of communicated data.
Data integrity is critical to prevent manipulation, which could lead to incorrect system actions.

- **C03-1**: The product MUST preserve the integrity of communicated data.

C04: The product MUST ensure data is only transmitted to and from authorised entities.
Authentication enforces zero-trust and need to know principles when configured correctly.

- **C04-1**: The product MUST verify authenticity on the sending end.
- **C04-2**: The product MUST verify authenticity at the receiving end.
- **C04-3**: The product MUST block communication attempts if authentication checks fail.

C05: The product MUST detect and alert on any unauthorised physical or logical tampering.
Early detection minimises potential harm and triggers timely responses to breaches.

- **C05-1**: The product MUST monitor for physical tampering with components.
- **C05-2**: The product MUST detect unauthorised logical changes.
- **C05-3**: The product MUST send a single alert to operators when tampering is detected.

4.3 Evaluation Process

Through research, three COTS products have been selected to secure communications between the two identified safety-critical ICS. To find the best option, a simplified Weighted Sum Model (WSM), a Multi-Criteria Decision-Making (MCDM) method (Department for Communities and Local Government, 2009), will be used for evaluation. WSM assigns weights to criteria based on importance, enabling product scoring. This method reflects the key factors relevant to the nuclear industry, as detailed in Table 2.

Category	% Weighting	Number of Requirements	Requirement Weighting
Safety	0.4	4	0.1000
Security	0.25	11	0.0227
Functional	0.25	5	0.0500
Non-Functional	0.1	6	0.0167

Table 2 Requirements Category Weightings

Each product is rated on its ability to meet specific requirements within the categories, receiving a quantitative score from the qualitative statements in Appendix A. Scores range between 0 (low) to 5 (high). The score of each requirement is then weighted, and the category scores are summed to assess the overall performance of each product based on an initial document review.

The final score for each product is calculated as:

Score = (**S***0.1000) + (**C***0.0227) (**F***0.0500) + (**N***0.0167)

Where:

S = Sum of safety requirement scores

C = Sum of cyber security requirement scores

F = Sum of functional requirement scores

N = Sum of non-functional requirement scores

The product with the highest score is potentially the most suitable for securing communications in safety-critical ICS.

4.4 Product Validation

An evaluation has been conducted on the identified COTS security products.

- **Data Diode:** Siemens CoreShield Data Capture Unit (Siemens, 2017)
- **Industrial Firewall:** Cisco Secure Firewall ISA3000 (Cisco, 2021)
- **Hardware Encryption:** Blueskytec ICSProtect (Blueskytec, 2024)

This evaluation validates the V-lifecycle by confirming product compliance with requirements, using available data sheets and technical documentation. The total WSM scores are presented in Table 3, rounded to two decimal places as needed. The full analysis can also be reviewed in Appendix A.

	Data Diode Siemens CoreShield	**Industrial Firewall** Cisco ISA3000	**Hardware Encryption** Blueskytec ICSProtect
Functional	1.00	1.05	1.15
Non-Functional	0.42	0.32	0.45
Safety	0.80	1.80	1.90
Cyber Security	0.39	0.68	1.07
Total Score	**2.60**	**3.85**	**4.57**

Table 3 WSM Requirements Validation

The BST ICSProtect stands out as a flexible solution for industrial integrations, offering bidirectional communication and superior data integrity preservation compared to traditional firewalls and unidirectional data diodes. However, it is the least proven option for nuclear ICS environments, lacking real-world implementation, which raises concerns about its suitability for CNI. Empirical testing is required to evaluate the performance and security for safety-critical ICS applications of the ICSProtect.

5 Design

This design section covers the architecture and security features of the selected ICSProtect as well as a network design that will be used for implementation and testing in a simulated lab environment.

5.1 Product Architecture

The BST ICSProtect, Figure 2, is a hardware encryption device designed to protect ICS from cyber threats. It is physically connected to each endpoint, shown in Figure 3, acting as an intermediary for all network communication. By encrypting network traffic before it leaves a device and decrypting it upon arrival, the ICSProtect ensures that data remains secure throughout transmission.

Figure 2 BST ICSProtect (Blueskytec, 2024)

Figure 3 System Configuration

Encryption is rarely used in safety-critical ICS systems due to the complex software it involves, which can introduce latency and disrupt real-time operations vital for safety. In 2023, software vulnerabilities were exploited in 38% of intrusions (Mandiant, 2024). The ICSProtect module avoids these risks, as it operates without software.

5.1.1 Hardware

The ICSProtect device uses Field-Programmable Gate Arrays (FPGAs) instead of traditional processors, enabling hardware-based security functions that outperform software solutions. FPGAs offer faster execution times, making the device highly efficient for industrial environments where low latency is essential (Monmasson et al., 2020). It also features physical anti-tamper mechanisms that trigger alarms upon unauthorised access, such as attempts to disconnect or open the device. Classified as a Physically Unclonable Function (PUF), its unique internal structure self-destructs if tampered with, preventing attackers from extracting keys or altering functionality (Mobley, 2024).

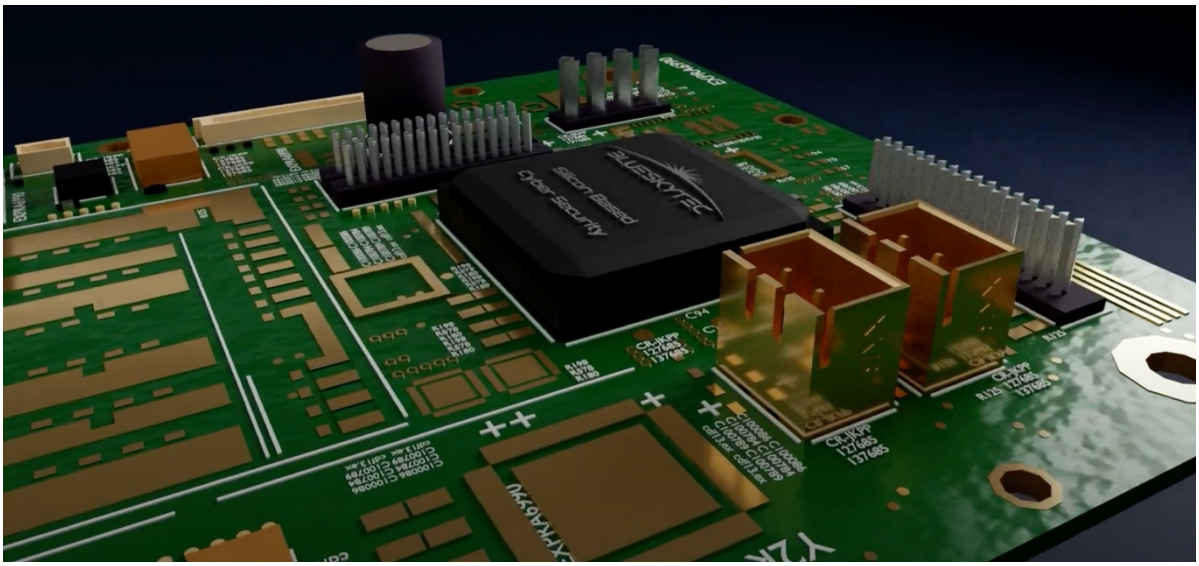

Figure 4 FPGA Hardware Graphic Mock-up (Blueskytec, 2024)

5.1.2 Functionality

The ICSProtect device processes packets through three main stages, shown in Figure 5, at both sending and receiving ends, utilising any protocol over a Transmission-Control-Protocol (TCP) communication line. It wraps data packets, like IEC-104, with encryption, with routing headers added in plaintext for network transfer.

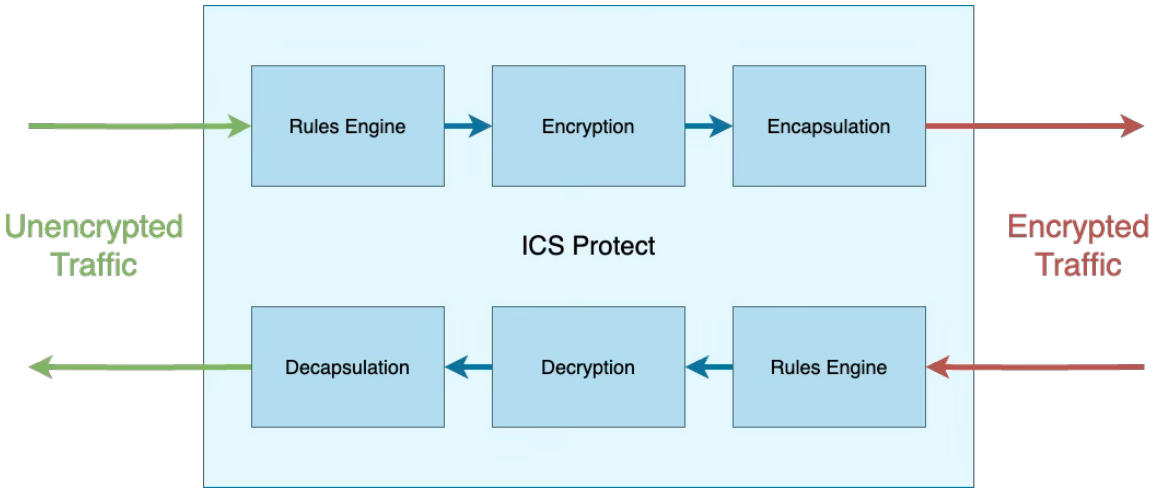

Figure 5 ICSProtect Processing Stages

5.1.3 Rules Engine

The rules engine filters network packets based on predefined security rules – such as protocol type, IP addresses, port numbers, and MAC addresses – acting as a firewall to ensure only authorised traffic is processed. Non-compliant packets are dropped before encryption.

5.1.4 Encryption and Decryption Process

Each ICSProtect device contains a pre-placed OTP block embedded during manufacturing. This block is derived from a high-entropy source. In cryptographic terms, entropy measures randomness; higher entropy equates to greater resistance against prediction or brute-force attacks. The OTP block enables the generation of over 2^{64} unique keys, using a mapping process. To protect the OTP block, it is encrypted using a Key Encryption Key (KEK), adding an layer of security for storage and handling.

An OTP is unbreakable when used correctly, as each key is used once and destroyed, limiting the impact of a compromised key to a single message (Easttom, 2022). However, OTPs typically pose key management challenges, as keys must be securely generated, stored, distributed, and exclusively used to maintain security. The ICSProtect does not suffer these issues, due to the OTP being embedded in hardware during manufacturing, eliminating key exchange. Devices are produced in pairs or multiples, each with the same OTP.

On the sending end, when a message is to be encrypted, bits from the OTP block are selected using an index (N) and an algorithm is used to derive a one-time key using these bits. This key is used to encrypt the data using a BST hardware implementation of the Twofish algorithm, a symmetric, Feistel-based cipher known for security and efficiency. Twofish splits the plaintext into halves and performs multiple rounds of transformation using key-dependent substitutions and a complex schedule (Easttom, 2022). Customisation of the Twofish can also be implemented if an organisation requires a non-standard, sovereign algorithm.

Before transmission, a Known Answer Test (KAT) is performed to provide a root-of-trust. The KAT serves as a cryptographic process to verify data integrity and authenticity of the message. The KAT uses a Cipher-based Message Authentication Code (CMAC). This works by encrypting the message using a Cipher Block Chain (CBC) and only keeping the last block of ciphertext as the guarantee of authenticity. The initialisation for this process is started with the KAT. This guarantees that any changes in the bit pattern or the KAT block will be detected, due to the chain process.

Once this is calculated, it is then pre-pended as the start of the message for the encryption process. The encryption process also uses the Cipher Block Chain (CBC) mode with a unique Initialisation Vector (IV) that incorporates the Station ID of the device and a random starting value that is derived from the OTP at index N. The CMAC followed by CBC-encryption ensures that every packet is cryptographically unique and indistinguishable from any other message.

On the receiving end, the corresponding key derived with index N of the OTP is used to decrypt the message. The ICSProtect devices then recomputes the KAT. If the KAT value does not match, it is assumed that the message has been altered and the packet is discarded (Mobley, 2025). Additionally, IEC-104 traffic is often transferred in binary; therefore, it would be difficult to tell if a message has been decrypted correctly without the use of a KAT.

5.1.5 Encapsulation and Decapsulation

ICSProtect devices use a TCP connection, therefore encapsulation is necessary to route and transfer packets in User-Datagram-Protocol (UDP) format, regardless of the original protocol. At the sending end, the device encases the encrypted data with header information before transmission. At the receiving end, it removes these elements to reconstruct the original message.

The final encapsulated network packet is shown in Figure 6.

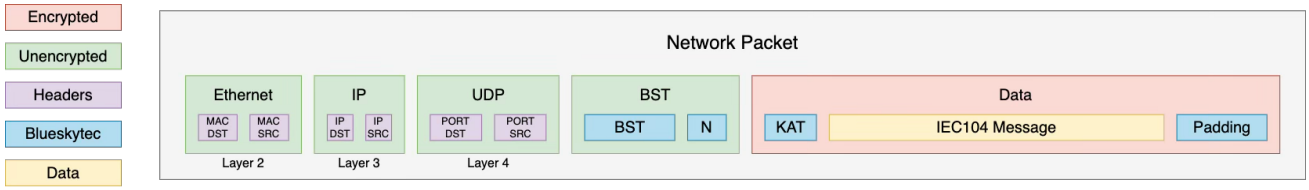

Figure 6 BST Network Packet Structure

When a packet is encrypted, the ICSProtect device adds a BST header and footer, with the header containing key components such as packet routing information and key index (N). Including N in the packet header ensures synchronisation between communicating devices. When a message is sent or received, the index increments. If a message arrives with an index of N-1 (outdated), the device discards it. If a message arrives with N+1 (indicating potential packet loss), the device assumes loss and adjusts the index. This method guarantees reliability even in networks with redundant lines. Among multiple packets, the device processes the first one that decrypts correctly and discards the rest, avoiding duplicate messages. (Mobley, 2024)

5.2 ICS Network Communications Design

In an ideal scenario, the network shown in Figure 7 represents a good, accurate setup of a communication network between two independent ICS, with inputs, outputs, a PLC, HMIs for each system, connected with a BST network. Please note that this diagram is purely exemplary, the systems are not real.

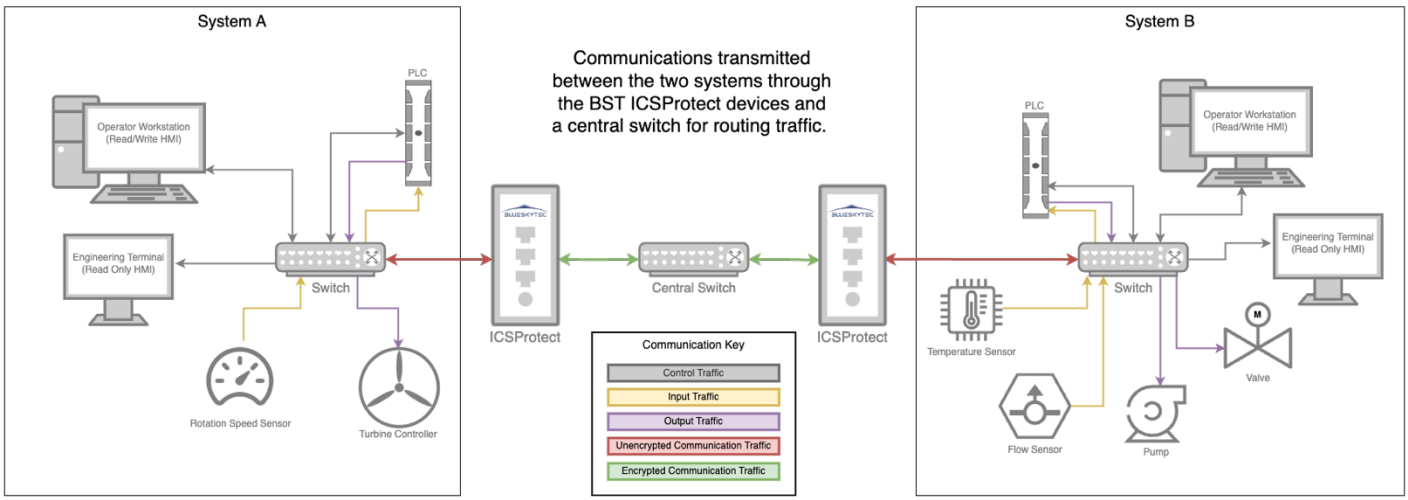

Figure 7 Representative example of ideal ICS network setup

However, this setup is not achievable with the available resources, equipment and time. Therefore, multiple network configurations will be designed to allow various tests to be performed.

