CPS PMA

Student ID or IDs for group work	2126529
Words	3517

Date set	03/02/2023
Submission date (excluding extensions)	06/03/2023 by 12:00pm (UK time)
Submission guidance	To be submitted electronically via Tabula
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	Cyberphysical Systems , WM089-15
Module owner	HS Lallie
Module tutor	HS Lallie
Module marker	HS Lallie
Assessment type	PMA
Weighting of mark	100%

Table of Contents

1. High Level Summary

Russia's large-scale cyber attack against the Ukrainian government has recently attracted much company attention. This cyber war targeted Ukraine's infrastructure, resulting in a large amount of data leakage and system failure, causing considerable losses to Ukraine. Therefore, implementing a comprehensive cybersecurity plan is essential to any business.

This report is tailor-made by ZKC Consulting for ACME Energy and provides solutions for cybersecurity strategies and plans for offshore wind farm with turbines, which covers five parts, including security architecture, security engineering, risk management, operational security, and data security.

First, we use the SABSA framework to provide the enterprise with a detailed system security architecture from a high to a low perspective and then provide the engineering team with an elaborate network security design diagram as a technical solution. Furthermore, we provide risk management process building and control measures assessment through risk management standards to mitigate potential threats related to cyber security threats. Finally, we provide data security solutions that comply with GDPR compliance to prevent significant losses caused by system damage for enterprises and greatly enhance the ability of enterprises to organise network security defences.

2. Security Architecture

In this section, we use the SABSA-based framework to give a detailed security architecture for ACME Energy based on its history and business needs[1].

2.1 Context Architecture

In this part, we will focus on how to transform business issues into high-level security requirements, and we will discuss them in the following three points:

- **Enabling offshore wind farm security:** Securing offshore wind farm with turbines is essential as it is the first line of defence for securing ACME Energy's data and systems. For example, if an offshore wind farm with turbines is attacked or damaged, it may damage or lose data and systems, affecting ACME Energy's business operations and causing a loss of interest for the company and investors. Therefore, securing an offshore wind farm with turbines is integral to protecting operations and interests while ensuring data and systems security.

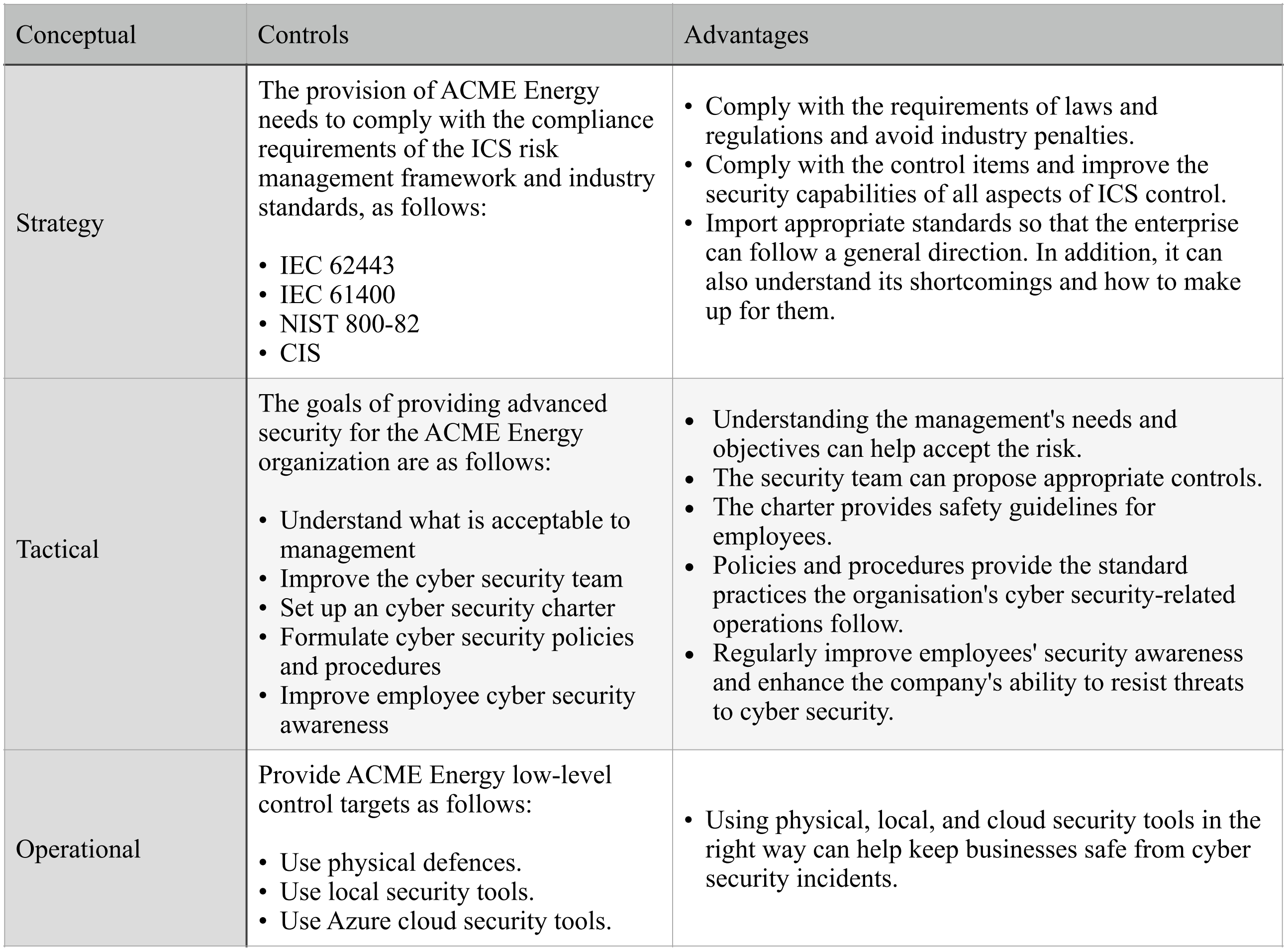
- **Achieving IT and OT system security:** IT and OT systems contain ACME Energy's core data, so protecting the system's safety is the key to realising the business benefits, mitigating security risks, and improving efficiency. For example, if the system is subject to any security incidents and threats, it will likely cause serious consequences such as business interruption, data damage or leakage, and loss of investor trust. Therefore, achieving the security of IT and OT systems is one of the necessary conditions for ACME Energy to conduct its business goals.

