# GridLink Utilities

## Operational Technology Gap Assessment

**28th September 2024**

Prepared by,
Aurnob Jahin Islam
Brampton, ON

# Executive Summary

This report presents findings from an Operational Technology (OT) Gap Assessment of GridLink's OT environment. The assessment was conducted over the last 3 months and included the following goals:

- Conducting a comprehensive assessment of GridLink's current OT environment an existing security measure.
- Identifying security gaps within GridLink's OT environment.
- Mapping GridLink's OT network to the Purdue Model for improved network understanding and segmentation.
- Providing recommendations to mitigate identified security gaps and enhance GridLink's overall OT security posture.
- Prioritizing the identified gaps based on their risk level.
- Proposing an implementation roadmap with estimated timelines and resources needed to address the gaps effectively.

A workshop was held with key stakeholders from GridLink's OT and IT departments, where 6 critical security gaps were identified. These gaps were evaluated based on their potential impact and likelihood of exploitation.

| Critical Risk | High Risk | Medium Risk | Low Risk |
|---|---|---|---|
| 1 | 3 | 2 | |

The following is a high-level summary of the gaps that were identified:

- A critical risk gap related to legacy systems running unsupported Windows 2012 servers, particularly in the Distribution Management System (DMS), creating exposure to known vulnerabilities.
- A high-risk gap related to not having multi-factor authentication (MFA) enabled for the VPN appliances used by operators to access OT workstations remotely, increasing the likelihood of unauthorized access.
- A high-risk gap related to insufficient network segmentation within the OT environment, as systems like the Distribution Management System (DMS) and Outage Management System (OMS) are not adequately isolated.
- A high-risk gap related to not hardening OT workstations in Transformers and Distribution stations, which leave critical network infrastructure vulnerable to attacks.
- A medium risk gap related to incomplete security monitoring due to lack of log collection from OT equipment located in Transformer and Distribution stations, resulting gaps in security visibility ad incident detection.
- A medium risk gap related to incomplete Firewall upgrades in key areas of the network, resulting in poor defense of the overall network.

Identified gaps have been prioritized and a suggested implementation roadmap has been included.

# Current State Analysis

## System Overview

GridLink is a utility company that operates the transmission and distribution of electricity across two-medium sized cities and surrounding areas. To manage these operations, GridLink utilizes two control centers; a primacy control center and a backup control center, located 30 minutes apart. These centers oversee the management of 10 transformer stations and 50 distributions stations, ensuring the delivery of electricity to customers in two large cities and nearby regions.

GridLink operates an Operational Technology (OT) network responsible for managing the physical processes that keep the electrical grid running. To maintain security, the OT network is segregated from the corporate IT network by a firewall, with a DMZ used to securely exchange data between the two networks. The organization leverages a Wide Area Network (WAN) to connect the control centers to their transformers and distribution stations.

The OT operations team manages approximately 250 Windows servers, and 75 Linux servers distributed between the primary and backup control centers. Each station houses one or two workstations dedicated to managing OT devices deployed at those locations.

GridLink employes a series of critical applications to ensure smooth operations and service delivery:

- The DMS (Distribution management system) is responsible for ensuring efficient and reliable power distribution to end customers.
- The EMS (Energy management system) monitors, controls, and optimizes the performance of the transmission network to maintain grid stability.
- The OMS (Outage management system) is designed to notify customers of outages via automated phone calls, SMS messages and a mobile application, ensuring prompt communication and customer satisfaction.

## Existing Security Measures

GridLink has implemented a range of security measures to ensure the protection of its operational technology (OT) and information technology (IT) networks, To maintain the separation between these networks, GridLink uses a DMZ (demilitarized zone) and NGFW (next generation firewalls), which regulate traffic flow between the OT and IT networks, Additionally, intrusion detection systems (IDS) have been deployed within the OT network to monitor traffic and detect potential threats.

GridLink is in the process of upgrading legacy firewalls at its stations, with about half of the stations having already transitioned to NGFWs (next generation firewalls) with built in IDS capabilities. Firewalls have been deployed across all stations to further restrict traffic, while ACLs (Access Control Lists) on routers manage incoming and outgoing traffic at each station.