5.2.1 Network Requirements

Testing of the ICSProtect should be conducted using network equipment that accurately replicates an ICS environment to ensure realistic assessments of its functionality and security effectiveness.

A list of required hardware, software and quantities can be found in Table 4.

Hardware	
BST ICSProtect Devices	2
Allen Bradley HMI	1
Allen Bradley PLCs	5
Light Emitting Diodes (LEDs)	5
Network Switch	3
Windows Desktop	2
Windows Monitor	3
Arduino	1
Oscilloscope	1
Ethernet Cables	12
Power Source	1
Power Cables	18
Software	
Vinci	
Packet Sender	
Wireshark	

Table 4 Required Networking Equipment

5.2.2 IEC104 Setup

Unfortunately, the PLCs available for this project do not have native IEC-104 functionality. Replicating IEC-104 protocol traffic involves complex timing, stateful communication, and hardware-specific behaviours that are not easily replicated on general-purpose devices like laptops or microcontrollers. Without dedicated equipment, emulating the full functionality of the protocol can be difficult.

Vinci (Elseta, 2025), a simulation tool for industrial protocols, overcomes general-purpose hardware limitations by enabling IEC104 traffic generation in connected devices. With Vinci, an Arduino can function as the IEC-104 master while a laptop serves as the slave, facilitating basic communication flow simulations. The Arduino runs a simple script. For traffic monitoring, Wireshark can be used with port mirroring on a switch, allowing for packet capture and analysis of encrypted IEC-104 communications between the master and slave devices, as illustrated in Figure 8.

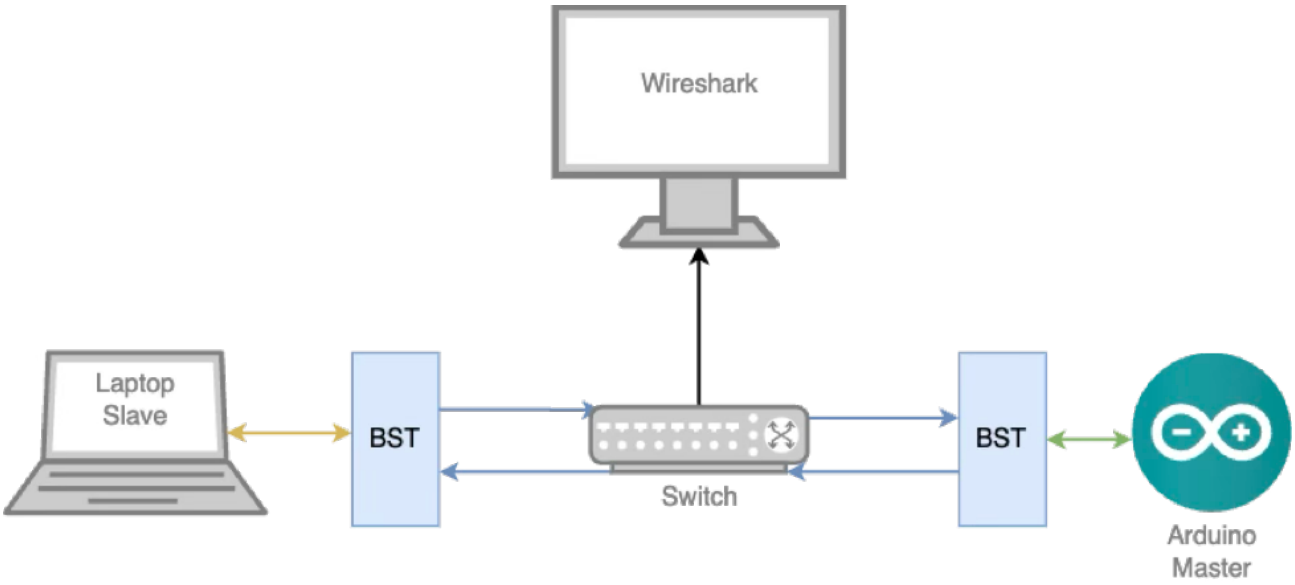

Figure 8 IEC104 Network Design

5.2.3 ICS Setup

To evaluate the system's functionality, a network environment can be established using BST ICSProtect devices, switches, Allen Bradley PLCs, an HMI, a Windows desktop, and a monitor, as illustrated in Figure 9. Unfortunately, this equipment does not have native IEC-104 communication but can still be used for functional tests.

This design aims to replicate ICS environments as accurately as possible with the available equipment. System A includes PLCs, LEDs and a HMI. The HMI interacts with the PLCs, offering real-time updates similar to a live industrial setting, reflecting many ICS configurations where the HMI is located separately from the PLCs for centralised operations. This network will facilitate functional and safety tests, including communication transmissions and interruptions. The HMI enables real-time monitoring of the PLC states when network and power cables are disconnected from the ICSProtect.

The Windows desktop serves as System B, facilitating traffic exchange with the PLCs. Packet Sender, a free and open-source network testing utility, will be deployed on the Windows desktop to generate network traffic of varying packet sizes, with the PLCs able to respond accordingly. This tool supports TCP, UDP, and SSL connections and is widely utilised in cybersecurity testing due to its ability to simulate network communication. Given that ICSProtect devices rely on UDP packets, this configuration provides a realistic assessment of network behaviour.

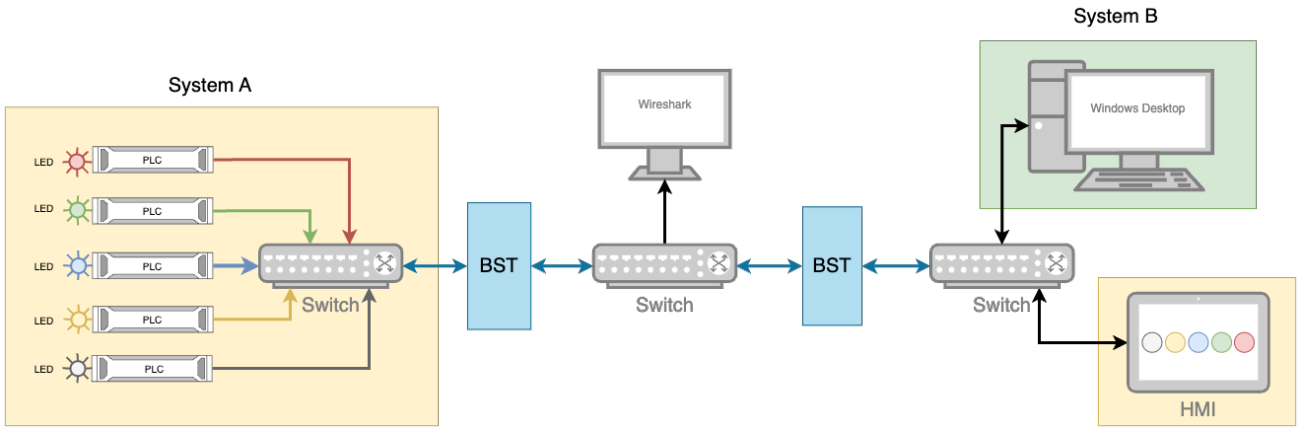

Figure 9 ICS Network Design

For network traffic analysis, Wireshark will utilise port mirroring on a switch for packet capture. However, it cannot accurately measure microsecond-scale latency due to software limitations. Therefore, an oscilloscope is necessary for precise timing measurements, offering high-resolution, real-time waveform analysis to detect small timing variations. This is crucial for verifying compliance with the 100µs latency specified in the product's datasheet (Blueskytec, 2024). The final setup, including the oscilloscope for accurate latency measurement, is shown in Figure 10.

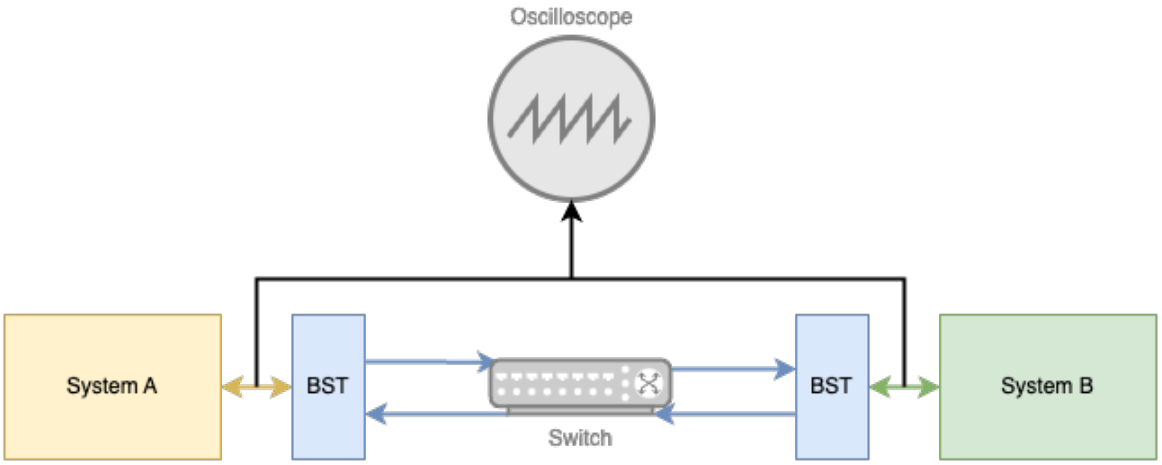

Figure 10 ICS Network with Oscilloscope

5.2.4 Cyber Attacker Setup

Figure 11 represents a very similar ICS environment, simulating a network where two systems communicate through ICSProtect devices connected via a switch. Wireshark is again able to analyse traffic. The malicious actor represents a cyber threat that has gained access to the network and is attempting to perform reconnaissance to devise an attack. Packet Sender will be used on the malicious actor's device to generate and transmit crafted packets, allowing the attacker to simulate various threats. This includes data exfiltration by attempting to extract sensitive ICS information such as system commands. The attacker can also perform traffic spoofing, generating false packets or modifying legitimate communication to inject malicious commands or cause operational disruptions. Additionally, this setup allows for man-in-the-middle (MitM) attacks, where the malicious actor manipulates data in transit between the systems, potentially altering critical commands or corrupting data. This configuration enables security testing by replicating realistic attack scenarios.

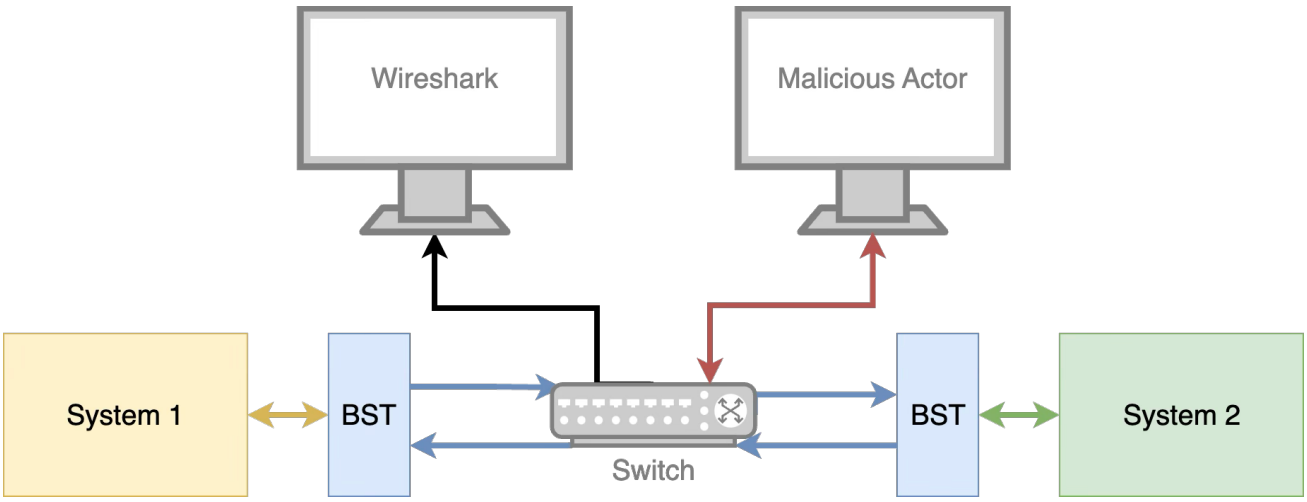

Figure 11 Cyber Attack Network Design

6 Implementation

6.1 Lab Setup

The test lab has been configured according to the network design, using the specified equipment.

Figure 12 depicts System A, aligned with the network design shown in Figure 9. In this setup, PLCs are connected to LEDs, controlling whether they are on or off. All PLCs are networked through a switch, which routes their data to the BST ICSProtect device.

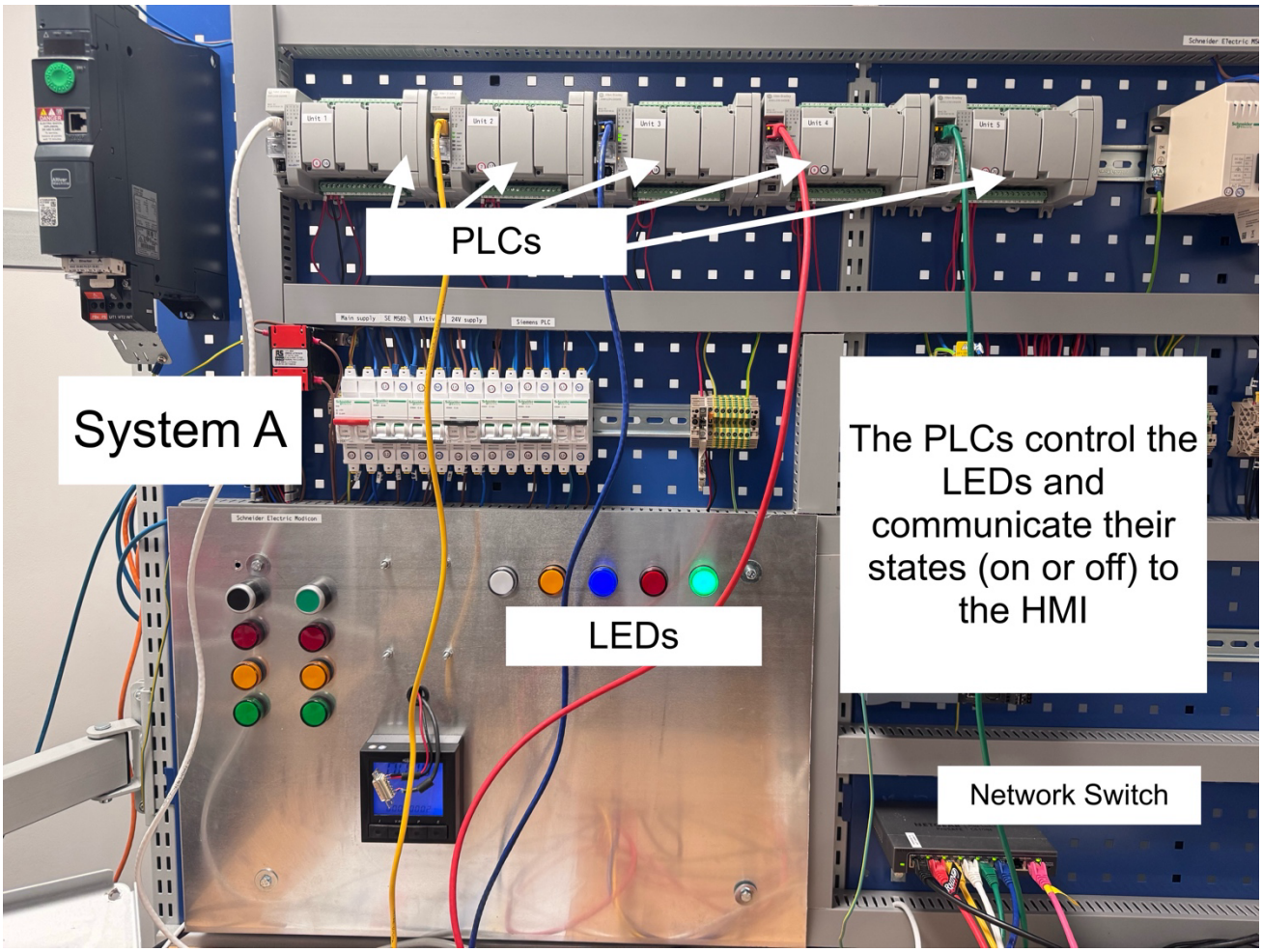

Figure 12 System A components connected to a switch

Figure 13 illustrates the ICSProtect devices and the network switch of System B, which is connected to the HMI. One ICSProtect unit interfaces with the switch in System A, enabling communication with the PLCs. The second ICSProtect device connects to the switch in System B, which includes a Windows desktop. There is a central switch to bridge communication between the two systems via the ICSProtect devices. This aligns with the design in Figure 9.

