AEGIS Case Study

Project title	Cybersecurity Risk Management
Date	April 2022

SCOPE/OBJECTIVE

The objective/purpose of the project is to define an ‘Operational Technology (OT) Cybersecurity’ policy for establishing guidelines for OT security and risk management process.
This policy is a brief outline of activities to be performed within an organisation for effective cybersecurity solutions.

TECHNOLOGY USED (IF APPLICABLE)

During this project, the state-of-the-art Information Technology (IT) policy, cybersecurity standards and code of practices such as ISO 27001, IEC 62443-3-2, CIS CSC20, TS 50701 and other Standards/guidelines were reviewed.

After analysing these best practices and existing IT security policies, a new revised cybersecurity management process was created for the risk analysis and assessment. This standardised process aims to recognise and assess the vulnerabilities that are leading to threats and risk according to the Technical Specification (TS) 50701. Also, a risk register has been developed as a tool for effective and efficient risk management.

HOW WE HELPED

The aim for OT cybersecurity policy is to define an implementation process for cybersecurity risk management. The cybersecurity risk assessment for fleets aims to ensure that data involved in the fleet operations is protected against the confidentiality, integrity, and availability point of view, and that the identified risks are well managed and mitigated. An assessment policy for cybersecurity risks is defined by considering as input the fleet/class generic architecture and the relevant assets.

For this purpose, the following activities are conducted:

- Evaluate the need for OT against the current digital architecture (fleets).
- A standardised process for recognition and assessment of vulnerabilities leading to threats and risks according to TS 50701 is defined.
- The architecture of fleets (digital trains) is understood to identify the risk factor (IT and OT).

Therefore, a detailed OT cybersecurity risk management policy derived from TS 50701 is devised.

OUTCOME

The policy was well-received by the Client.

Based on their positive feedback, a corresponding Fleet Engineer training programme has been designed to support them.
The training aims to raise the knowledge of the Fleet Engineers for managing the risk registers and identifying potential mitigation strategies for risks.
Also, a detailed risk assessment has been recommended to identify corresponding risk factor to the digital fleets, conduct vulnerability assessment for fleets based on scope and effect analysis, evaluate, and prioritize the risk, present an action plan for minimizing threats leading to risks, and monitor and review the plan/ policy.

AEGIS Certification Services
29 Brunel Parkway, Derby DE24 8HR
www.aegisengineering.co.uk
info@aegiscertification.co.uk
+44 (0) 1332 384 302