- **Realising the security of the public cloud environment:** Azure public cloud will serve as a platform for building an IT environment, so it is indispensable to protect the security of the Azure public cloud environment. For example, making sure that the Azure public cloud environment is secure protects ACME Energy's business operations and keeps security risks in check. Therefore, connecting to the Azure public cloud environment is an essential part of ACME Energy's plan to realise its plans, and it is also a necessary condition to ensure that its business and interests are protected.

2.2 Conceptual Architecture

In this part, we figure out what the most important security controls are and how they will improve security, as shown in FigureA.:

FigureA.



Conceptual	Controls	Advantages
Strategy	The provision of ACME Energy needs to comply with the compliance requirements of the ICS risk management framework and industry standards, as follows: • IEC 62443 • IEC 61400 • NIST 800-82 • CIS	• Comply with the requirements of laws and regulations and avoid industry penalties. • Comply with the control items and improve the security capabilities of all aspects of ICS control. • Import appropriate standards so that the enterprise can follow a general direction. In addition, it can also understand its shortcomings and how to make up for them.
Tactical	The goals of providing advanced security for the ACME Energy organization are as follows: • Understand what is acceptable to management • Improve the cyber security team • Set up an cyber security charter • Formulate cyber security policies and procedures • Improve employee cyber security awareness	• Understanding the management's needs and objectives can help accept the risk. • The security team can propose appropriate controls. • The charter provides safety guidelines for employees. • Policies and procedures provide the standard practices the organisation's cyber security-related operations follow. • Regularly improve employees' security awareness and enhance the company's ability to resist threats to cyber security.
Operational	Provide ACME Energy low-level control targets as follows: • Use physical defences. • Use local security tools. • Use Azure cloud security tools.	• Using physical, local, and cloud security tools in the right way can help keep businesses safe from cyber security incidents.

2.3 Logical Architecture

In this part, we have explained in detail how security controls will be implemented in risk management in part 4. We have recommendations for NIST 800-82 following ACME Energy, controls implementing IEC 62443.

3. Security Engineering

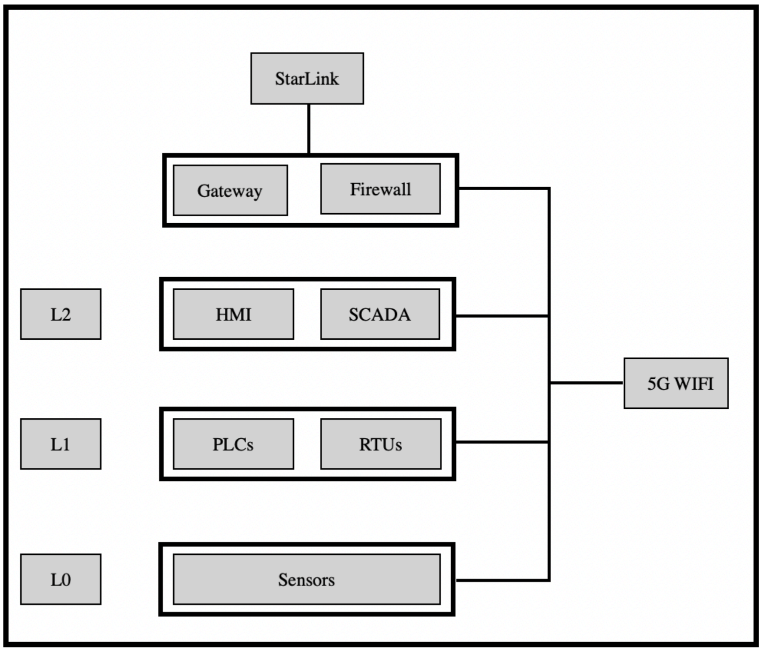
In this section, we provide a detailed low-cost ICS/SCADA local network and Azure cloud network solutions to provide ACME Energy a robust network architecture.