Additionally, the central switch is connected to a laptop running Wireshark via a mirrored port, enabling packet capture and traffic analysis.

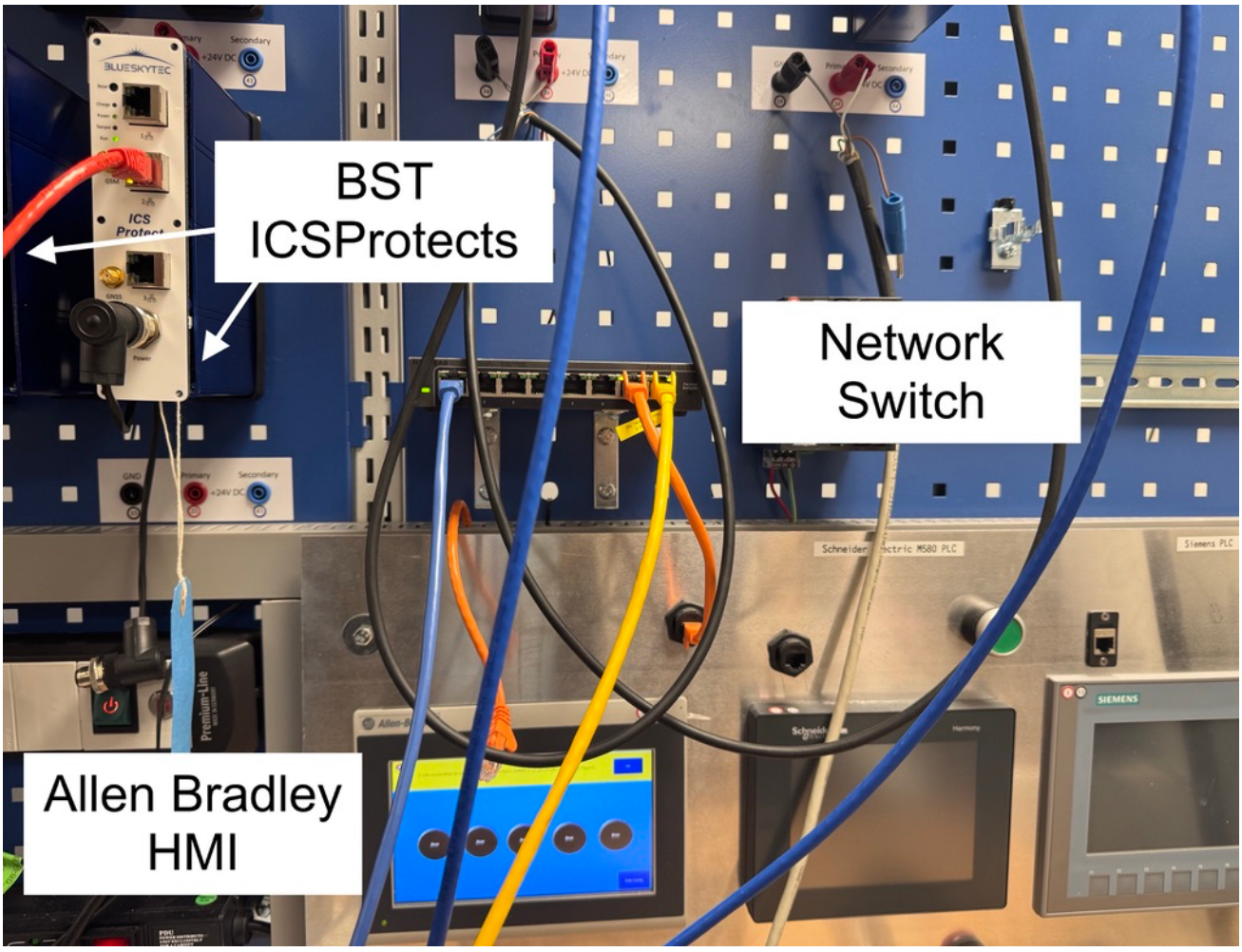

Figure 13 ICSProtect Devices and System B components

Figure 14 presents System B, the Windows desktop setup. Figure 15 shows the Wireshark monitoring laptop.

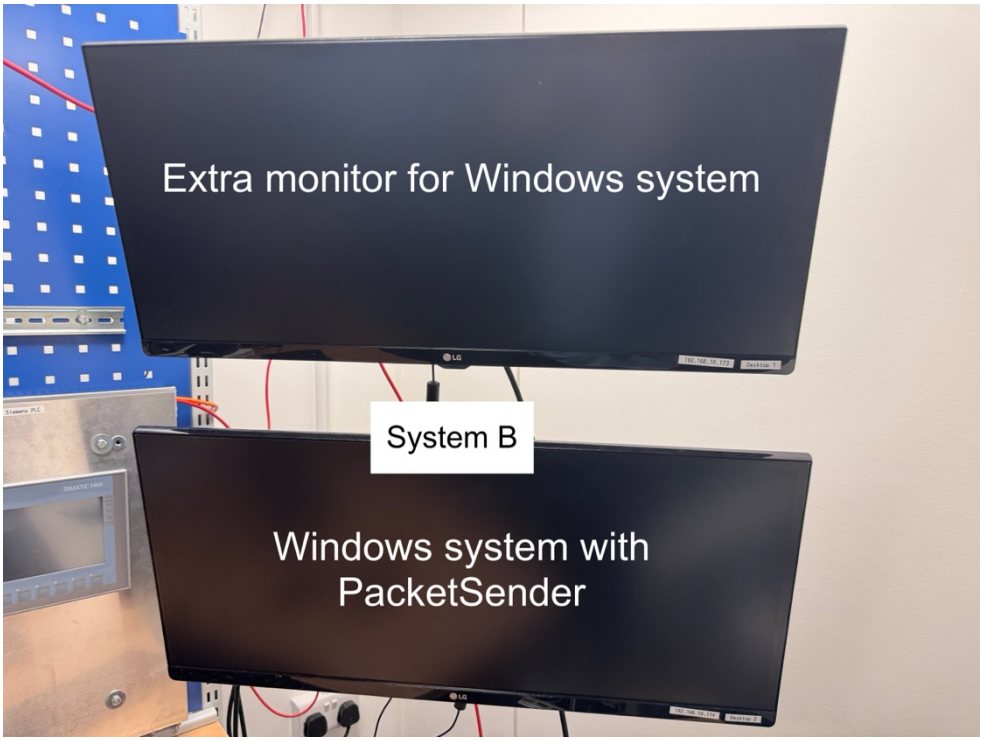

Figure 14 System 2, Windows desktop

Figure 15 Wireshark laptop

For testing IEC-104 protocol traffic, an Arduino and a laptop running Vinci software are used, as in Figure 8. The Arduino functions as the master device, issuing commands to which the laptop responds. The Arduino unit utilised in this setup is shown in Figure 16.

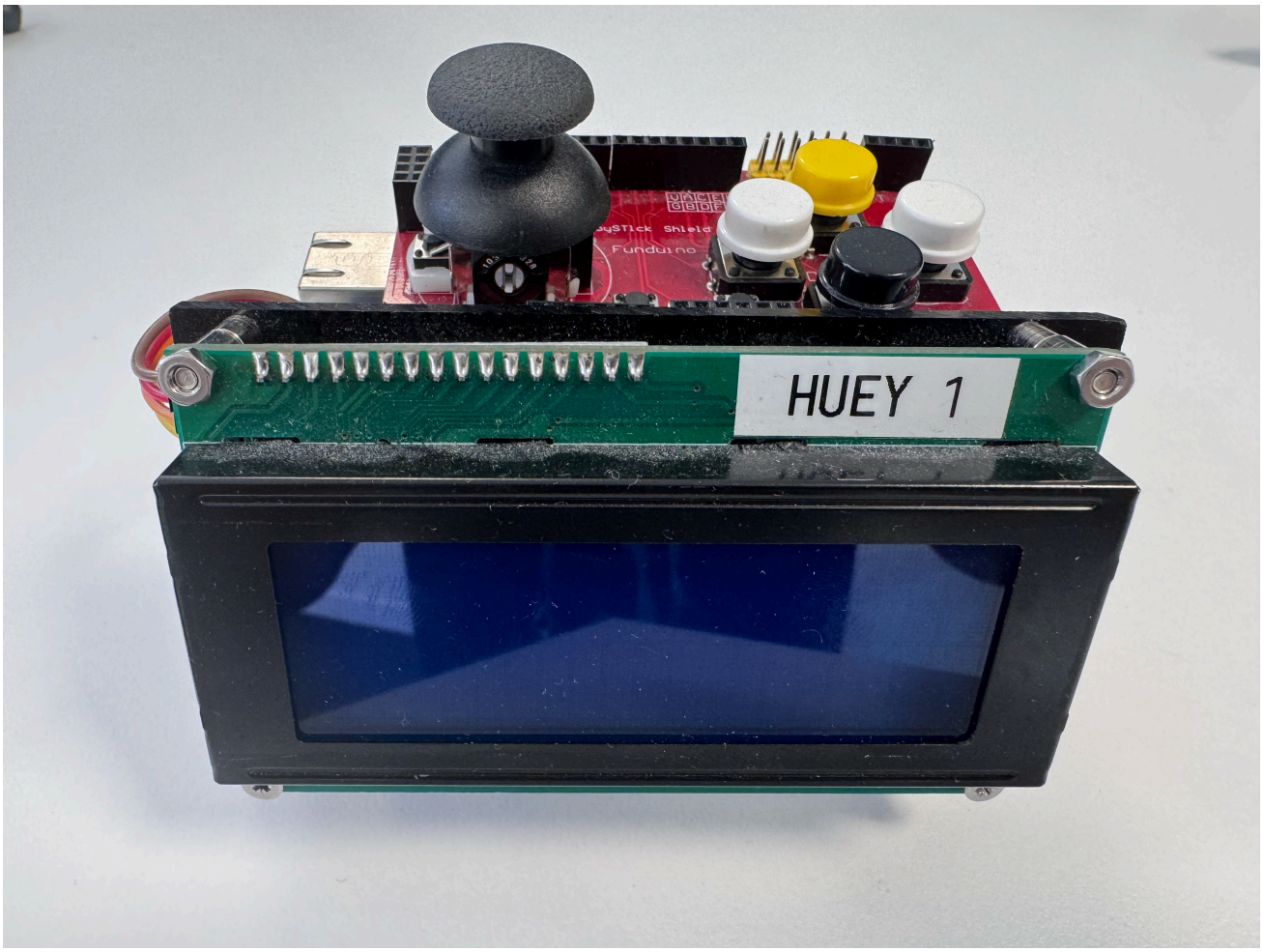

Figure 16 Arduino master unit

7 Testing

A series of tests have been conducted to verify the product's performance against the specified requirements. Each section includes a concise test plan summarising the tests carried out. The network configuration used matches the network designs outlined in Section 5. Each test plan outlines a Test ID for traceability (Test ID), the mapped requirement ID (Req ID), a summary test aim (Test Aim), the network used (Network), and the Pass/Fail status (State).

Certain requirements cannot be empirically tested Therefore, the status "Assumed Pass" is used to indicate that the requirement is considered satisfied based on judgement of the available documentation.

Extensive test plans are provided in Appendix B, offering additional detail, including the full test methods, expected outcomes, and actual results.

7.1 Functional Testing

This section outlines the tests conducted to verify that the system meets its defined functional requirements. Each test was designed to assess a specific aspect of system performance, including protocol validation, latency, and throughput. The results are documented in Table 5.

Test ID	Req ID	Test Aim	Network	State
BST-FT1	F01-1 F02-1 F02-2	Validate IEC104 protocol usage and bidirectional communication.	Figure 8	Pass
BST-FT2	F03-1	Measure data transmission latency	Figure 10	Pass
BST-FT3	F04-1	Measure data transmission throughput	Figure 9	Pass

Table 5 Functional Test Plan

7.1.1 BST-FT1

Figure 17 displays the traffic captured using Wireshark on the laptop slave in the network diagram Figure 9. The traffic consists of IEC-104 protocol bidirectional communication between the Arduino master (192.168.10.240) and the laptop slave (192.168.10.178).

TESTFR act: Send a test frame to check connection

TESTFR con: Confirmation response to a test frame activation

61	54.099824	192.168.10.178	192.168.10.240	IEC 60870-5-104	60 <- U (TESTFR act)
62	54.100345	192.168.10.240	192.168.10.178	IEC 60870-5-104	60 -> U (TESTFR con)

Figure 17 IEC104 Traffic Capture

When Wireshark is used on a switch with port mirroring enabled, Figure 18 shows the traffic being transmitted as UDP packets. This occurs because the product encapsulates the encrypted data, enabling it to be transferred over the TCP connection between the ICSProtect devices.

54	42.830780	192.168.10.240	192.168.10.178	UDP	132 2404 → 49168 Len=90
55	42.830780	192.168.10.178	192.168.10.240	UDP	132 49168 → 2404 Len=90
56	43.600318	192.168.10.178	192.168.10.240	UDP	132 49168 → 2404 Len=90
58	44.604777	192.168.10.178	192.168.10.240	UDP	132 49168 → 2404 Len=90
59	44.606133	192.168.10.240	192.168.10.178	UDP	132 2404 → 49168 Len=90
60	44.606133	192.168.10.178	192.168.10.240	UDP	132 49168 → 2404 Len=90

Figure 18 UDP Traffic Capture

Figure 18 shows alternating IP addresses, communicating bidirectionally, therefore BST-FT1 is validated.

7.1.2 BST-FT2

As in Figure 10, the oscilloscope has been connected either side of the two ICSProtect devices, to measure latency of the whole transmission. The oscilloscope capture in Figure 19 shows a latency of 89.6 µs between the transmission and reception of a 600-byte packet.

