Comprehensive risk assessment based on 62443 reports for DCS, PLC and Control network

Engineer Name: Funke Karole

Risk Assessment Report

Version 0.1

Table of Contents

[1. Introduction 2](#_Toc175004291)

[2. Purpose 3](#_Toc175004292)

[3. Scope of this risk assessment 3](#_Toc175004293)

[1. **Asset Inventory and Classification** 3](#_Toc175004294)

[**2.** **Vulnerability Identification:** 3](#_Toc175004295)

[**3.** **Threat Analysis:** 3](#_Toc175004296)

[**4.** **Risk Evaluation:** 3](#_Toc175004297)

[**5.** **Mitigation Strategies:** 3](#_Toc175004298)

[4. Risk Assessment Approach 3](#_Toc175004299)

[5. Risk Identification 5](#_Toc175004300)

[6. Risk Analysis and Evaluation 6](#_Toc175004301)

[7. Risk Treatment and Mitigation 6](#_Toc175004302)

[8. Residual Risk and SL-T (Security Level Target) Determination 6](#_Toc175004303)

[9. Conclusions 7](#_Toc175004304)

[10. Appendices 7](#_Toc175004305)

**RISK ASSESSMENT REPORT**

# Introduction

This report provides a concise risk assessment of the assets mentioned below in table below, a key component within the Industrial Control System (ICS) at Your Organization/XYZ Plant Name]. Following the IEC 62443 standard, the assessment identifies vulnerabilities, evaluates potential threats, and suggests mitigation strategies to enhance the server's security.

Given the critical role of this server in the overall ICS architecture, securing it against cyber threats is essential to maintaining operational safety and reliability. The report covers asset classification, vulnerability analysis, risk evaluation, and recommended actions, offering a clear path to strengthen the server's defense and ensure the integrity of the entire system.

|  |  |  |
| --- | --- | --- |
| **Level** | **Asset** | **Description** |
| Level 4 | Work Laptops | Used by enterprise users for accessing various applications. |
| Level 4 | Enterprise Desktops | Desktop computers for enterprise users. |
| Level 4 | Business Server | Server hosting business-critical applications. |
| Level 4 | Domain Controller | Manages user authentication and domain resources. |
| Level 4 | Webservers | Internet-facing servers hosting web applications. |
| Level 4 | Scheduling | System for managing schedules and tasks. |
| Level 4 | IP Cam | Internet Protocol camera for surveillance. |
| Level 3.5 | Enterprise AD Replica | Replica of the Active Directory for redundancy. |
| Level 3.5 | Patch Management Server | Manages the deployment of patches and updates. |
| Level 3.5 | Remote Access Server | Facilitates remote access to the network. |
| Level 3 | Historian | Collects and stores historical process data. |
| Level 3 | Database Server (DB Server) | Stores data for various applications. |
| Level 3 | Domain Controller | Manages user authentication within the control system. |
| Level 3 | Application Server | Hosts various applications critical to ICS operations. |
| Level 3 | EWS-1, EWS-2 | Engineering workstations used for control system configuration and monitoring. |
| Level 2 | SCADA | Supervisory Control and Data Acquisition system servers. |
| Level 2 | HMI-1, HMI-2 | Human-Machine Interface for operators to monitor and control processes. |
| Level 2 | Historian-1 | Additional historian server for redundancy. |
| Level 1 | PLCs | Programmable Logic Controllers managing process control. |
| Level 1 | Process Controller | Controls and monitors physical processes. |
| Level 1 | RTU-1, RTU-2 | Remote Terminal Units collecting data from remote locations. |
| Level 1 | Network Switches (SW-1, SW-2) | Network switches facilitating communication between devices. |
| Level 0 | Sensors | Devices measuring physical properties (temperature, pressure, etc.). |
| Level 0 | Actuators | Devices that control physical mechanisms based on controller signals. |
| Level 0 | UPS | Uninterruptible Power Supply ensuring power stability. |

# Purpose

The purpose of this risk assessment is to evaluate the cybersecurity posture of the ICS architecture at [Company Name], with a focus on identifying vulnerabilities and potential threats that could compromise the system's integrity, availability, and confidentiality. This assessment follows the IEC 62443 standard, providing a structured approach to assessing and mitigating risks across various levels of the ICS.