3.1 ICS/SCADA Local Network

In this part, we considers how to design a low-cost ICS/SCADA local network.

According to business requirements, we must create a 5G wireless mesh network to connect all wind turbines and send data to the Internet using Starlink satellite connections. In terms of design, we first connect OT equipment to the 5G network according to Purdue Architecture design and business requirements[2]. In addition, before we transmit data to Starlink or receive data from Starlink, we use Gateway and firewall for routing and security protection measures. We provides a high-level architecture diagram and a table of how to use low-level detailed design methods, as shown in FigureB. and FigureC..

FigureB.[2]



FigureC.

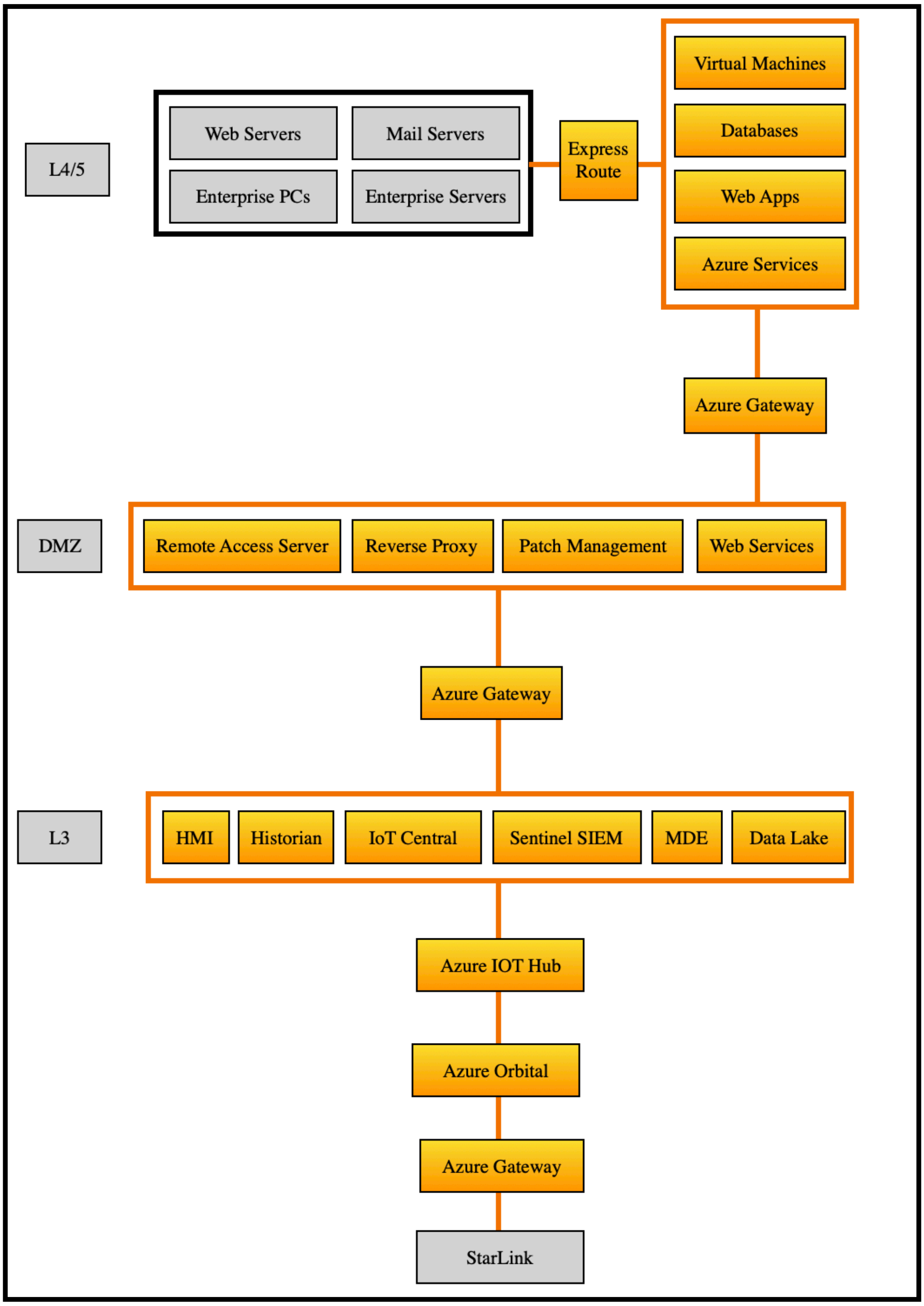
ICS/SCADA Local Network	Functions	Details
SCADA	Systems for monitoring and controlling industrial processes.	• Use open-source software: Open-source SCADA software, such as Eclipse SCADA, OpenSCADA, etc., can achieve data collection, monitoring and control, and control enterprise costs. • Transmission process: SCADA open-source software supports multiple communication protocols, such as Modbus, OPC UA, etc., allowing us to integrate different turbine OT devices and systems easily.