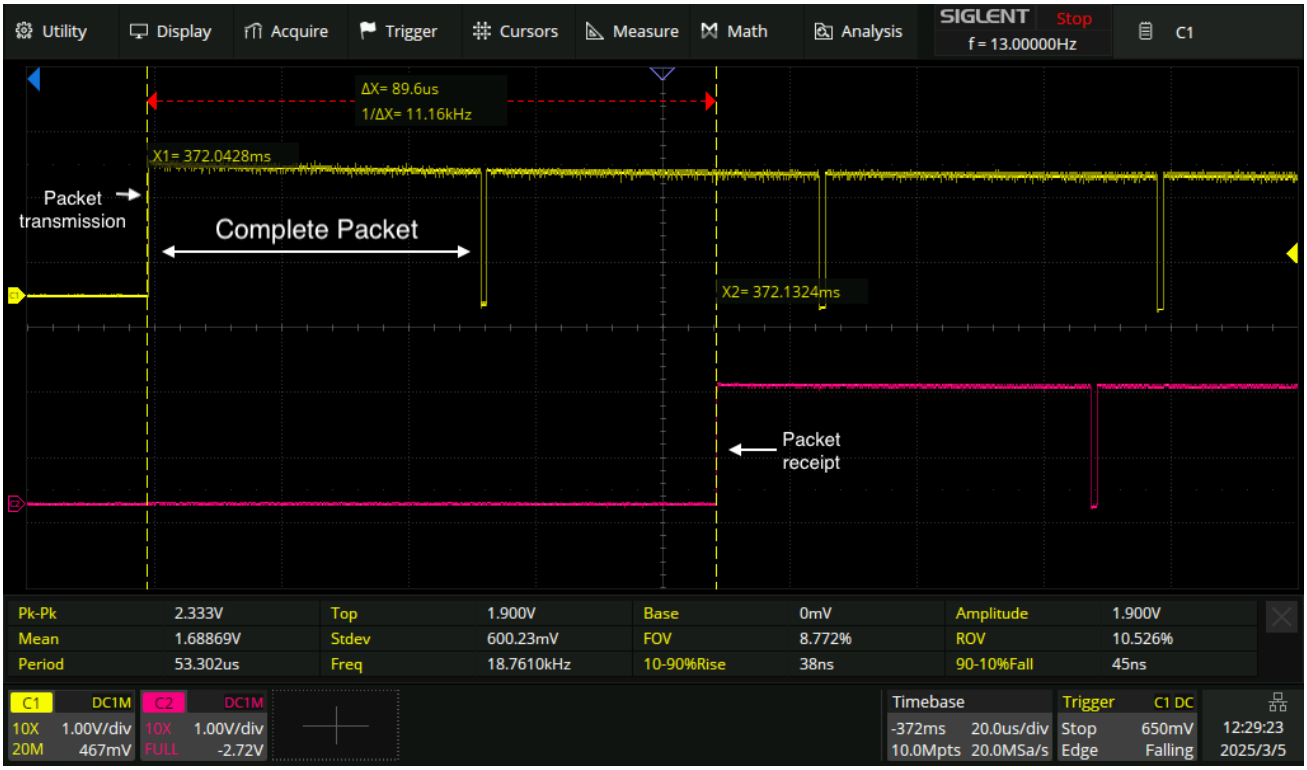

Figure 19 Oscilloscope Capture

A standard packet size is 600 bytes; however, as packet sizes can vary significantly, latency is likely to increase with larger packet sizes. Further tests were conducted to verify latency across different packet sizes, as shown in Figure 20, which lists the standard tests that have been created to transmit packets of certain lengths. The graph in Figure 21 displays the result of each packet size test. As depicted in the bars, the packet transmission period is the primary contributor to latency, not the encryption process.

	Send	Name	Resend	To Address	To Port	Method	
1	Send	0060 byte message UDP	0	192.168.10.174	505	UDP	60messagelength60m
2	Send	0100 byte message UDP	0	192.168.10.174	505	UDP	100messagelength100messagelength100messagelength100message
3	Send	0150 byte message UDP	0	192.168.10.174	505	UDP	150messagelength150messagelength150messagelength150messagelength150messagelen
4	Send	0250 byte message UDP	0	192.168.10.174	505	UDP	250messagelength250messagelength250messagelength250messagelength250messagelen
5	Send	0400 byte message UDP	0	192.168.10.174	505	UDP	400messagelength400messagelength400messagelength400messagelength400messagelen
6	Send	0550 byte message UDP	0	192.168.10.174	505	UDP	550messagelength550messagelength550messagelength550messagelength550messagelen
7	Send	0700 byte message UDP	0	192.168.10.174	505	UDP	700messagelength700messagelength700messagelength700messagelength700messagelen
8	Send	0850 byte message UDP	0	192.168.10.174	505	UDP	850messagelength850messagelength850messagelength850messagelength850messagelen
9	Send	1000 byte message UDP	0	192.168.10.174	505	UDP	1000messagelength1000messagelength1000messagelength1000messagelength1000messa
10	Send	1150 byte message UDP	0	192.168.10.174	505	UDP	1150messagelength1150messagelength1150messagelength1150messagelength1150messa
11	Send	1300 byte message UDP	0	192.168.10.174	505	UDP	1300messagelength1300messagelength1300messagelength1300messagelength1300messa

Figure 20 Packet Size Transmission Tests

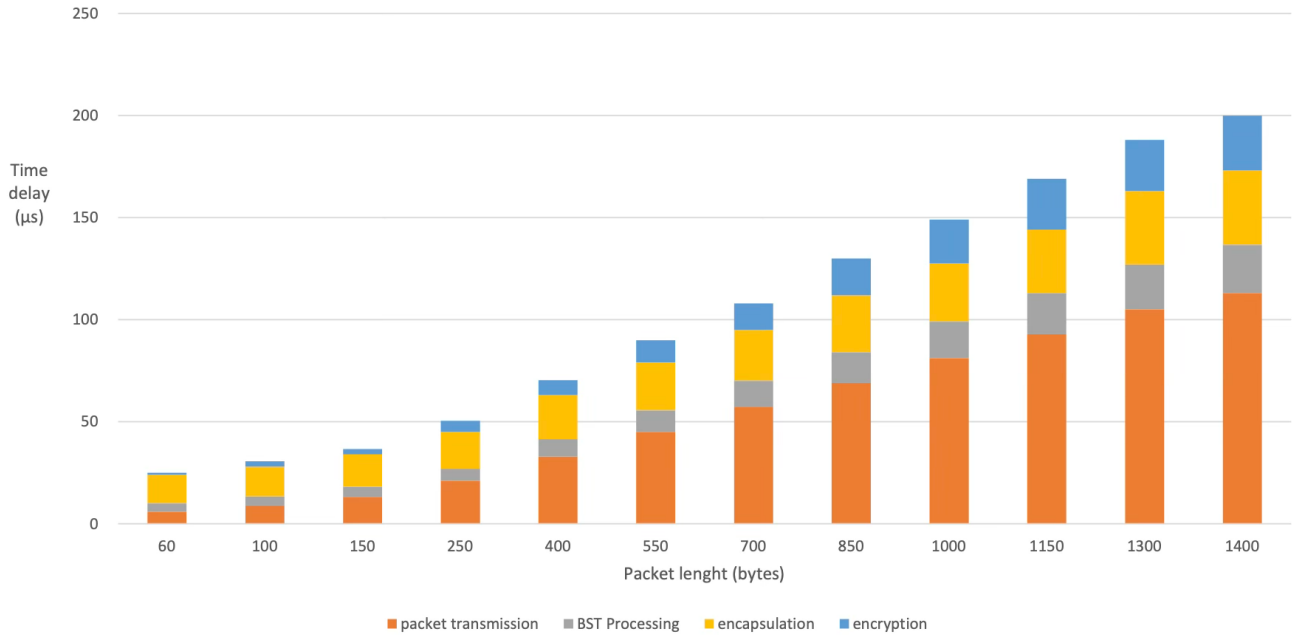

Figure 21 Bar Graph of Packet Size vs Time Delay in Transmission

F03-1 has been met sufficiently, because even at a packet size of 1400 bytes, the measured latency is 200µs, which is well within the specified latency requirement of ≤250 µs. Additionally, in the IEC-104 protocol, the maximum packet size is determined by the APDU (Application Protocol Data Unit) length, which consists of the fixed 6-byte APCI (Application Protocol Control Information) and the ASDU (Application Service Data Unit), typically limited to 253 bytes. This results in a maximum packet size of 259 bytes. With this packet size, the estimated latency is 50µs, which is 1/5th of the allocated latency specified in the requirement.

7.1.3 BST-FT3

At the maximum capability of PacketSender, the ICSProtect devices successfully transmitted traffic with no loss of traffic. Throughput measurements from the activity monitors on the sending and receiving systems showed values between 93MB/s and 96MB/s over one minute. This far exceeds the 1.12MB/s required for 800 updates/second, even with the maximum packet size of 1400 bytes.

- 1400bytes * 800updates/s = 1120000bytes/s = 1.12MB/s

Latency measurements also support the system's throughput capability. The time delay for sending and receiving the maximum packet size was 200µs (Figure 19), which is well within the update time required to achieve 800 updates/s:

- Time per update: 1/800 = 1250µs
- Latency: 200µs < 1250µs
- Since 200µs is significantly less than 1250µs, the system can easily handle 800 updates per second.

As in the previous test, the maximum packet size expected for IEC-104 is 259 bytes. The estimated latency is 50µs for a 259-byte packet. These values allow the system to support up to 20,000 updates per second:

- 1s / 50µs = 20,000 updates/s.

7.2 Non-Functional

This section outlines the non-functional testing undertaken to verify that ICSProtect meets non-technical operational requirements. These tests evaluate the system's interoperability with connected devices, its long-term maintainability and durability, and its environmental resilience.

Test ID	Req ID	Test Aim	State
BST-NT1	N01-1 N01-2	Verify interoperability with all connected devices, ensuring no reconfiguration is required for deployment.	Assumed Pass
BST-NT2	N02-1 N02-2	Verify maintenance and lifetime expectations.	Pass
BST-NT3	N03-1 N03-2	Verify environmental suitability.	Assumed Pass

Table 6 Non-Functional Test Plan

7.2.1 BST-NT1

Interoperability for N01-1 and N01-2 cannot be thoroughly tested due to limited equipment diversity. However, functional tests demonstrate that ICSProtect devices can seamlessly interoperate with laptops, desktops, Arduinos, PLCs, and HMIs without requiring reconfiguration or modification.

7.2.2 BST-NT2

In the BST ICSProtect, keys are derived from a OTP key block containing bits for 2^{64} unique keys. At the specified usage rate of 800 keys per second (one key per message), this key block is sufficient to last for ~730.67 million years, verifying the operational requirements for N02-1.

To maintain security, ICSProtect allows the entropy block to be rotated or remixed with salt if compromised, generating a fresh OTP keyspace. This process can be repeated $2^{(32-1)}$ times, resulting in an overall possible entropy of $2^{(64+31)}$. Consequently, this generates a total of 2^{95} unique keys, extending the operational lifespan of the system to ~1.57 quintillion years.

Calculation results can be seen in Table 7, rounded to two decimal places. The complete calculations are included in Appendix C.

OTP keys	18446744073709600000
Keys used per second	800
Keys used per year	25246080000
Years of use	~730.67 million years
Years of use with remixing	~1.57 quintillion years

Table 7 Key Usage Calculation Results

Additionally, the need for a low-maintenance product is satisfied as ICSProtect devices have no software, eliminating updates or patches, achieving N02-2 as the product does not need regular maintenance.

7.2.3 BST-NT3

Due to lack of equipment, environmental conditions such as temperature and humidity have not been tested. However, the ICSProtect's data sheet (Blueskytec, 2024) has the values in Figure 22, which comply with the required temperature and humidity ranges of N03-1 and N03-2, as in Table 8.

Operational Ranges	**Requirement**	**Datasheet Value**
Temperature Range	+4ºC to + 55ºC	-40ºC to +100ºC
Humidity Range	40% to 60%	0% to 70%

Table 8 Environmental Conditions

It should be noted that devices with a battery have a smaller temperature range of -20ºC to +60ºC, which is still within the specified requirements.

Temperature (operational)	-20 °C to +60 °C (with to Li-ion battery) -40 °C to +100 °C without Li-ion battery
Temperature (storage)	-20 °C to +60 °C (with to Li-ion battery) -40 °C to +100 °C without Li-ion battery
Humidity	0 – 70% humidity

Figure 22 Environmental Values (Blueskytec, 2024)

7.3 Safety

This section addresses the safety aspects of ICSProtect by evaluating its resilience to power and network faults, ensuring that the system behaves predictably and recovers promptly without compromising operational integrity. The conducted tests simulate power and network failures.

Test ID	Req ID	Test Aim	Network	State
BST-ST1	S01-1 S01-2 S01-3 S01-4	Introduce power faults. Observe network behaviour to ensure system recovers quickly and effectively.	Figure 9	Pass
BST-ST2	S01-1 S01-2 S01-3 S01-4	Introduce network faults. Observe network behaviour to ensure system recovers quickly and effectively.	Figure 9	Pass

Table 9 Safety Test Plan

7.3.1 BST-ST1

Once the power cable has been disconnected, the device stops operating. However, there is a device available that does include a battery, which would mitigate this failure. Additionally, NPPs typically have extensive power backups that automatically activate in the event of failure.

When the power cable is reconnected, the device continues operations within ~2 seconds, with the indication of amber lights whilst powering on, and green lights when operating.

7.3.2 BST-ST2

Once the network cable has been disconnected, the HMI displays an error to demonstrate that communications with the PLCs have been interrupted, as in Figure 23.

When the network cable is reconnected, the device continues operations within ~1.5 seconds, with the HMI once again displaying the PLC’s communicated states, as in Figure 24.

Additionally, devices can be connected in parallel redundantly, meaning that in the event of one network line failing, the redundant one could be used to continue operations.