# Scope of this risk assessment

The scope of this risk assessment is focused on evaluating the security posture of the various components within the provided Industrial Control System (ICS) architecture. This assessment will cover the following key areas:

1. **Asset Inventory and Classification**:

* Identification of all assets within the ICS architecture, including hardware, software, network devices, and data flows across different levels.
* Classification of assets based on their criticality and role within the ICS environment.

1. **Vulnerability Identification:**

* Analysis of potential vulnerabilities in servers, workstations, controllers, and network devices at each level of the architecture.
* Identification of weaknesses related to software versions, configurations, network segmentation, and physical security.

1. **Threat Analysis:**

* Evaluation of potential threats that could target the identified vulnerabilities, including external threats (e.g., cyber-attacks, unauthorized access) and internal threats (e.g., insider misuse, equipment failure).

1. **Risk Evaluation:**

* Assessment of the likelihood and impact of each threat exploiting the identified vulnerabilities, using the IEC 62443 framework.
* Prioritization of risks based on their potential impact on the ICS operations.

1. **Mitigation Strategies:**

* Development of mitigation measures to address identified risks, including technical controls (e.g., firewalls, access controls), administrative controls (e.g., policies, procedures), and physical controls (e.g., access restrictions).

This assessment covers all levels of the ICS architecture, from Level 0 (field devices) to Level 4 (enterprise network). The assessment aims to provide a comprehensive view of the security posture of the ICS and to recommend actionable measures to enhance its resilience against potential cyber threats.

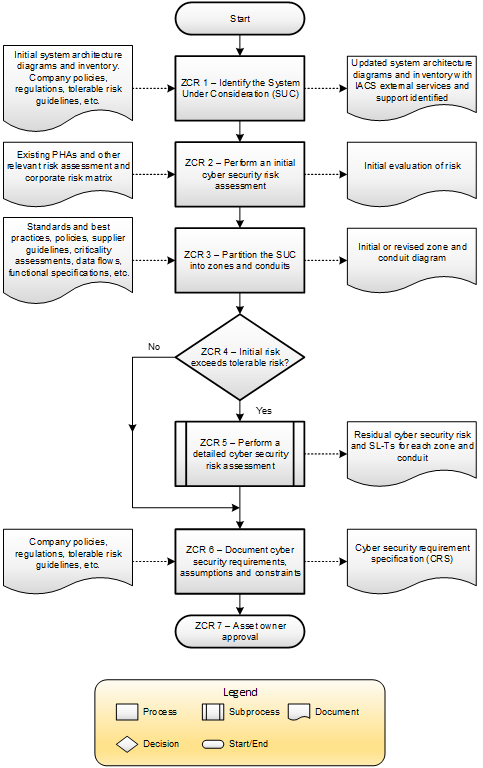
# Risk Assessment Approach

The risk assessment methodology employed includes asset identification, vulnerability assessment, threat analysis, and risk evaluation using a risk matrix. Each risk was evaluated based on its severity, likelihood, and potential impact on the ICS environment. The IEC 62443 standard guided the assessment process, ensuring that risks were prioritized and treated according to industry best practices.

The table below represents the participants along with their roles:

|  |  |  |
| --- | --- | --- |
| **Participant Role** | **Responsibilities** | **Typical Title** |
| Risk Assessment Leader (Facilitator) | Oversees the entire risk assessment process, ensures adherence to standards, coordinates participants. | Cybersecurity Manager, Risk Assessment Lead |
| ICS/SCADA Engineer | Provides detailed knowledge of ICS and SCADA systems, architecture, and technical details. | ICS Engineer, SCADA Engineer, Control Systems Engineer |
| Cybersecurity Specialist | Identifies and mitigates cybersecurity threats specific to industrial environments. | Cybersecurity Analyst, Cybersecurity Engineer |
| Network Engineer | Analyzes network architecture, segmentation, data flow, and communication protocols. | Network Engineer, Network Architect |
| System Administrator | Manages servers, workstations, and IT infrastructure; identifies software vulnerabilities. | IT System Administrator, IT Infrastructure Manager |
| Safety Engineer | Ensures safety implications of risks are considered, particularly in relation to physical processes. | Safety Engineer, Process Safety Manager |
| Operations Manager | Provides insight into day-to-day plant operations and how risks might impact efficiency and safety. | Operations Manager, Plant Manager |
| Compliance Officer | Ensures compliance with relevant regulations, industry standards, and company policies. | Compliance Officer, Regulatory Affairs Manager |
| Asset Owner | Has overall responsibility for the ICS environment; reviews and approves risk assessment findings. | Asset Owner, Plant Owner |
| External Vendor/Consultant (if applicable) | Provides specialized expertise or external perspective on the risk assessment. | External Consultant, Third-Party Vendor |
| Human Resources Representative (if applicable) | Provides input on insider threats, employee-related vulnerabilities, and human factors in cybersecurity. | HR Manager, Insider Threat Analyst |
| Legal Advisor (if applicable) | Offers guidance on legal implications of risk assessment findings, particularly data protection and liability. | Legal Counsel, Legal Advisor |

