# Laboratory #3.1

# ISA/IEC 62443 Risk Assessment


**Dr Diarmuid Ó Briain**

**Version: 1.0**

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

**Dr Diarmuid Ó Briain**

# Table of Contents



# Illustration Index

*This page is intentionally blank*

# Assessment of Location Alpha (U101) for WindPower Limited

## 1 Part 1 – Risk Assessment Briefing

### 1.1 Introduction

Location Alpha (U101) is a key component of the WindPower's electrical utility operations, responsible for generating and distributing electricity to homes and businesses across Ireland. This assessment will focus on evaluating U101's performance and identifying areas for improvement within the context of cybersecurity standards.

### 1.2 Scope

The scope of this assessment includes:

- **System Architecture**: Understanding the overall layout and interconnectivity of U101's power generation and distribution systems, including its connection to other power plants and distribution networks.
- **Asset Inventory Details**: Reviewing U101's asset management practices, including tracking of maintenance supplies, and spare parts.
- **Cybersecurity Practices**: Assess the cybersecurity practices in terms of the WindPower Limited security posture.

### 1.3 Assessment Objectives

The primary objectives of this assessment are to:

- Assess U101's overall cybersecurity efficiency and effectiveness compared to WindPower standards.
- Identify areas where U101's operations could be optimised to improve cybersecurity efficiency, reduce costs, and enhance reliability.
- Evaluate U101's asset management practices and make recommendations for improvement.

### 1.4 Assessment Methodology

Get the class to brainstorm assessment methodologies, how will the assessment be conducted?


5

The assessment will utilise a combination of methods, including:

- **Document review**: Thoroughly reviewing relevant documentation, including system architecture diagrams, inventory control procedures, and energy consumption reports.
- **Site visits**: Conducting site visits to U101 to gain a first-hand understanding of the plant's operations, infrastructure, and equipment.
- **Interviews**: Engaging with plant personnel, including engineers, operators, and maintenance staff, to gather insights and perspectives.

## 1.5 Expected Outcomes

Get the class to brainstorm on the outcomes that should come from the assessment?


5

The expected outcomes of this assessment include:

- A comprehensive report outlining U101's strengths and weaknesses compared to WindPower standards.
- Detailed recommendations for improving U101's cybersecurity efficiency, cost effectiveness, and reliability.
- Actionable insights to guide U101's decision-making and implementation of operational improvements.

# 2 General Observations post visit

Give the class the following observations from the assessment visit. Give a little time for them to discuss them.


5

## 2.1 Documentation

- The current asset inventory is incomplete and missing important information.
- Proper architecture and network diagrams are not available to reveal logical and physical network connections between assets.
- Interconnection between U101–U103 is not available.

## 2.2 Antivirus

- Most of endpoints have antivirus software.
- There is no central management for antivirus software.
- Stand-alone systems do not have antivirus software, but they have manual scanning procedures.

## 2.3 Backups

- Network connected computer-based systems are automatically backed up using Windows Server Backup (WSP).
- For Programmable Logic Controllers (PLC), there is a manual backup procedure.
- Most Human Machine Interfaces (HMI) panels do not have backup capabilities.

## 2.4 DCS and Safety systems:

- The Distributed Control System (DCS) network is not segregated from the safety network on each location.
- Same username and password is being used by all operators for using workstation
- Only one engineer know the process of resetting password if lost or expired.

## 2.5 Operating System Configuration:

- All Windows OS systems were hardened by the respective vendor guidelines, but there are no controls in place to verify if this is still the case.
- There is not hardening procedure, each vendor has done their own way.
- Logs are not enabled for applications and security.

## 2.6 Network Management

- Process engineer was using telnet to access network switches in Level 2.
- Network connecting PLC to HMI is single and routed using metal conduits and separate cable tray.
- Engineer sitting in U101 can take Remote Desktop Protocol (RDP) of workstation of U105 without any approval from U105, was editing log rotation of machine.

# 3 Assessment output

Get the class to write up their the observations in an assessment report template based on the Foundational Requirements (FR).

| FR | Requirement | Recommendation | Results | Score |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | Total | |
| | | | Score (Total/100X) | % |

*Figure 1: Example Foundational Requirements Assessment Sheet*

X = number of rows


15

| SR | Requirement | Recommendation | Results | Score |
|---|---|---|---|---|
| FR1 | Identification and Authentication | All human users shall be uniquely identified and authenticated. | Operators are sharing same user name and passwords | **40** |
| FR2 | Use Control | The control system should be set up to produce auditable events into the system log. | Logs are not enabled on the windows for application and security | **20** |
| FR3 | System Integrity | Communication integrity: Transmitted information should be protected. | Telnet is in use, so not compliant to communication integrity | **45** |
| FR4 | Data Confidentiality | Information like passwords should be secured and protected. | Passwords are shared and telnet also show password in plaintext | **60** |
| FR5 | Restricted Data Flow | Zone boundary protection should be enforced at zone boundaries. | Remote access is not configured or boundary protection is not implemented | **25** |
| FR6 | Timely response to events | The audit logs should (only) be accessible for authorised users from a read-only device. | Engineer was able to change log rotation from other unit. | **67** |
| FR7 | Resource Availability | The IACS should be set up so that up-to-date backups are available for full system recovery. | Some backups are not taken, so can be tough when full system recovery is required. | **56** |
| | | | Total | **313** |
| | | | Score (Total/700) | **44.7%** |

*Figure 2: Foundational Requirements Assessment Sheet*

*This page is intentionally blank*