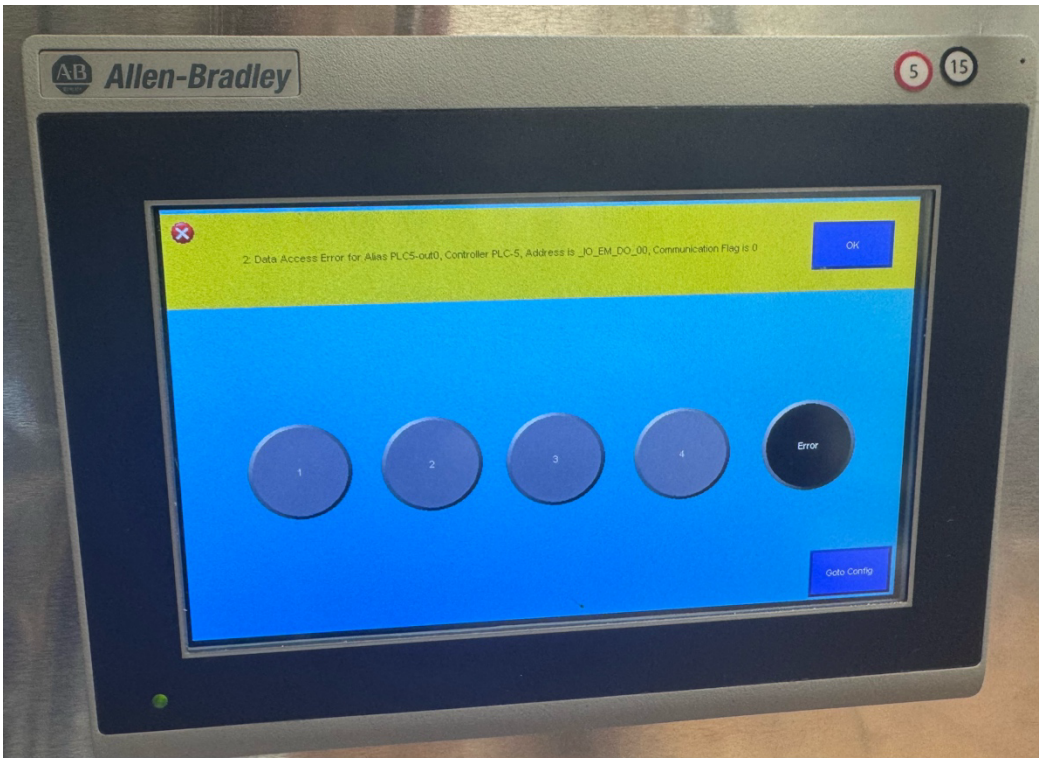

Figure 23 Error on HMI due to Network Cable Disconnection

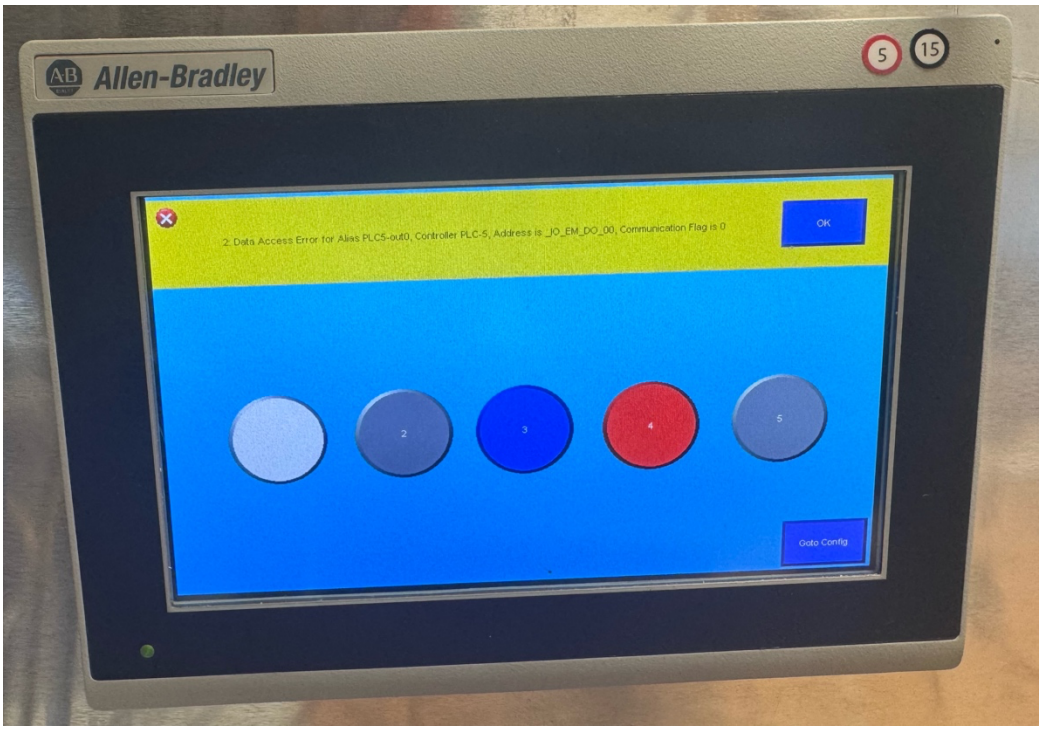

Figure 24 Reconnection of Network Cable and HMI Functioning Correctly

7.4 Cyber Security

It is typically quite difficult to predict what attackers may do inside a network. Therefore, ICS Cyber Kill Chain is a useful framework to follow for cyber testing as it has a broad scope and focuses on mitigating attacks early and disrupting the chain of events. In Stage 1, attackers may aim to infiltrate the system through various means (Assante and Lee, 2015). Due to time constraints, not all entry methods will be thoroughly tested. For this project, it is assumed the attacker has successfully accessed the central network switch and is operating as a MITM.

Once inside the system, the attacker may conduct reconnaissance, including network scanning, to gather information and plan a targeted Stage 2 attack. The goal of these cyber tests is to perform reconnaissance and execute initial attacks to gain information about the system.

Test ID	Req ID	Test Aim	Network	State
BST-CT1	C01-1 C01-2 C01-3	Verify that the product adheres to secure-by-design principles, defence-in-depth and zero-trust.	Figure 11	Assumed Pass
BST-CT2	C02-1 C04-1 C04-2 C04-3	Ensure that transmitted packets remain confidential and authentic, safeguarding against unauthorised access.	Figure 11	Pass
BST-CT3	C03-1	Ensure that transmitted packets maintain their integrity, preventing unauthorised modifications.	Figure 11	Pass
BST-CT4	C05-1 C05-2 C05-3	Perform tampering to ensure detection and prevention occurs.	Figure 11	Assumed Pass

Table 10 Cyber Security Test Plan

7.4.1 BST-CT1

For C01-1, the product's documentation claims adherence to secure-by-design principles, supported by its architecture. Using FPGAs instead of general-purpose processors removes reliance on traditional software stacks, eliminating classes of software vulnerabilities and reducing cyber intrusion risks. Pre-placed OTP keys negate the need for key exchanges, lowering exposure to key distribution attacks. Physical anti-tamper mechanisms and PUF classification provide hardware-level protection. Security is integrated from the outset, not added retroactively.

For C01-2, the product employs layered security through hardware components, OTP encryption, and anti-tamper controls. These overlapping safeguards ensure that if one layer is bypassed, others still provide protection. OTP, Twofish, and PUF technologies bolster cryptographic resilience, while physical protections deter tampering – forming strong defence-in-depth.

For C01-3, BST follow zero-trust principles as the product assumes no network component is inherently trustworthy. Each device operates independently, enforcing strict validation at every communication point. Embedded OTP keys eliminate the need for trust-based key exchanges, and the rules engine ensure only authorised packets are transmitted and received. Message authenticity is confirmed via cryptographic KAT, establishing trust through verification rather than assuming it by default.

7.4.2 BST-CT2

These tests aim to ensure that transmitted packets remain confidential and authentic, safeguarding against unauthorised access. A MitM attacker attempting to exfiltrate data is able to receive packets, as shown in Figure 25; however, the data is encrypted, assuring C02-1. Implementing stricter firewall rules – such as allowing traffic only from a defined list of trusted IP addresses – would prevent unauthorised devices from receiving packets unless they successfully spoof a permitted IP address.

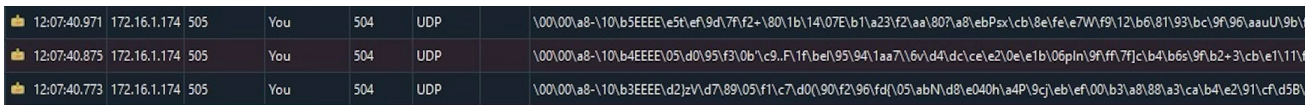

Figure 25 Encrypted Packet Data

A MitM attacker attempting to inject data packets into the network fails, as ICSProtect devices automatically drop unauthorised traffic, achieving C04-1, C04-2, C04-3. The endpoints do not register these packets because falsified traffic lacks the required BST header, which includes essential information such as the key index needed for decryption. Without this header, the packets are considered invalid and discarded immediately.

Additionally, the key index prevents replay attacks. If a man-in-the-middle (MitM) attacker captures traffic and attempts to replay it, the key index of the packet will be N-1, making it invalid. As a result, the packet will be immediately discarded by the system.

A MitM attacker attempting to modify packets would find it difficult due to the encryption of the traffic. However, if a MitM device does modify the packet, the endpoints will attempt to process it by first decrypting the KAT. The KAT is pre-placed in each device and never transmitted, so it will always decrypt to the expected value. If the KAT does not decrypt correctly, the packet will be discarded.

The KAT also serves to verify that legitimate traffic has been decrypted correctly. While plaintext traffic is easily identifiable as legitimate, IEC104 communications are often transferred in a format that is unreadable to humans. In such cases, the KAT ensures that the data has been decrypted correctly, providing a safeguard against tampering.

7.4.3 BST-CT3

The aim of the test was to verify that transmitted packets remain secure and unaltered, ensuring data integrity and resistance to unauthorised modification.

A MITM device can record traffic and attempt data exfiltration.

PacketSender was used to send the data '100messagelength' repeated up to 100 bytes to a legitimate endpoint, as shown in Figure 26.

12:07:45.944	172.16.1.174	505	You	504	UDP		100messagelength100messagelength100messagelength100message
12:07:45.832	172.16.1.174	505	You	504	UDP		100messagelength100messagelength100messagelength100message
12:07:45.752	172.16.1.174	505	You	504	UDP		100messagelength100messagelength100messagelength100message

Figure 26 Transmitted Plaintext Data Packets

Figures 27, 28 and 29 are packet captures that have been selected randomly. The data from the packets is shown to be encrypted. Despite all transmitted messages containing the same repeated plaintext ('100messagelength'), each packet displays a different ciphertext in the capture. This confirms that traffic is encrypted, and the encryption process produces unique outputs for identical inputs, validating the functionality of the OTP and achieving C03-1.

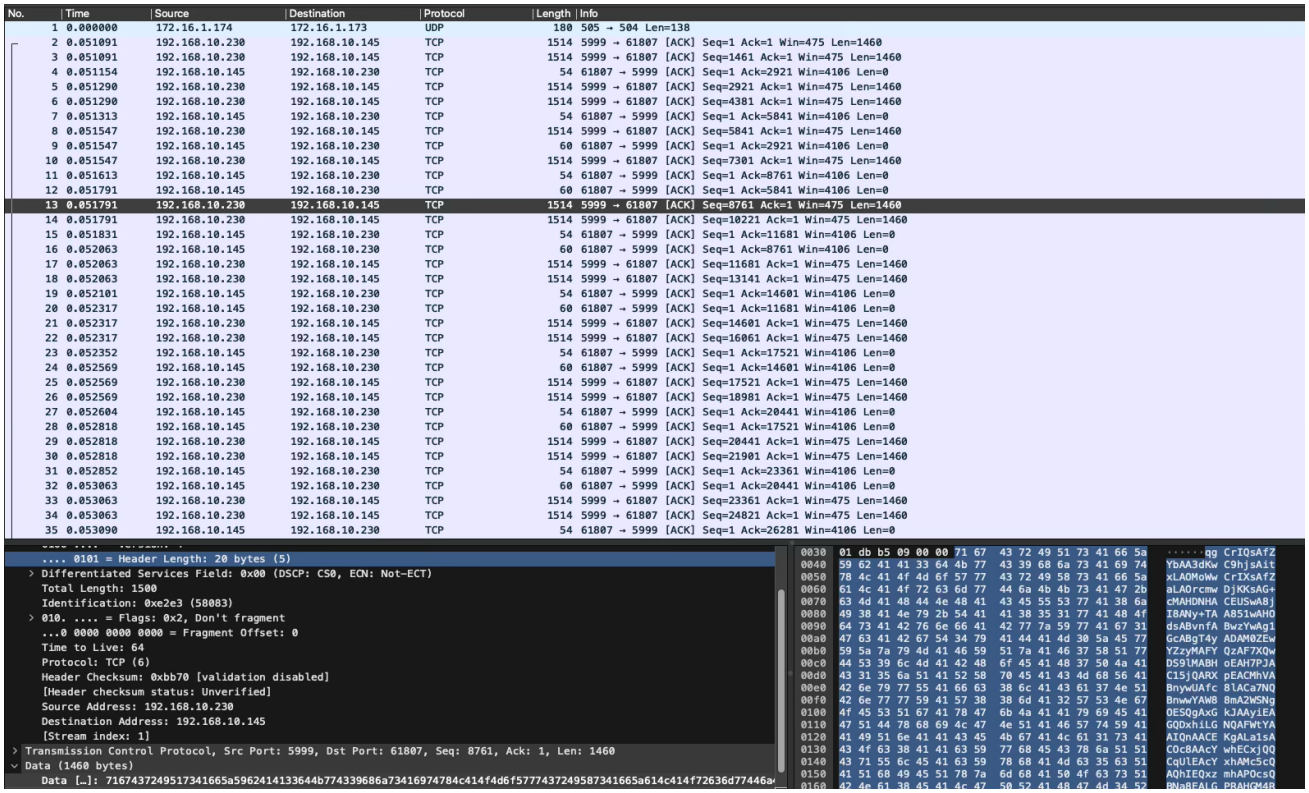

Figure 27 Encrypted Traffic Capture Sample '13'

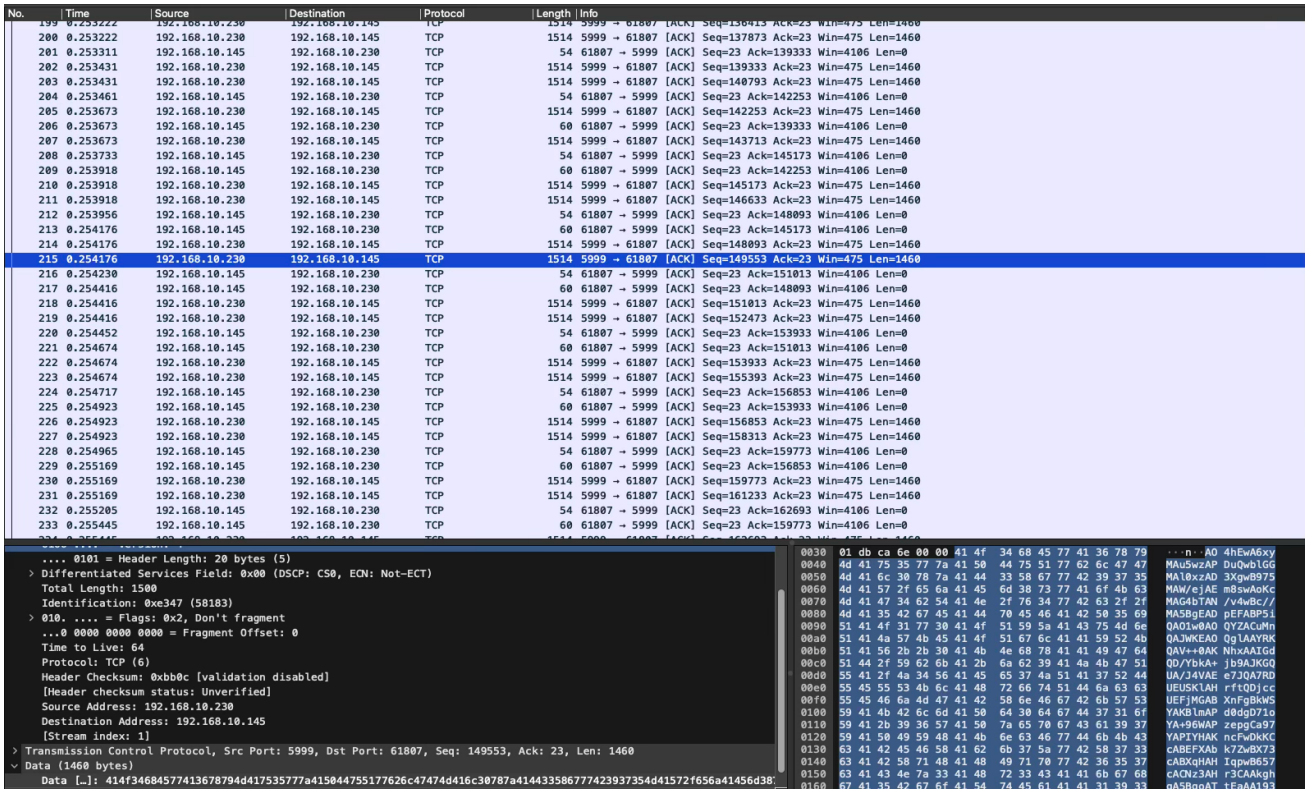

Figure 28 Encrypted Traffic Capture Sample '215'