This risk assessment follows a systematic process designed to ensure a thorough evaluation of the Industrial Automation and Control System (IACS) architecture, aligned with the IEC 62443 standard.



# Risk Identification

The risk identification process revealed several critical vulnerabilities across the ICS architecture:

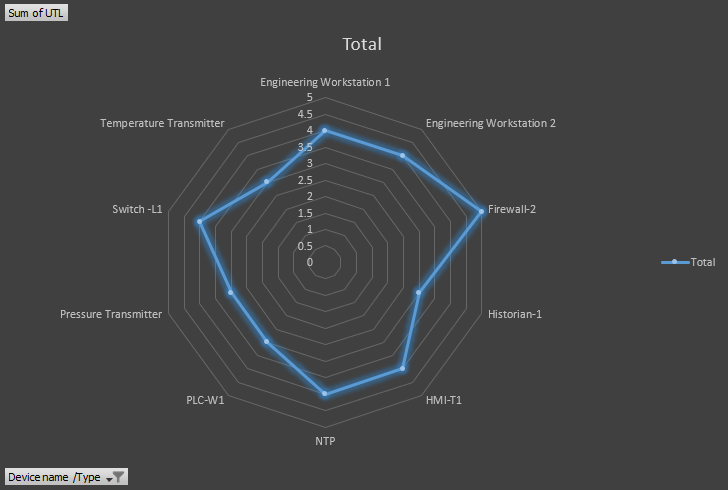
* **Level 0:** Configurable sensors (Pressure and Temperature Transmitters) are susceptible to tampering due to inadequate physical security controls.
* **Level 1:** PLCs and Network Switches are vulnerable to unauthorized access and exploitation due to weak access controls and outdated firmware.
* **Level 2:** RTUs and HMIs are at risk of unauthorized access through brute force attacks and inadequate logging mechanisms.
* **Level 3:** Engineering Workstations are highly vulnerable due to outdated operating systems, making them prime targets for remote code execution and privilege escalation.
* **Level 4:** Business-critical servers, including Domain Controllers, are at risk from malware and unauthorized access due to weak password policies and insufficient monitoring.

# Risk Analysis and Evaluation

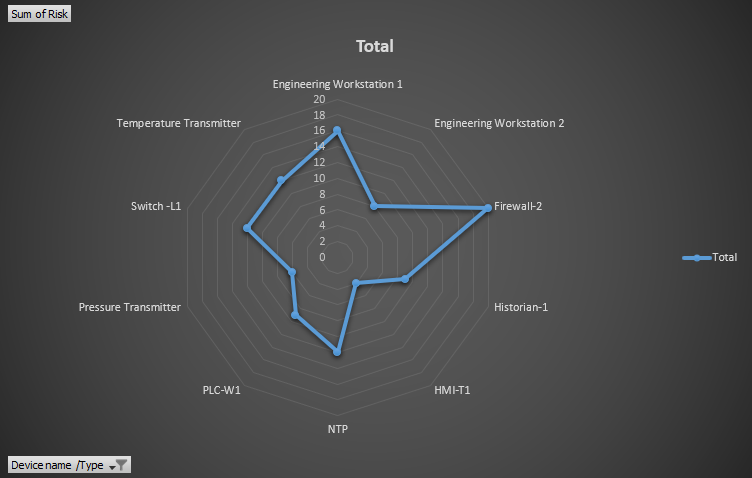
Each identified risk was analysed based on the severity of its impact and the likelihood of its occurrence. The analysis was conducted using a risk matrix, which categorized risks into different levels, ranging from low to critical:

* **High-Risk Areas:**
  + **Level 3 Engineering Workstations:** Classified as high risk due to the outdated OS, which presents a significant vulnerability for system takeover and data breaches.
  + **Level 1 Network Switch:** Identified as a high risk because of its susceptibility to unauthorized access, which could lead to system compromise and loss of control.
* **Medium-Risk Areas:**
  + **Level 2 HMIs and Historians:** These components are vulnerable to data tampering and unauthorized access but with a moderate likelihood of exploitation.
* **Low-Risk Areas:**
  + **Level 0 Sensors:** While tampering is a concern, the likelihood of physical access is lower, making this lower priority for immediate action.