3.2 Azure Cloud Network

In this part, we consider how to transfer turbine data to the Azure cloud securely.

When Starlink transmits data to the Azure cloud, it must go through Azure Gateway, Azure Orbital, and Azure IOT Hub to achieve the purpose of data security transmission. We provides a high-level architecture diagram and a table of low-level detailed design methods[3], as shown in FigureD. and FigureE..

FigureD.[3]



FigureE.

Azure Cloud Network	Functions	Details
Azure IoT Hub	Collect turbine data and transmit data to the cloud.	• Communication protocol settings: Azure IoT Hub supports various communication protocols, including MQTT, AMQP, and HTTP, for data collection. • Data transmission: Azure IoT Hub supports two-way communication from device to the cloud and from cloud to machine, so we can safely collect data from turbines and send them to IoT Central and MDE.
Azure Orbital	Collect starlink information through Azure Orbital.	• Gateway Settings: Manage and control communications with satellites. • Terminal setting: After completing the Gateway setting, we connect the terminal to the OT device to process and filter the data. Furthermore, the filtered data is sent to Azure IOT Hub.
Azure Gateway	Route and protect starlink data.	• Gateway settings: Manage accessible network segments. • Firewall Rule Settings: Set firewall rules according to business needs to ensure security.

4. Risk Management

In this section, we provide risk management process recommendations and explain how related controls will mitigate potential risks associated with cybersecurity threats.

4.1 NIST 800-82 Implementation and Recommendations

As an organisation-level ACME Energy, the first thing managers face is formulating a security plan for establishing a secure ICS environment, and NIST 800-82 provides recommendations and guidelines[4]. The following are our recommendations for the current status of ACME Energy according to the level division in NIST 800-82:

High level:

- Confirm the conditions acceptable to the management: Based on the actual situation of ACME Energy's operations, understand what the administration cares about and what needs to be known, including the acceptable risk level, the scope of coverage, resource costs that need to be invested, etc.

Mid level:

- Determine the cyber security team: It is necessary to determine the cooperation relationship between the CIO and CISO of ACME Energy Group and the regional CIOs and CISOs of their respective countries, and the team members should at least include control, IT, cyber security and other professionals, to ensure adequate staffing for proper cyber security risk management.
- Define the Charter: The cyber security director should establish the charter of the cyber security plan to provide the guiding principles for ACME Energy's executives, including objectives, roles and responsibilities, execution scope, budget and resources, etc.
- Define policies and processes: Charter needs policies and processes to match, so ACME Energy needs to further define policies and implementation processes based on the charter's content. The cyber security supervisor should refer to the existing corporate process specifications to consider how to integrate and adjust the parts related to cyber security as a standard process for organising cyber security-related operations.
- Introduce ICS cyber security risk management framework set standards: Refer to relevant frameworks and standards for ICS risk management, carry out risk analysis and processing planning, and must be certified according to the ACME Energy needs.

Low level:

- Provide cyber security awareness training: In addition to defining handling measures through middle and high-level policy processes, the most important thing is to enhance the awareness of ACME Energy colleagues' cyber security. The best way to improve cyber security awareness is through education, training, and appropriate drills according to the company's needs.