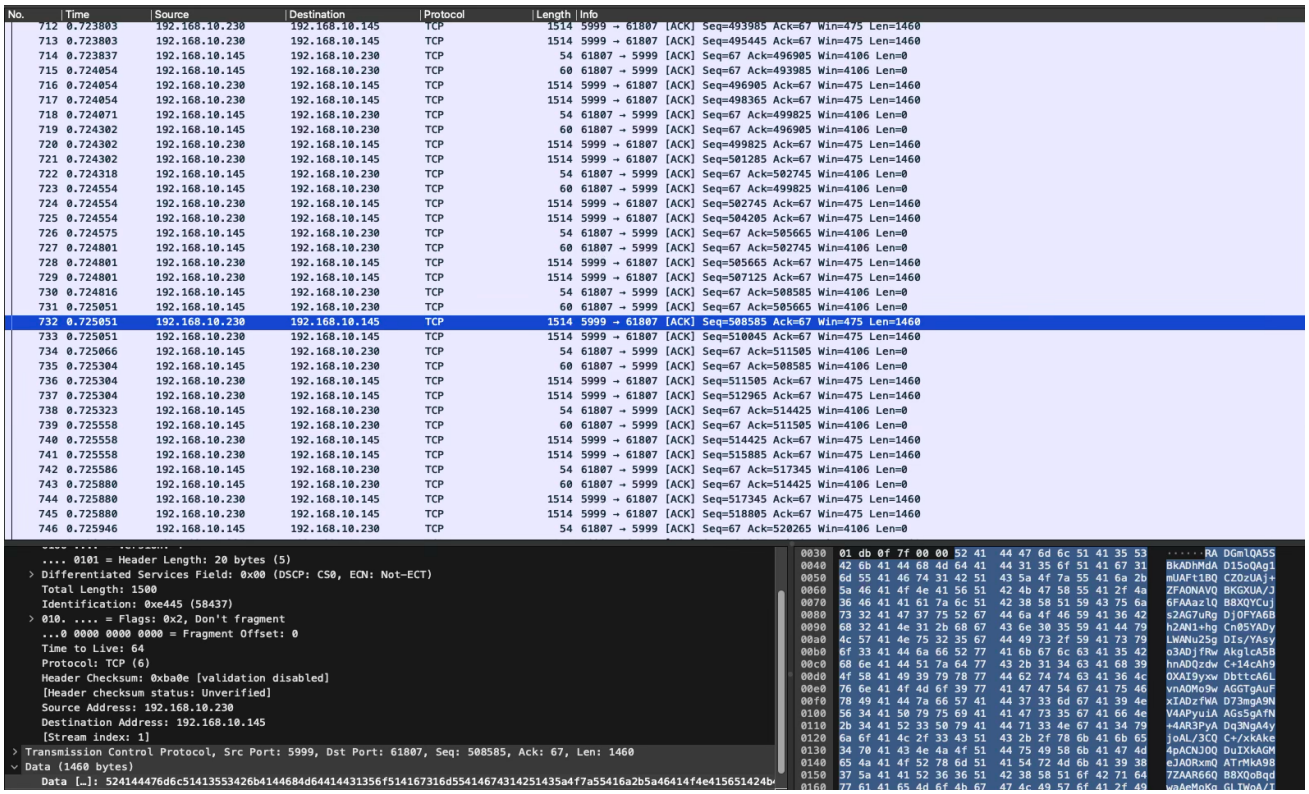

Figure 29 Encrypted Traffic Capture Sample '732'

Basic cryptanalysis was conducted on the extracted ciphertext in Figure 30 using open-source online tools, as shown in Table 11. While limited statistical analysis was possible, none of the tools succeeded in decrypting the message or revealing any meaningful information. The use of such tool increases our confidence, but it should be noted that an APT would likely possess greater capabilities and attempt more sophisticated cryptanalysis attacks.

Figure 30 Extracted Ciphertext for Analysis

Tool	Link	Methods attempted	Results
Cyber Chef	https://gchq.github.io/CyberChef/	Intensive ‘magic’ brute force decryption	Nothing of significance 4.95 entropy consistent with encrypted data, not plaintext
CrypTool Online	https://www.cryptool.org/en/cto/ncid/	AI algorithm identifier	54.76% Likelihood of Polyalphabetic Substitution Cipher
Enigmator	https://merri.cx/enigmator/cryptanalysis/crypto_identifier.html	Algorithm identifier	0.06 Index of Coincidence for Monoalphabetic Substitution
		Frequency analysis	Nothing of significance
CipherTools	https://www.ciphertools.co.uk/	Algorithm identifier	Incorrect plaintext
		Statistical analysis	Insignificant statistical findings
AI Cipher Solver	https://www.yeschat.ai/gpts-9t55Qj1n4LY-Cipher-Solver	This AI tool was given the encrypted text as ASCII, it was also given the algorithm Twofish and ECB mode as extra details.	Index of Coincidence: 1.62978 Chi-squared test: 6.16918

Table 11 Cryptanalysis Tool Results

Twofish is a highly secure, theoretically unbreakable (Easttom, 2016) encryption algorithm, strengthened by its key-dependent substitutions. When combined with the OTP, ICSProtect's encryption becomes extremely difficult – if not impossible – to break without access to the key.

Additionally, even with the emerging threat of quantum computing, the ICSProtect device remains secure due to its reliance on cryptographic methods that are inherently resistant to quantum attacks. The OTP is unaffected as it does not rely on mathematical problems such as prime factorisation or discrete logarithms, which underpin algorithms like Rivest-Shamir-Adleman (RSA). In the Additionally, the Twofish encryption algorithm used in ICSProtect derives its security from key-dependent transformations rather than mathematical assumptions vulnerable to quantum algorithms. Together, these elements provide strong, quantum-resistant protection well-suited to future developments.

Full captures of cryptanalysis have been included in Appendix D.

7.4.4 BST-CT4

To identify both physical and logical tampering, ICSProtect devices employ several mechanisms. Physically, the device functions as a PUF, ensuring that the OTP key block and internal FPGA logic are destroyed if the device is opened. Multiple methods are in place to detect such tampering and trigger this self-destruction, achieving C05-1.

For logical tampering, the devices can identify if their endpoint has been compromised and subsequently alert operators via syslog. As illustrated in Figure 31, a 'tamper cable' alert is raised when a network cable is disconnected and reconnected to a different endpoint, achieving C05-2 and C05-3. Device serial numbers have been redacted for confidentiality. There is capability to feed this syslog data into EDF's Security Operations Centre (SOC) for aggregated monitoring and analysis.

Figure 31 SYSLOG Displaying Tamper Alerts

7.5 Testing Conclusions

Testing of the ICSProtect device indicates strong performance in critical areas. Functionally, it meets key requirements for network communication, latency, throughput, and system response, successfully supporting bidirectional communication via the IEC-104 protocol. Latency remains within limits even at maximum packet sizes, essential for real-time data exchange in industrial control systems, and throughput is sufficient for operations.

Non-functional testing shows that the ICSProtect device meets long-term requirements for industrial applications, with a key management system based on an OTP that has a very long lifespan of encryption keys, reducing maintenance needs and enhancing longevity in environments where downtime is infrequent and costly.

Safety testing confirms quick recovery from power or network disruptions and providing clear device status indicators, ensuring reliable performance amidst interruptions.

Cybersecurity testing reveals strong protection against various attacks. The encryption provided by the ICSProtect secures data against breach attempts. It effectively blocks unauthenticated traffic to prevent data manipulation and maintain system integrity. It prevents exfiltration of data with strong encryption. Nonetheless, endpoints present a potential vulnerability, although containment measures mitigate risks from malware, limiting attack vectors. While firewall restrictions can limit endpoint commands, enhancing endpoint security remains beyond the scope of the protection provided by the ICSProtect device and relies on overall ICS architecture.

Overall, the ICSProtect provides significant security for industrial control system communications, including in NPPs. Its encryption, key management, and defence against common attack vectors form a solid foundation for securing critical infrastructure.

8 Evaluation

8.1 Project Approach

From the outset, this project has aimed to deliver a tangible real-world impact, addressing gaps in current ICS security tactics. It set out to be innovative and experimental, achieving this by exploring technologies previously unused in the nuclear industry. With strong interest and support from EDF, the project sought to meet critical industry needs, offering exciting potential for real-world implementation EDF NPPs.

Throughout the project, feedback from supervisory meetings helped refine both the methodology and scope. Early input was particularly useful in clarifying goals and ensuring purpose of the project was clearly communicated. One key suggestion led the project to look at the International Atomic Energy Agency (IAEA) as a valuable resource, prompting an analysis of global NPP ICS standards instead of just UK-based ones. This wider approach was crucial in defining requirements for the project. Feedback also led to a more technical product selection process during the requirements analysis, moving from qualitative to a more justified quantitative analysis. Discussions over various possible testing methods were crucial to the cyber methods used, with the ICS Cyber Kill Chain identified as a strong, applicable framework.

8.2 Project Successes

The project achieved several key successes, mainly due to its structured, engineering-based approach. A major decision was the use of the V-lifecycle model, which, while typically used in systems engineering, worked well for this cybersecurity-focused project. Its focus on thorough validation and verification at each stage of development, implementation, and testing matched the high levels of certainty needed for ICS. It also ensured that each phase of development was paired with verification and validation activities, which is critical in safety-focused fields.

The requirements analysis was a strong point of the project. It followed the INCOSE Systems Engineering Handbook, which is aligned with IEC15288, ensuring best practices for defining and managing engineering systems. The requirements were based on academic literature, OT security standards, and industry guidance. This approach ensured that the selected product addressed real-world constraints such as low-latency communication, support for industrial protocols, and resilience to environmental conditions. Customer-provided documentation was also reviewed to make sure the requirements aligned with operational realities.

The product selection phase used engineering methods, specifically the WSM method, to evaluate potential technologies. Safety was prioritised as the most important factor, given the NPP ICS context. This approach provided a clear, data-driven reason for selecting the best solution, rather than relying on assumptions.

The project also shows strong problem-solving skills with the test network design. For example, the lack of native IEC-104 hardware was addressed by simulating IEC-104 traffic using software tools and an Arduino, which helped confirm compatibility with the ICS protocol. Another challenge was the inability of Wireshark to measure microsecond-level latency, which was solved by using an oscilloscope for precise timing analysis, ensuring accurate validation of ICS real-time performance.

A realistic ICS testbed was built, enabling testing in an environment similar to real operational settings. This added to the reliability and validity of the test results. Testing was thorough, covering functional,

non-functional, safety, and security requirements. This reflects the systems engineering approach, where testing ensures that the entire system works reliably, safely, and as expected in realistic conditions.

8.3 Project Limitations

The testing process effectively demonstrated the capabilities of the ICSProtect, but several areas for improvement were identified. Although PLCs were used, they did not natively support the IEC-104 protocol, requiring emulation of IEC-104 traffic. Using hardware that natively supports IEC-104 would provide a more accurate representation of real-world ICS environments. However, the simulated set-up provides a good level of confidence in alignment with the expectations of this project, and further confirmation would be done during commissioning of the device, using the actual ICS in the NPP.

Additionally, while the PLCs included LEDs for basic control, no industrial sensors were part of the setup. This limited the system's exposure to live, changing data inputs, therefore it would be interesting to assess the impact of encryption on live process control and system responsiveness.

The Twofish encryption algorithm used is secure and resistant to most common attacks. However, due to limited access to advanced tools, only basic cryptanalysis was performed using open-source software, which did not allow for detailed inspection of encrypted traffic. Future work could involve deeper cryptographic analysis, including brute-force attempts or stress testing, to gain a better understanding of the system's resilience under targeted attacks.

While the project primarily focused on threats from remote attackers using man-in-the-middle techniques, insider threats – where an attacker operates from a trusted endpoint – present a different risk. In such cases, malware could impersonate legitimate traffic and issue harmful IEC-104 commands. Although the firewall offers some protection by restricting traffic to IEC-104, a skilled attacker could still exploit the protocol to cause damage. Although, standard endpoint hardening practices in critical infrastructure, such as access controls, unnecessary service disabling and physical port blocking would help mitigate this risk. Future studies could explore endpoint vulnerabilities and the resilience to internal cyber attacks.

8.4 Project Conclusion

In conclusion, this project successfully achieved its goals and objectives of finding a solution to secure communications within two safety-critical ICS. Through a comprehensive evaluation, the project provided valuable insights to EDF, offering a detailed assessment of the ICSProtect capabilities and its potential for deployment. The findings not only demonstrated the system's effectiveness but also highlighted its real-world significance, which will particularly impact the future deployment of BST's ICSProtect devices onto EDF NPPs. The project has made a tangible impact, showcasing its relevance and importance in enhancing the security of safety-critical ICS.

Bibliography

Ahmad, A., Webb, J., Desouza, K.C. and Boorman, J. (2019) Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security* [online]. 86, pp. 402–418. Available from: https://www.researchgate.net/publication/334274476_Strategically-Motivated_Advanced_Persistent_Threat_Definition_Process_Tactics_and_a_Disinformation_Model_of_Counterattack [Accessed 14 March 2025].

Anon (2019) *V-Model Wikipedia*. 16 March 2019 [online]. Available from: https://en.wikipedia.org/wiki/V-Model.

Arinze, U.C., Longe, O.B. and Eneh, A.H. (2020) Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues. *International Journal of Nuclear Security* [online]. 6 (1). Available from: https://trace.tennessee.edu/cgi/viewcontent.cgi?article=1096&context=ijns [Accessed 26 March 2025].

Assante, M. and Lee, R. (2015) *The Industrial Control System Cyber Kill Chain* [online]. Available from: https://sansorg.egnyte.com/dl/k7gJ2gVBj5 [Accessed 26 March 2025].

Ayodeji, A., Mohamed, M., Li, L., Di Buono, A., Pierce, I. and Ahmed, H. (2023) Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors. *Progress in Nuclear Energy* [online]. 161, p. 104738. Available from: https://www.sciencedirect.com/science/article/pii/S0149197023001737.

Balaji, S. and Sundararajan, M. (2012) International Journal of Information Technology and Business Management WATEERFALLVs V-MODEL Vs AGILE: a COMPARATIVE STUDY ON SDLC. *International Journal of Information Technology and Business Management* [online]. 2 (1). Available from: https://mediaweb.saintleo.edu/Courses/COM430/M2Readings/WATEERFALLVs%20V-MODEL%20Vs%20AGILE%20A%20COMPARATIVE%20STUDY%20ON%20SDLC.pdf [Accessed 18 November 2024].

Bhole, M., Kastner, W. and Sauter, T. (2024) IT Security Solutions for IT/OT Integration: Identifying Gaps and Opportunities. *2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA)* [online]. All Days, pp. 01–08. Available from: https://www.researchgate.net/publication/384985182_IT_Security_Solutions_for_ITOT_Integration_Identifying_Gaps_and_Opportunities [Accessed 26 March 2025].

Blueskytec (2024) *ICSProtect Datasheet*.

Bouhdada, J. and Ayala, M. (2024) *Securing Industrial Control Systems and Safety Instrumented Systems*. Packt Publishing Ltd.

Bradner, S. (1997) *Key Words for Use in RFCs to Indicate Requirement Levels (RFC 2119) Ietf.org*. 1997 [online]. Available from: https://www.ietf.org/rfc/rfc2119.txt [Accessed 26 March 2025].

Cappelli, M. (2023) *Instrumentation and Control Systems for Nuclear Power Plants*. Woodhead Publishing.

Carlson, J., Gunter, D., Roberts, C., Gordon, C. and Masters, G. (2022) *Do IT Cryptographic Security Controls Work for Energy Systems? Do IT Cryptographic Security Controls Work for Energy Systems?* [online]. Available from: https://selinc.com/api/download/134054/ [Accessed 9 April 2025].