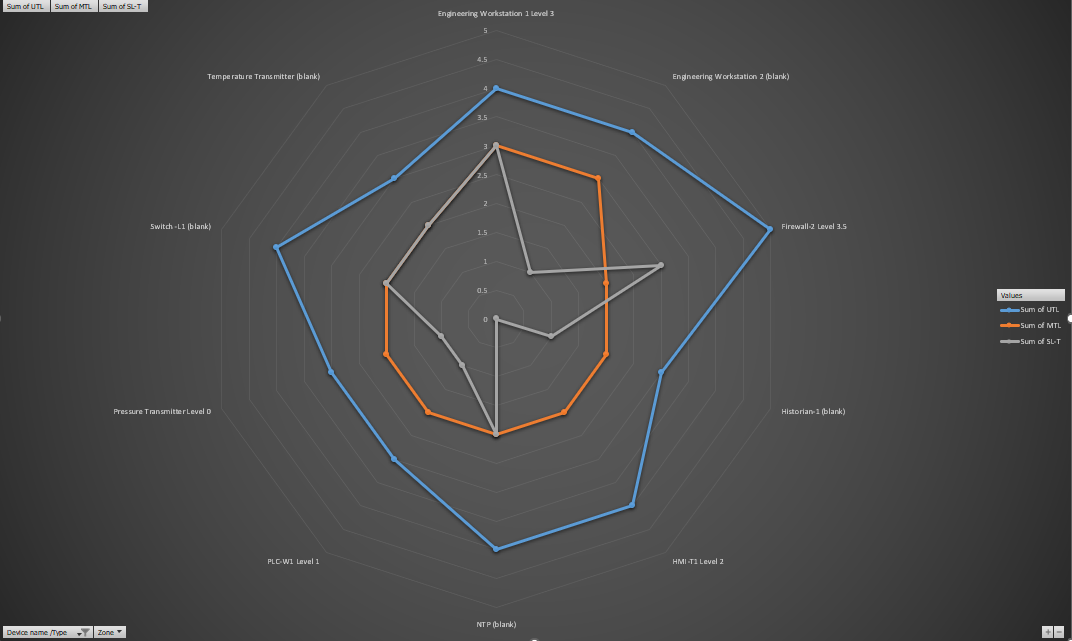
**Unmitigated Threat Likelihood of Assets**



**Risk Score for the Assets**



**Consolidated view of UTL, MTL and SL-T**



# Risk Treatment and Mitigation

The following mitigation strategies are recommended to address the identified risks:

* **Level 3 Engineering Workstations:** Implement immediate OS updates, disable unnecessary services (such as RDP), and enforce strict access controls.
* **Level 1 Network Switch:** Upgrade to managed switches with strong access controls, apply firmware updates, and monitor for unauthorized access attempts.
* **Level 2 HMIs and Historians:** Secure data with encryption, implement rigorous data integrity checks, and configure audit logging to detect unauthorized access.

# Residual Risk and SL-T (Security Level Target) Determination

After implementing the recommended mitigation strategies, the residual risks were evaluated to ensure they meet the acceptable Security Level Targets (SL-Ts). The residual risk for the engineering workstations at Level 3, while reduced, requires ongoing monitoring due to its critical role in system operations. All other mitigations have brought the risks within acceptable levels according to the defined SL-Ts.

### 9. Conclusions

This risk assessment has identified key vulnerabilities within the ICS architecture and provided targeted recommendations for mitigating these risks. The implementation of these measures will significantly enhance the security posture of the ICS. However, continuous monitoring and regular reassessment are essential to maintain a robust defense against evolving cyber threats.

Action items, Timeline, RACI Matrix, Budgeting, Project Management, Next Risk Assessment , Lessons learnt

### 10. Appendices

* **Appendix A:** Detailed risk matrix used in the assessment.
* **Appendix B:** Full system architecture diagrams.
* **Appendix C:** Relevant IEC 62443 standard references and guidelines.