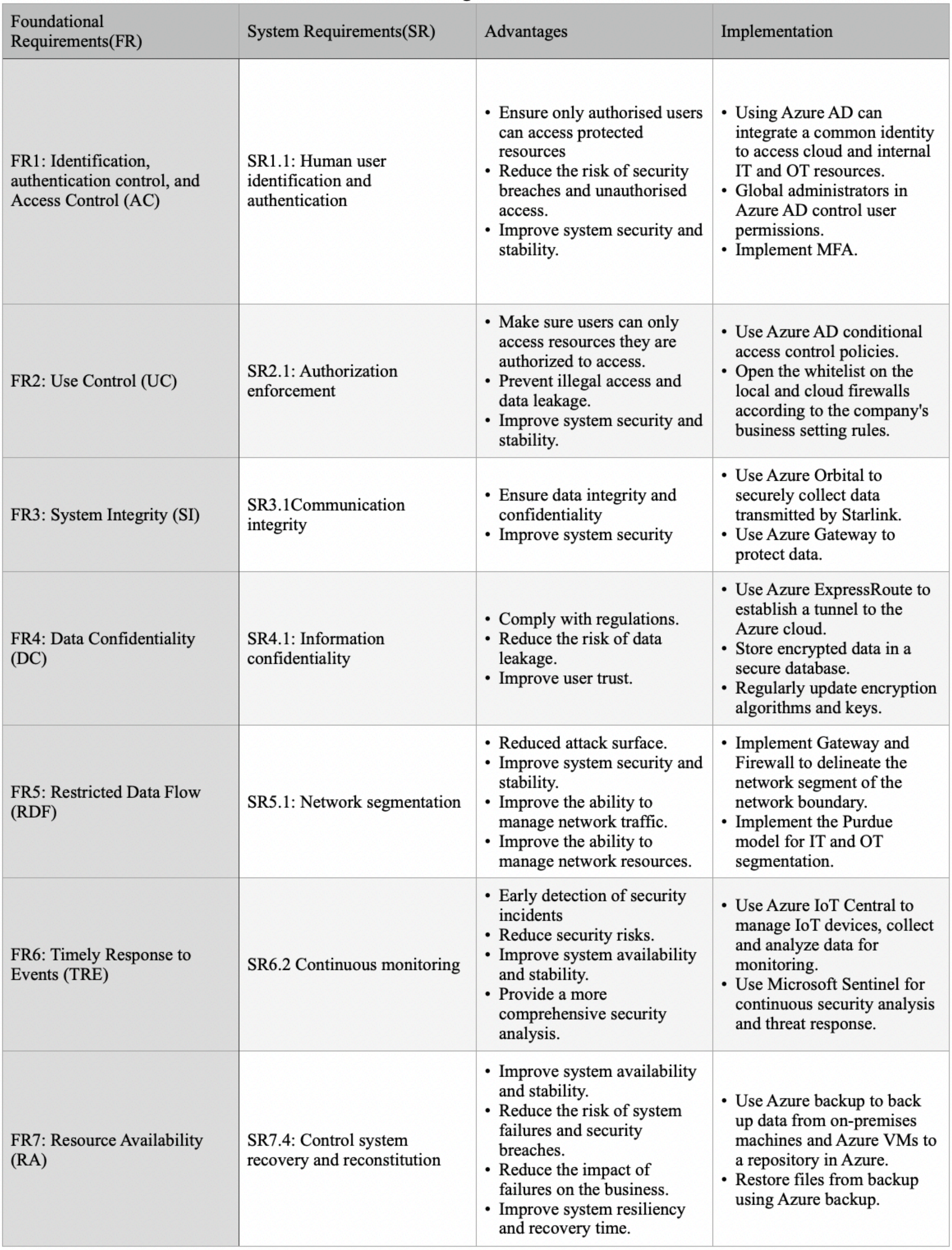
4.2 IEC 62443 Implementation and Recommendations

The security plan formulated by NIST 800-82 can assist ACME Energy in moving towards the safety of the ICS environment and effectively managing risks. The next step is to plan feasible technical solutions. We use IEC 62443 to illustrate how the requirements can be derived from regulators because IEC 62443 can be a suitable reference standard and is required by industry regulators. With IEC 62443, we can step by step from the design and planning of the ACME Energy wind farm with turbines architecture to the implementation of particular control items to ensure that the wind farm with turbines is free from the threat of cyber security attacks, as follows:

- **Architecture**: A reference model for ICS environment planning is proposed in IEC 62443-4-1, which is used to classify and understand the entire ICS network environment and can be used as a reference when planning a high-level security architecture[5]. Here we use Purdue Architecture, adopted by IEC62443 and used to describe the association, dependency and data flow of essential components in OT environment, and can also identify existing risks. The architecture of ACME Energy as shown in the figureB. and figureD..

- **Controls**: After completing the design of the architecture diagram, we will use IEC62443-3-3 to conduct a more specialised evaluation of the cyber security control level of the entire ICS we designed[6]. We propose a critical control in seven control areas and an explanation of how those controls will mitigate potential risks associated with cybersecurity threats, as shown in FigureF..

FigureF.[6]