'CipherTools' (2025) *Ciphertools.co.uk*. 2025 [online]. Available from: https://www.ciphertools.co.uk/ [Accessed 9 April 2025].

Cisco Systems (2021) *Cisco Secure Firewall ISA3000 Datasheet* [online]. Available from: https://www.cisco.com/c/en/us/products/collateral/security/industrial-security-appliance-3000/data-sheet-c78-735839.pdf [Accessed 08 January 2025]

Conklin, Wm.A. (2016) IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc. *2016 49th Hawaii International Conference on System Sciences (HICSS)* [online]. Available from: https://ieeexplore.ieee.org/document/7427514?denied= [Accessed 13 February 2025].

'Crypto Identifier - Enigmator' (2025) *Merri.cx*. 2025 [online]. Available from: https://merri.cx/enigmator/cryptanalysis/crypto_identifier.html [Accessed 9 April 2025].

Department for Business, Energy & Industrial Strategy (2022) *Civil Nuclear Cyber Security Strategy* [online]. Available from: https://assets.publishing.service.gov.uk/media/627df8658fa8f53f9a15c1d5/civil-nuclear-cyber-security-strategy-2022.pdf [Accessed 26 March 2025].

Department for Communities and Local Government (2009) *Multi-criteria analysis: a manual* [online]. Available from: https://assets.publishing.service.gov.uk/media/5a790545e5274a2acd18b975/1132618.pdf.

Doran, G.T. (1981) *There's a SMART Way to Write Management's Goals and objectives.* In: *Journal of Management Review* [online]. Available from: https://community.mis.temple.edu/mis0855002fall2015/files/2015/10/S.M.A.R.T-Way-Management-Review.pdf.

Dragos (2025) *2025 OT/ICS Cyber Security Report* [online]. Available from: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsLang=en [Accessed 26 March 2025].

Easttom, C. (2016) *Modern Cryptography Applied Mathematics for Encryption and Information Security*. New York Mcgraw-Hill Education.

Elseta (2025) *IEC 60870-5-104 | Elseta Knowledge Base Elseta.com*. 2025 [online]. Available from: https://wiki.elseta.com/books/the-vinci-software/page/iec-60870-5-104 [Accessed 26 March 2025].

Emerson (2015) *Safety Integrity Level (SIL) -61508/61511 Background: Background* [online]. Available from: https://www.emerson.com/documents/automation/technical-white-paper-safety-integrity-level-sil-en-71898.pdf.

Fang, S., Amy Myers Jaffe, Loch-Temzelides, T. and Chiara Lo Prete (2024a) Electricity grids and geopolitics: A game-theoretic analysis of the synchronization of the Baltic States' electricity networks with Continental Europe. *Energy Policy* [online]. 188 (114068). Available from: https://bpb-us-e1.wpmucdn.com/blogs.rice.edu/dist/e/12335/files/2024/09/Geopolitics-of-Electricity-Grids.pdf.

Fang, S., Jaffe, A.M., Loch-Temzelides, T. and Lo Prete, C. (2024b) Electricity Grids and geopolitics: a game-theoretic Analysis of the Synchronization of the Baltic States' Electricity Networks with Continental Europe. *Energy Policy* [online]. 188, p. 114068. Available from: https://bpb-us-e1.wpmucdn.com/blogs.rice.edu/dist/e/12335/files/2024/09/Geopolitics-of-Electricity-Grids.pdf [Accessed 26 March 2025].

GCHQ (2019) *CyberChef Github.io*. 2019 [online]. Available from: https://gchq.github.io/CyberChef/.

Genge, B., Haller, P. and Kiss, I. (2017) Cyber-Security-Aware Network Design of Industrial Control Systems. *IEEE Systems Journal* [online]. 11 (3), pp. 1373–1384. Available from: https://www.researchgate.net/publication/283165318_Cyber-Security-Aware_Network_Design_of_Industrial_Control_Systems [Accessed 26 March 2025].

Ghosh, A. (2020) Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks. *International Research Journal of Engineering and Technology* [online]. Available from: https://www.researchgate.net/publication/342764235_Comparison_of_Encryption_Algorithms_AES_Blowfish_and_Twofish_for_Security_of_Wireless_Networks [Accessed 9 April 2025].

INCOSE (2023) *INCOSE Systems Engineering Handbook*. 5th edition. Newark: John Wiley & Sons, Incorporated. [Accessed 08 January 2025]

International Atomic Energy Agency (2016) *Approaches for overall I&C architectures of NPPs Iaea.org*. 2016 [online]. Available from: https://www.iaea.org/publications/np-t2.11 [Accessed 26 March 2025].

International Atomic Energy Agency (2021) *Nuclear Security Series No. 42-G Implementing Guide* [online]. Available from: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf [Accessed 26 March 2025].

International Electrotechnical Commission (2015) *Systems and Software Engineering – System Life Cycle Processes (IEC 15288:2015)*. 2015 [online]. Available from: https://www.iso.org/standard/63711.html#:~:text=ISO%2FIEC%2FIEEE%2015288%3A2015%20establishes%20a%20common%20framework,hierarchy%20of%20a%20system's%20structure..

Jones, S.G. (2025) *Russia's Shadow War against the West* [online]. Centre for Strategic and International Studies. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250318_Jones_Russia_Shadow.pdf?VersionId=LHamL2L7HJwLgZ7a_wq6xkTIwMh3TFpk.

Karmakar, G., Wakankar, A., Kabra, A. and Pandya, P. (2023) *Development of Safety-Critical Systems* [online]. Springer. Available from: https://link.springer.com/book/10.1007/978-3-031-27901-0.

Kumar, A., Behera, R.P., Kumar, A. and Narasimhan, S. (2023) Strengthening Network Security in Safety-Critical I&C Systems of Nuclear Reactors: Design and Implementation of a Robust Data Diode. *2023 IEEE 20th India Council International Conference (INDICON)* [online]. pp. 1398–1403. Available from: https://www.researchgate.net/publication/378531814_Strengthening_Network_Security_in_Safety-Critical_IC_Systems_of_Nuclear_Reactors_Design_and_Implementation_of_a_Robust_Data_Diode [Accessed 26 March 2025].

Mandiant (2024) *M-Trends 2024 Special Report* [online]. Google Cloud Security. Available from: https://services.google.com/fh/files/misc/m-trends-2024.pdf [Accessed 26 March 2025].

Mannion, M. and Keepence, B. (1995) SMART requirements. *ACM SIGSOFT Software Engineering Notes* [online]. 20 (2), pp. 42–47. Available from: https://www.researchgate.net/publication/2937339_SMART_requirements.

Matoušek, P. (2017) *Description and Analysis of IEC 104 Protocol Petr Matoušek* [online]. Available from: https://www.fit.vut.cz/research/publication-file/c168651/279814/TR-IEC104v2.pdf [Accessed 26 March 2025].

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M. and Karri, R. (2016) The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE* [online]. 104 (5), pp. 1039–1057. Available from: https://www.researchgate.net/publication/298728032_The_Cybersecurity_Landscape_in_Industrial_Control_Systems [Accessed 26 March 2025].

Mobley, C. (2024) *High Availability for Legacy Systems*. Blueskytec.

Mobley, C. (2025) *KST Technical Overview*. Blueskytec.

Monmasson, E., Idkhajine, L., Cirstea, M.N., Bahri, I., Tisan, A. and Naouar, M.W. (2011) FPGAs in Industrial Control Applications. *IEEE Transactions on Industrial Informatics* [online]. 7 (2), pp. 224–243. Available from: https://centralesupelec.hal.science/hal-01337007v1/document [Accessed 26 March 2025].

National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0* [online]. 2.0 (29). Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

‘Neural Cipher Identifier - CrypTool’ (2025) *Cryptool.org*. 2025 [online]. Available from: https://www.cryptool.org/en/cto/ncid/ [Accessed 9 April 2025].

Office for Nuclear Regulation (2022) *Security Assessment Principles for the Civil Nuclear Industry* [online]. Available from: https://www.onr.org.uk/media/g05fszjn/security-assessment-principles.pdf [Accessed 26 March 2025].

Richardson, J.C. (2011) Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. *SSRN Electronic Journal* [online]. 29 (1). Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888.

Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. *NIST Special Publication* [online]. 800 (207). Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Rubio, M. (2019) *The Mini Book of Agile Everything You Really Need to Know about Agile, Agile Project Management and Agile Delivery*. Birmingham, Packt Publishing, Limited.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D. and Hall, C. (1998) *Twofish: A 128-Bit Block Cipher* [online]. Available from: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf [Accessed 9 April 2025].

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N. and Kohno, T. (2000) *The Twofish Team’s Final Comments on AES Selection* [online]. Available from: https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-final.pdf?utm_source=chatgpt.com [Accessed 9 April 2025].

Siemens (2017) *CoreShield Data Capture Unit Data Sheet* [online]. Available from: https://dq3yfnoirppqu.cloudfront.net/dex-assets/03-catalog-section/03-applications/coreshield-data-capture-unit/DCU%202.0_datasheet_EN.pdf [Accessed 08 January 2025].

Siemens (2020) *Data Diodes Vs Firewalls* [online]. Available from: https://www.mobility.siemens.com/global/en/portfolio/digital-solutions-software/cybersecurity/cybersecurity-rail-infrastructure/difference-data-diode-and-firewall.html [Accessed 26 March 2025].

Stephen, O. and Oriaku, K.A. (2014) Software Development Methodologies: Agile Model Vs V-Model. *International Journal of Engineering and Technical Research (IJETR)* [online]. 2 (11). Available from: https://www.erpublication.org/published_paper/IJETR022742.pdf [Accessed 26 March 2025].

Stouffer, K. *et al.* (2023) Guide to Operational Technology (OT) Security. *Guide to Operational Technology (OT) Security* [online]. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

Toepper, J. (2013) *Industrial Networking Security Best Practices* [online]. MOXA. Available from: https://www.moxa.com/en/literature-library/industrial-networking-security-best-practices [Accessed 26 March 2025].

Walden, D.D., Roedler, G.J., Forsberg, K., Hamelin, R.D. and Shortell, T.M. (2023) *INCOSE Systems Engineering Handbook* 5th edition. Hoboken, New Jersey, Wiley.

Yastrebenetsky, M.A. (2020) *Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems Advances in information security, privacy, and ethics book series* [online]. IGI Global. Available from: https://pure.bangor.ac.uk/ws/portalfiles/portal/59763018/1_s2.0_S0149197023001737_main.pdf [Accessed 21 March 2025].

Appendix A

Score	Description
5	Requirement fully satisfied.
4	Requirement likely satisfied, but testing is needed for confirmation.
3	Requirement mostly satisfied, but with some uncertainty or limitations.
2	Requirement partially satisfied, but with limitations.
1	Requirement not fully satisfied, with clear limitations.
0	Requirement not met, or information not available.

Table 12 Requirement Scoring Criteria

Req ID	Data Diode	Firewall	Encryption	Analysis
Functional (0.25)				
F01-1	5	5	5	All devices support the IEC104 protocol.
F02-1	5	5	5	All devices can send data, but the diode only in one direction.
F02-2	0	5	5	Data diode only supports unidirectional flow.
F03-1	5	3	4	Data diode has low latency; firewall latency varies based on security policies; encryption latency varies on the data packet size.
F04-1	5	3	4	All devices meet the throughput requirement to some extent.
Non-Functional (0.1)				
N01-1	4	3	4	All devices are designed to integrate with industrial systems, firewalls may not permit all industrial protocols.
N01-2	5	3	5	Firewall may require rule configurations.
N02-1	5	3	5	Firewall may require more frequent updates.
N02-2	4	2	3	Firewalls have long lifespans but may require hardware refresh, data diodes are designed for longevity, the encryption device does not require updates.
N03-1	4	3	5	Data Diode: 0 °C to +70 °C Firewall: -40º to +60ºC Encryption: -40ºC to +100ºC
N03-2	3	5	5	Firewall: 5% to 95% Encryption: 0% to 70%
Safety (0.4)				
S01-1	0	5	4	Encryption and firewalls include detection features; data diodes do not.
S01-2	0	5	5	Firewalls and encryption devices can adapt; data diodes are static in design.
S01-3	4	4	5	Firewalls and encryption devices enter a fail-safe mode.
S01-4	4	4	5	Firewalls and encryption devices resume operation when faults are fixed.

Cyber Security (0.25)				
C01-1	4	4	5	All devices follow secure-by-design principles.
C01-2	4	5	5	All devices can be used in redundant configurations.
C01-3	1	3	5	Not all devices apply zero-trust.
C02-1	1	2	4	Only the firewall and encryption device prevent unauthorised receipt of information, however the firewall does not prevent plaintext communications from being read.
C03-1	1	1	4	Only the encryption device ensures data integrity.
C04-1	1	3	4	Authentication mechanisms available on the firewall and encryption device, firewall is dependent on configuration security.
C04-2	1	3	4	Authentication mechanisms available on the firewall and encryption device, firewall is dependent on configuration security.
C04-3	1	3	4	Firewall and Encryption can enforce authentication controls.
C05-1	1	2	4	Firewall has “anti-tamper chip”. Encryption has multiple physical and logical anti-tamper mechanisms.
C05-2	1	2	4	Firewall and encryption device both include tamper detection.
C05-3	1	2	4	Firewall and encryption device both include tamper detection.
Scoring Totals				
Func	1.00	1.05	1.15	The scores reveal that the BST ICSProtect is the most suitable solution for deployment.
Non-Func	0.42	0.32	0.45	
Safety	0.80	1.80	1.90	
CyberSec	0.39	0.68	1.07	
Total	**2.60**	**3.85**	**4.57**	

Table 13 MCDM Analysis

Appendix B

Test ID	Req ID	Test Aim	Network	Method	Expected Outcome	Actual Outcome	State
BST-FT1	F01-1 F02-1 F02-2	Validate IEC104 protocol usage and bidirectional communication.	Figure 8	Use Vinci to generate IEC-104 and send traffic between devices. Verify that messages are received and correctly interpreted in both directions.	Messages sent, received and correctly interpreted in both directions	IEC104 traffic observed on laptop UDP traffic observed on Wireshark	Pass
BST-FT2	F03-1	Measure data transmission latency	Figure 10	Use Packet Sender to send 600-byte packets continuously. Record timestamps for packet transmission and reception. Calculate the time difference between transmission and reception.	Time delay between packet transmission and receipt less than 250µs	89.6µs time delay observed	Pass
BST-FT3	F04-1	Measure data transmission throughput	Figure 9	Use Packet Sender to send 600-byte packets continuously. Measure the data rate over a defined period. Record the throughput in MB/s.	Successful throughput of MB/s observed for 600byte packets.	MB/s observed	Pass
BST-NT1	N01-1 N01-2	Verify interoperability with all connected devices, ensuring no reconfiguration is required for deployment.	N/A	Connection of ICSProtect devices into PLC and HMI network, ensuring the PLCs and HMIs can function as intended.	ICS functioning as intended.	ICS functioning as intended with no interoperability issues.	Assumed Pass
BST-NT2	N02-1	Verify maintenance and lifetime expectations	N/A	Calculations for expected traffic and key usage	≥60 years of operational support with minimal maintenance	~730.67 million years of use possible with no updates required	Pass
BST-NT3	N03-1 N03-2	Verify environmental suitability.	N/A	Examine data sheets.	The product meets the expected temperature range of X and humidity range of X.	Temperature range of -40ºC to +60ºC, humidity range of	Assumed Pass
BST-ST1	S01-1 S01-2 S01-3 S01-4	Introduce power faults and observe network behaviour to ensure system recover quickly and effectively.	Figure 9	Disconnect power cable from ICSProtect device. Observe system reactions. Reconnect power cable and observe time to recover and resume operations.	Device continues operating with no errors after cable has been reconnected.	Device continues operating within 2 seconds, with amber and green light indications.	Pass
BST-ST2	S01-1 S01-2 S01-3 S01-4	Introduce network faults and observe network behaviour to ensure system recover quickly and effectively.	Figure 9	Disconnect network cable from ICSProtect device. Observe system reactions. Reconnect network cable and observe time to recover and resume operations.	Device continues operating with no errors after cable has been reconnected.	Device continues operating within 1.5 seconds, with the indication of the HMI registering the PLC states.	Pass
BST-CT1	C01-1 C01-2 C01-3	Verify that the product adheres to secure-by-design principles and defence-in-depth.	Figure 11	Documentation review of design and architecture.	Product adheres to secure-by-design and defence-in-depth principles.	Product appears to adhere to secure-by-design and can be used redundantly.	Assumed Pass
BST-CT2	C02-1 C04-1 C04-2 C04-3	Ensure that transmitted packets remain confidential and	Figure 11	MitM device attempting to exfiltrate and inject data.	No readable plaintext on attacking machine.	No readable plaintext on attacking machine.	Pass

		authentic, safeguarding against unauthorised access.			No ability to send packets to systems from attacking machine.	No ability to send packets to systems from attacking machine.	
BST-CT3	C03-1	Ensure that transmitted packets maintain their integrity, preventing unauthorised modifications.	Figure 11	Analyse encrypted packet captures in Wireshark and using cryptanalysis tools to ensure no plaintext is gained.	No plaintext gained.	No data gained from cryptanalysis. Packets are securely encrypted.	Pass
BST-CT4	C05-1 C05-2 C05-3	Identify physical and logical tampering efforts.	Figure 11	Unplug network cable and monitor logs.	Tamper alert sent to logs.	Tamper alert sent to logs and device is PUF, so physical tampering will destroy internal structure.	Pass

