Theme 1

eApplication



Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Copyright © 2026 C²S Consulting

Licenced under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Incident Timeline & Forensic Briefing.....5

2 2. Current Plant Configuration Metrics.....6

3 The Team Dilemma.....7

3.1 The Specific Choice Challenge.....7

3.2 Dataset.....7

4 Simultaneous Reporting Instructions.....8

Theme 1 Case Study: The Cascading Failure at the Blessington Catchment (Ballymore Eustace)

1 Incident Timeline & Forensic Briefing

Teams act as elite automation and cybersecurity response engineers dispatched by Uisce Éireann. Six hours ago, a devastating water treatment compromise occurred at the critical infrastructure interface feeding the Dublin trunk mains.

1. Initial Perimeter Ingress: T-Minus 4 Hours.

An engineering contractor's laptop was infected with malware via a public Wi-Fi hotspot in Dublin. Using valid, legacy VPN credentials, the contractor established a direct remote access connection into the facility's Level 3 Supervisor Network. Because the asset uses a completely Decentralised Account Architecture, there was no centralised authentication server (such as Kerberos) or reverse proxy enforcing perimeter validation.

2. Lateral Movement: T-Minus 2 Hours.

The malware scanned the flat interior network architecture, bypassed the unconfigured internal firewall separating corporate IT from the treatment plant's OT networks, and compromised the local SCADA historian server. The attacker used this access to run a script that systematically harvested operational passwords from unencrypted memory strings.

3. Process Manipulation: T-Minus 45 Minutes.

Using compromised administrative accounts, the attacker sent malicious configuration binaries down to the Level 1 PLCs over an unencrypted Fieldbus protocol. The malicious payload altered the ladder logic controlling the chemical dosing pumps at the rapid gravity filtration stage, forcing an unsafe over-chlorination setpoint.

4. System Blindness & Power Drop: T-Minus 15 Minutes.

To prevent plant operators from intervening, the attacker modified the SCADA HMI database to display perfectly normal, static residual chlorine readings (spoofing). At the exact same moment, the local ESB grid experienced a localised power failure. While the backup generators kicked on to handle critical water flows, the building's HVAC system failed under the initial generator load switch, causing rapid thermal accumulation in the main control room and triggering an automated thermal shutdown of the Safety Instrumented System (SIS).

2 Current Plant Configuration Metrics

The current system data state across plant parameters reveals highly critical structural vulnerabilities:

Architectural Component	Current Security Rating	Primary Engineering Protocol / Defect
Perimeter Isolation	Vulnerable (Low)	Flat network topology; no Industrial DMZ or Reverse Proxies.
Authentication Logic	Deficient (None)	Decentralised user databases; no token-based or centralised IAAA.
Physical Hardening	Moderate	Locked doors, but unmonitored Fieldbus routing and HVAC single point of failure.
Process Logic Integrity	Critical (High Risk)	No verification of logic/binary updates on Level 1 PLCs.

3 The Team Dilemma

Uisce Éireann has authorised an immediate emergency engineering allocation of €150,000. Due to the critical reliance of Dublin's hospitals and citizens on this exact water supply, you can only implement ONE major remediation project before the plant is brought fully back online tomorrow afternoon.

3.1 The Specific Choice Challenge

Review the technical plans below. Your team must debate, choose exactly ONE option, and prepare to defend your choice against competing teams simultaneously.

- **Option A: The Logical Boundary Overhaul**
  - **Remediation**: Deploy a centralised Kerberos network domain controller and implement an authenticated Reverse Proxy at the industrial network perimeter.
  - **Impact**: Completely prevents credential-stuffing and unauthorised network ingress via external contractors.

- **Option B: The Purdue Architectural Isolation Project**
  - **Remediation**: Re-engineer the perimeter firewalls to create a strict, multi-layered Industrial DMZ between Levels 3 and 4, and physically rewire the Level 1/0 serial Fieldbuses into isolated, cryptographically segmented network segments.
  - **Impact**: Blocks all lateral traversal of malware and stops unauthorised modification of local PLC command lines.
  -
- **Option C: Environmental & Safety Hardening**
  - **Remediation**: Reconfigure the facility's backup generator circuitry to keep the main server/controller room HVAC running during blackouts, and hard-code the Safety Instrumented System (SIS) logic to default to a mechanical "fail-safe" isolated state regardless of SCADA feedback.
  - **Impact**: Ensures absolute safety, maintainability, and operational visibility even during catastrophic infrastructure power failures.

3.2 Dataset

To help your team evaluate the cascading risk profiles of each option under varying environmental conditions, use the spreadsheet, ***Theme 1 eApplication: Risk Mitigation Simulation Data***, as a tool for assessment before making your definitive selection.

4 Simultaneous Reporting Instructions

When the timer expires, every team will simultaneously select their option in the virtual learning system (A, B, or C).

Cross-Examination Prep*: Be prepared to justify why your chosen remediation is the most critical structural dependency.*

5 Lecturer Notes

5.1 The Strongest Engineering Argument: Option B (Purdue Isolation)

Why it’s the most correct technical defence: In an industrial environment, network segregation is your absolute fallback line of defence.

- Even if an attacker steals valid credentials (which beats Option A), strict Purdue Model isolation and an Industrial DMZ prevent that attacker from moving laterally from the corporate or supervisor network down to the engineering/process layers (Levels 1 and 0).
- Furthermore, segmenting and encrypting the serial Fieldbus lines directly stops the rogue hardware or malicious scripts from pushing unauthorized command binaries to the PLCs. It addresses the physical execution of the attack vector.

5.2 The Absolute Operational Safety Argument: Option C (Environmental Hardening)

Why a team can successfully argue this is the true priority: This option honours the Inverted CIA Triad where physical safety and process availability trump everything else.

- A team choosing Option C can argue: "What good is a perfectly patched network (Option A) or a bulletproof firewall (Option B) if a simple power cut causes the controller room to overheat, turning off our Safety Instrumented System (SIS) and leaving us completely blind while a chemical pump fails?" * In a water facility feeding Dublin, preventing a catastrophic physical fail-deadly state (over-chlorination) during a power instability is the immediate life-safety priority.

5.3 The Flawed (But Common) Choice: Option A (Logical Boundary)

Why this is a trap choice (and why competing teams will attack it): Many students coming from a traditional IT background will instinctively choose Option A because Kerberos and Reverse Proxies are standard best practices.

- The counter-argument: While Option A prevents the initial ingress method (the contractor's stolen credentials), it does absolutely nothing to fix the flat internal network topology. If an attacker finds another way in (e.g., a rogue USB stick on the plant floor, or a different compromised device), they still have a completely open, unsegmented path to destroy the PLC logic.

This page is intentionally blank