Foundational Requirements(FR)	System Requirements(SR)	Advantages	Implementation
FR1: Identification, authentication control, and Access Control (AC)	SR1.1: Human user identification and authentication	• Ensure only authorised users can access protected resources • Reduce the risk of security breaches and unauthorised access. • Improve system security and stability.	• Using Azure AD can integrate a common identity to access cloud and internal IT and OT resources. • Global administrators in Azure AD control user permissions. • Implement MFA.
FR2: Use Control (UC)	SR2.1: Authorization enforcement	• Make sure users can only access resources they are authorized to access. • Prevent illegal access and data leakage. • Improve system security and stability.	• Use Azure AD conditional access control policies. • Open the whitelist on the local and cloud firewalls according to the company's business setting rules.
FR3: System Integrity (SI)	SR3.1Communication integrity	• Ensure data integrity and confidentiality • Improve system security	• Use Azure Orbital to securely collect data transmitted by Starlink. • Use Azure Gateway to protect data.
FR4: Data Confidentiality (DC)	SR4.1: Information confidentiality	• Comply with regulations. • Reduce the risk of data leakage. • Improve user trust.	• Use Azure ExpressRoute to establish a tunnel to the Azure cloud. • Store encrypted data in a secure database. • Regularly update encryption algorithms and keys.
FR5: Restricted Data Flow (RDF)	SR5.1: Network segmentation	• Reduced attack surface. • Improve system security and stability. • Improve the ability to manage network traffic. • Improve the ability to manage network resources.	• Implement Gateway and Firewall to delineate the network segment of the network boundary. • Implement the Purdue model for IT and OT segmentation.
FR6: Timely Response to Events (TRE)	SR6.2 Continuous monitoring	• Early detection of security incidents • Reduce security risks. • Improve system availability and stability. • Provide a more comprehensive security analysis.	• Use Azure IoT Central to manage IoT devices, collect and analyze data for monitoring. • Use Microsoft Sentinel for continuous security analysis and threat response.
FR7: Resource Availability (RA)	SR7.4: Control system recovery and reconstitution	• Improve system availability and stability. • Reduce the risk of system failures and security breaches. • Reduce the impact of failures on the business. • Improve system resiliency and recovery time.	• Use Azure backup to back up data from on-premises machines and Azure VMs to a repository in Azure. • Restore files from backup using Azure backup.

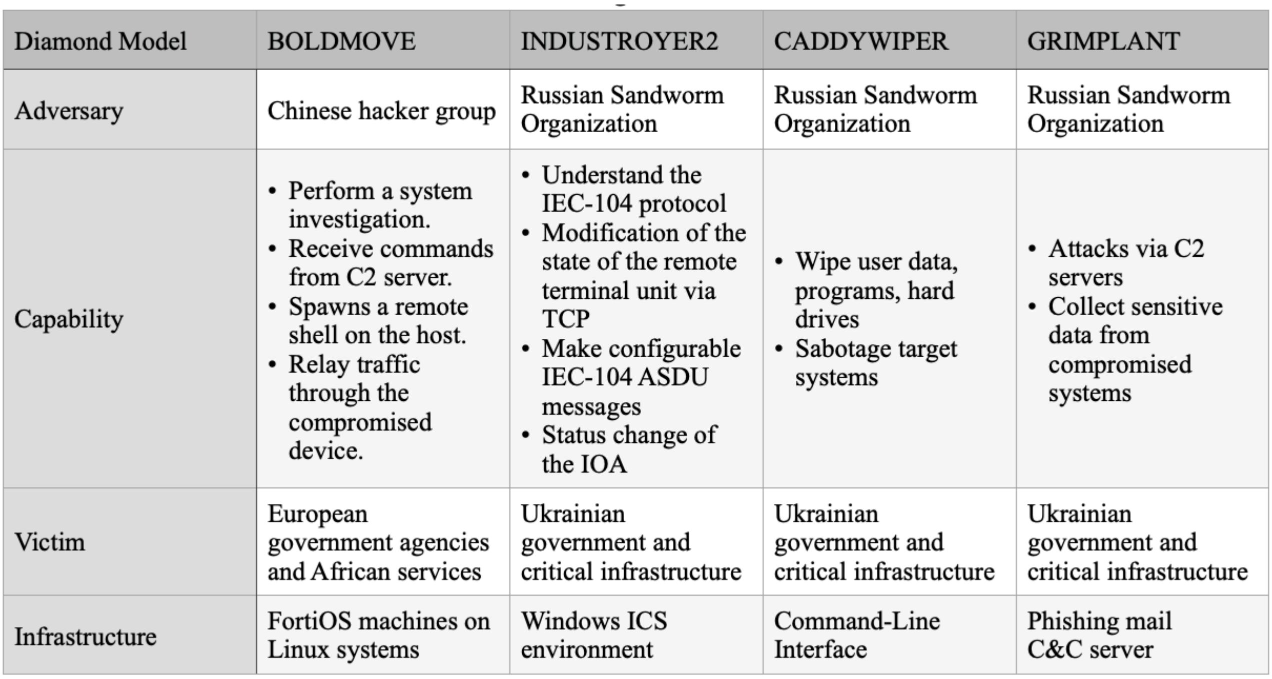
5. Operational Security

In this section, we provide a diamond model, threat intelligence summary and reports, security tools recommendations, SIEM playbook, and incident response plan for ACME energy to establish an operational security framework to increase security posture.

5.1 Diamond Model

In this part, we provide a diamond model to learn about the following four types of malware including Adversary, Capability, Victim, and Infrastructure, as shown in FigureG..

FigureG.