Table 14 Complete Test Plan

Appendix C

	Letter	Calculation	Value	Notes
OTP Entropy	E	2^64	18446744073709600000	Key bit entropy within OTP
Number of expected messages per second	M	800 updates per second	800	From requirements analysis (800 updates/second)
Keys used per second	K/s	K/s = M	800	Each message uses a unique key
Keys used per year	K/y	K/y = K/s * 60^2 * 24 * 365.25	25246080000	Use of 365.25 to account for leap years
Years of use	Y	Y = E ÷ K/y	730677557.613285	~730.7 million years

Table 15 ICSProtect Key Usage Calculations

	Letter	Calculation	Value	Notes
OTP Entropy	E	2^64	18446744073709600000	Key bit entropy within OTP
Total Number of Keys	T	T = E * 2^31	396140812571323000000000000000	2^31 for possible new entropy blocks
Number of expected messages per second	M	800 updates per second	800	From requirements analysis (800 updates/second)
Keys used per second	K/s	K/s = M	800	Each message uses a unique key
Keys used per year	K/y	K/y = K/s * 60^2 * 24 * 365.25	25246080000	Use of 365.25 to account for leap years
Years of use	Y	Y = T ÷ K/y	15691181069351100000	~1.57 quintillion years

Table 16 ICSProtect Key Usage Calculations with 'Remixing'

Appendix D

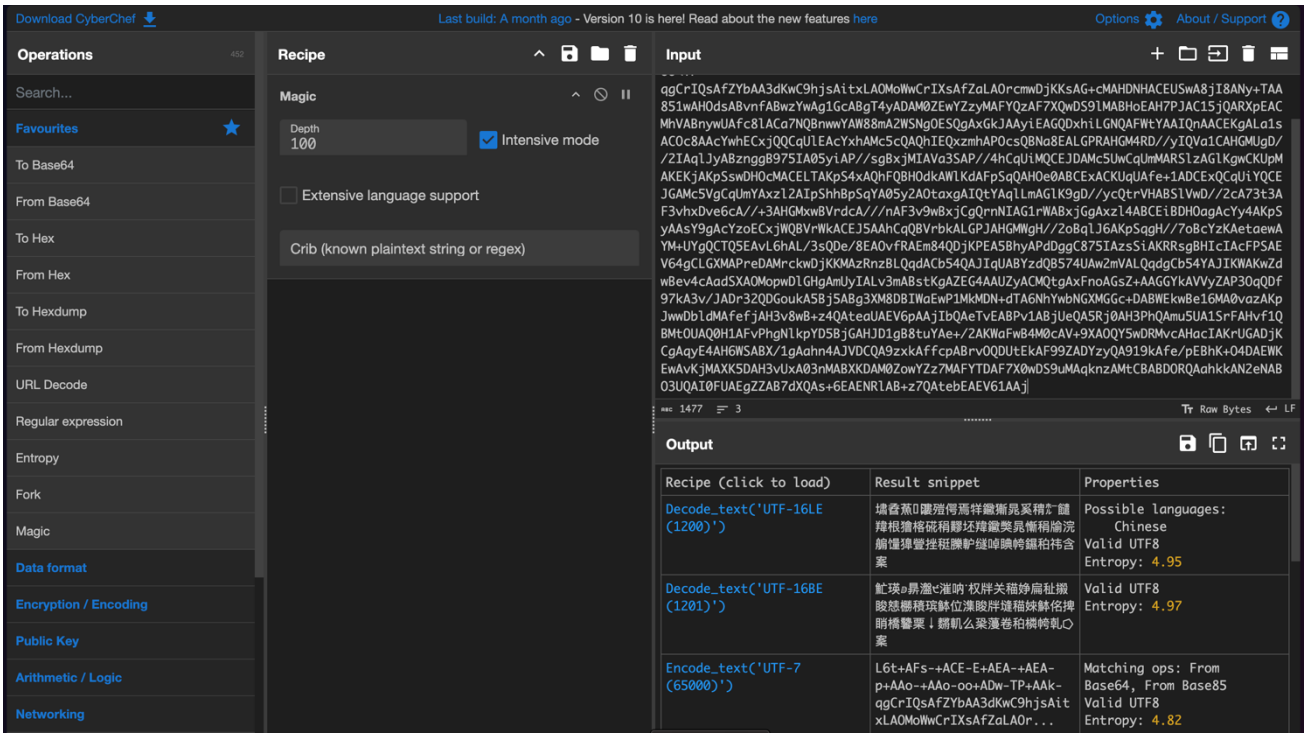

Figure 32 CyberChef Cryptanalysis

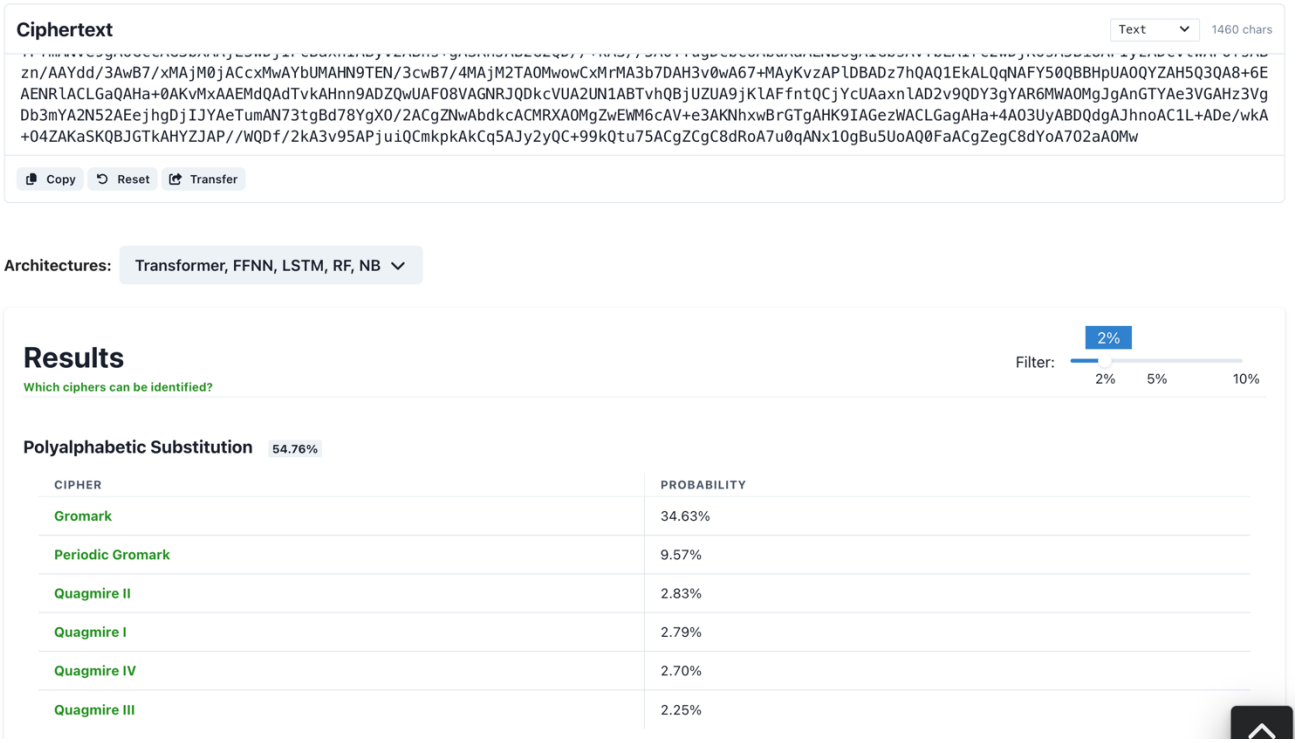

Figure 33 CrypTool Online Cryptanalysis

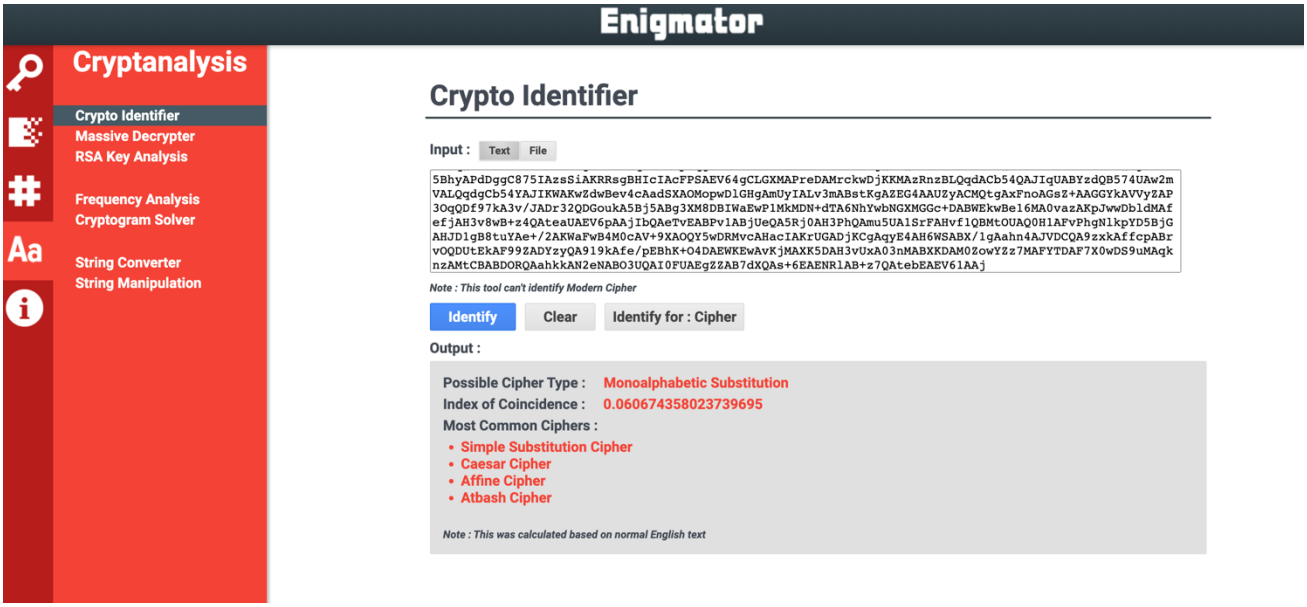

Figure 34 Enigmator Cryptanalysis

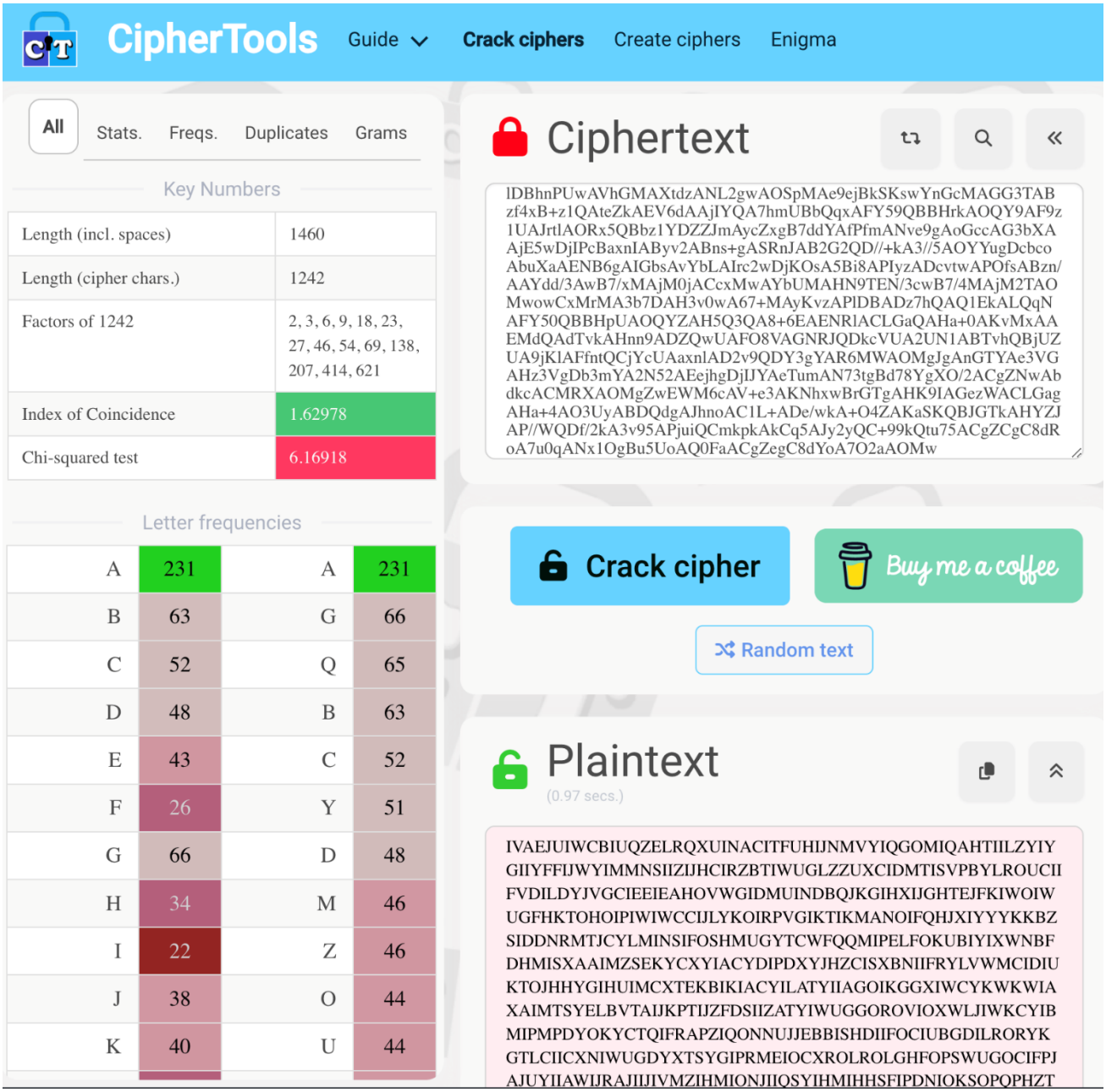

Figure 35 CipherTools Cryptanalysis