Diamond Model	BOLDMOVE	INDUSTROYER2	CADDYWIPER	GRIMPLANT
Adversary	Chinese hacker group	Russian Sandworm Organization	Russian Sandworm Organization	Russian Sandworm Organization
Capability	• Perform a system investigation. • Receive commands from C2 server. • Spawns a remote shell on the host. • Relay traffic through the compromised device.	• Understand the IEC-104 protocol • Modification of the state of the remote terminal unit via TCP • Make configurable IEC-104 ASDU messages • Status change of the IOA	• Wipe user data, programs, hard drives • Sabotage target systems	• Attacks via C2 servers • Collect sensitive data from compromised systems
Victim	European government agencies and African services	Ukrainian government and critical infrastructure	Ukrainian government and critical infrastructure	Ukrainian government and critical infrastructure
Infrastructure	FortiOS machines on Linux systems	Windows ICS environment	Command-Line Interface	Phishing mail C&C server

5.2 Threat Intelligence Summary and Report

In this part, we partnered with engineers from the ACME Energy Cyberthreat Intelligence team to provide an advanced threat intelligence summary and report of BOLDMOVE, INDUSTROYER2, CADDYWIPER, and GRIMPLANT malware, as shown in link:

Threat Intelligence Summary and Report:

- https://docs.google.com/document/d/1RbfQROpwWPbrX-P8zDDdajQyjxwQKfWyYJWi-Wq-rw4/edit?usp=sharing

5.3 Security Tools

In this part, we will provide advice from the vulnerability management sector on using Qualys for vulnerability management of IT and OT networks and SonarQube for software testing.

Qualys is an automated vulnerability scanning tool that automatically scans for vulnerabilities and implements a vulnerability management program across ACME Energy's IT and OT networks to discover and patch vulnerabilities in the network, improving network security. The following provides recommendations for vulnerability management with Qualys:

- Setting up Qualys: We needed to ensure that Qualys had correctly set up ACME Energy's network topology and access IT and OT equipment properly.
- Start Scan: We can choose to scan our network automatically and manually.
- Analysis results: Qualys provides vulnerability and threat classifications to help us assess the severity of the vulnerability.
- Vulnerability handling: Vulnerabilities are handled according to the severity and business considerations based on vulnerability analysis results.
- Monitor progress: Use the progress reports provided by Qualys to determine the security of our IT and OT networks continuously.

SonarQube is an open-source platform for software testing and code analysis that provides ACME Energy with detailed information on code quality and detects bugs and vulnerabilities in code to improve the security and performance of our applications. The following provides recommendations for software testing with SonarQube:

- Setting up the repository: This is done using the repository's webhook or Jenkins plugin.
- Create a project: Complete by setting the project name and code base path.
- Start analysis: By running a Maven or Gradle build script.
- Analysis complete: View details about code quality in SonarQube.
- Problem-Solving: Based on the analysis results, address and resolve issues based on ACME Energy business considerations.

With the above operation suggestions, we can better conduct vulnerability management and security scanning for ACME Energy to reduce security risks.

5.4 Sentinel SIEM Playbook

In this part, we provide a detailed description of the Sentinel SIEM deployment process as part of creating a playbook:

- Develop alert rules: Alert rules can be configured based on event type, source, destination, protocol, and other conditions to detect threats.
- Vulnerability management: The vulnerability management process includes steps such as vulnerability scanning, vulnerability assessment, vulnerability patching, and vulnerability management reporting to ensure that vulnerabilities in the system are discovered and repaired in time to reduce the risk of being attacked.
- Implement log analysis: The log analysis process includes steps such as log collection, log analysis, event analysis, and reporting to ensure we identify and investigate events and respond to threats faster.
- Define automated processes: Establish computerised processes to detect incidents, investigate incidents, and respond to threats faster to mitigate risk and increase efficiency.

The above Sentinel SIEM playbook can help us better manage and secure ACME Energy's IT and OT environment and mitigate security risks.

5.5 Incident Response Plan

In this part, we refer to NIST SP800-61 to provide ACME Energy with the four phases of a high-level cyber security incident response plan so that it can quickly and effectively respond and deal with security incidents when they occur[7]. The following are the main steps of this plan:

Preparation:

- Identify Response Teams: Identify Group CIOs and CISOs working in partnership with regional CIOs and CISOs in their respective countries, as well as internal security personnel within the company, to ensure an entire response team is in place to address security incidents and threats.
- Define responsibilities and authorities: Response team members must have clear responsibilities and rules to ensure effective collaboration and decision-making.
- Prepare relevant tools and resources: Prepare necessary tools and resources, such as storage devices, log management systems, event monitoring systems, etc.

Detection and Analysis:

- Monitoring IT and OT systems of wind farm with turbines: Monitor IT and OT systems of wind farm with turbines using monitoring systems to detect and identify any unusual activities and threats.
- Assess the severity and impact of security incidents and threats: Detected security incidents and threats are assessed to determine their severity and impact to determine countermeasures and priorities.

Containment, Eradication, and Recovery:

- Implement response measures: Implement immediate response measures to network incidents, such as cutting off network connections, collecting evidence, etc.
- Recover affected systems and data: Recover affected systems and data, and restart systems and applications.

Post-incident Activity:

- Notify relevant personnel: Notify appropriate personnel, such as response team members, PR departments, legal departments, etc.
- Logging and Reporting: Log and report security incidents and responses for review and analysis.

The above is ACME Energy's high-level response plan, which helps enterprises respond to security incidents and threats quickly and effectively but also protects the assets and interests of enterprises. Additionally, ACME Energy must continually update and upgrade its response plan to address ever-changing security threats and attacks.

6. Data Security

In this section, we will explain how to protect data at rest in the on-premises ICS/SCADA network, Azure network, and data in transit for GDPR compliance[8].

6.1 Administrative Measures

In this part, according to the GDPR, ACME Energy following administrative measures are recommended:

- Data Transparency: ACME Energy must inform customers how and for what purpose data is processed.
- Right to Data Forgotten: When a customer raises this right with ACME Energy, the customer's data must be deleted from the system.
- Right to Data Portability: ACME Energy must enable the secure movement of customer data between IT environments without compromising data availability.
- Data Confidentiality: ACME Energy must protect customer and company data confidentiality and prevent data from being accessed or used by unauthorised third parties.
- Data penetration notification: If ACME Energy is attacked by a cyber security incident that affects data leakage, the company must notify the competent authority within 72 hours.

6.2 Technical Measures

In this part, according to the GDPR, the following suggestions are provided for technical protection measures at the ACME Energy Operational level, as shown in FigureH..

FigureH.

Data state	Technical protection measures
Data at rest in the local ICS/SCADA network	• Use data encryption technology to encrypt data at rest. • Regularly update encryption algorithms and keys. • Use open source SCADA software for security monitoring. • Use the Purdue model for IT and OT segmentation. • Implement Gateway and Firewall to delineate the network segment of the network boundary.
Data at rest in the Azure network	• Global administrators in Azure AD control user permissions. • Use Azure AD conditional access control policies. • Use data encryption technology to encrypt data in rest • Regularly update encryption algorithms and keys. • Use the Purdue model for IT and OT segmentation. • Using Azure AD can integrate a common identity to access cloud and internal IT and OT resources. • Use Azure IoT Central to manage IoT devices for monitoring. • Implement the Purdue model for IT and OT segmentation. • Implement Gateway and Firewall to delineate the network segment of the network boundary.

Data state	Technical protection measures
Data in transit	• Use encryption algorithm to encrypt data in transmission. • Use Azure ExpressRoute to establish a tunnel to the Azure cloud. • Use open source SCADA software for security monitoring. • Use the Purdue model for IT and OT segmentation. • Open the whitelist on the local and cloud firewalls according to the company's business setting rules. • Use Azure Gateway to protect the transmitted data. • Use Azure Orbital to securely collect data transmitted by Starlink. • Use Azure IoT Central to manage IoT devices, collect and analyse data for monitoring. • Continuous Security Analysis with Microsoft Sentinel.

7. Conclusion

In summary, ZKC Consulting conducts comprehensive network security considerations and proposes appropriate solutions for ACME Energy's five significant aspects of offshore wind farm with turbines, including security architecture, security engineering, risk management, operational security, and data security. Based on the SABSA framework, network security design diagram, NIST 800-82 and IEC 62443 risk management measures, threat detection and response, and GDPR compliance, we provide suitable solutions and suggestions for high-level and middle-level and low-level personnel in the enterprise. ACME Energy can prevent significant losses caused by future threats and improve ability to organise network security defences.

8. Reference

[1]. SABSA Institute. (2022) SABSA framework. Available from: https://sabsa.org/sabsa-executive-summary/

[2]. Zscaler Inc. (2023) Purdue Model. Available from: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

[3]. Sameera Perera (2022) Extending Operational Technology to Azure. Available from: https://techcommunity.microsoft.com/t5/azure-infrastructure-blog/extending-operational-technology-to-azure/ba-p/3265466

[4]. NIST. (2015) Guide to Industrial Control Systems (ICS) Security. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[5]. ISO/IEC. (2018) ISO/IEC 62443-4-1. Available from: https://webstore.iec.ch/preview/info_iec62443-4-1%7Bed1.0%7Den.pdf

[6]. ISO/IEC. (2013) ISO/IEC 62443-3-3. Available from: https://webstore.iec.ch/preview/info_iec62443-3-3%7Bed1.0%7Db.pdf

[7]. NIST. (2008) Computer Security Incident Handling Guide. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61r1.pdf

[8]. The European Parliament And The Council Of The European Union. (2016) GDPR. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679