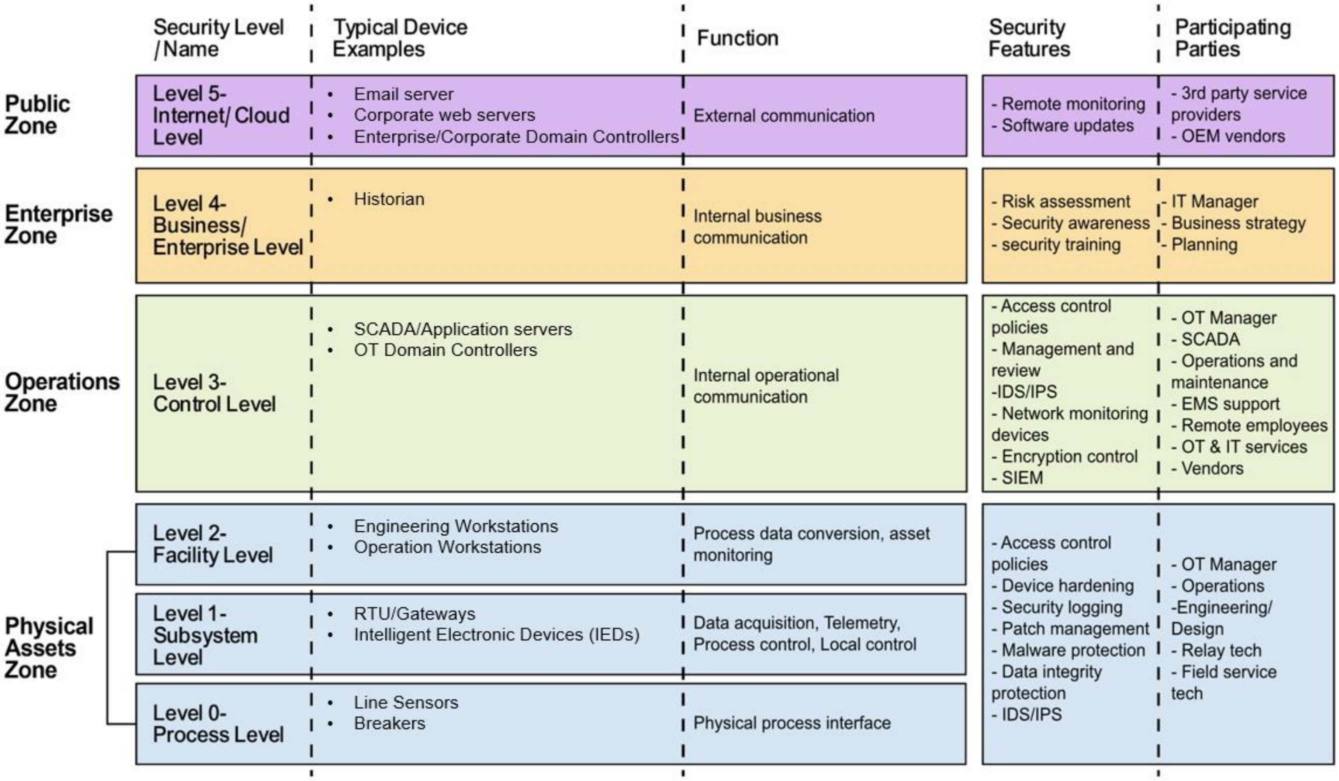
To limit Internet exposure, proxy servers are used to regulate which OT systems can connect to specific vendor websites to download critical update files, such as security patches. Internet access is not permitted from transformer and distribution stations downstream from the control centres, enhancing security at these remote locations.

Remote access is carefully controlled using VPNs for employees and vendors who need to access the OT network remotely. Jump servers are used as a secure bridge between the IT and OT networks, ensuring that access to critical systems is tightly regulated.

In terms of vulnerability and patch management, GridLink follows a strict schedule. Patches for the OT environment is applied monthly using an automated patch deployment platform. Updates to key applications like the DMS (Distribution management system) and the EMS (Energy management system) are performed quarterly to ensure system stability and security.

Lastly, AV (Antivirus Software) is installed on all OT workstations including those in the control centres and stations, as well as on the Windows and Linux servers housed in the control centres, providing an additional layer of defence against malware

## Mapping of GridLink's Network to the Purdue Model



| | Security Level /Name | Typical Device Examples | Function | Security Features | Participating Parties |
|---|---|---|---|---|---|
| Public Zone | Level 5- Internet/ Cloud Level | • Email server<br>• Corporate web servers<br>• Enterprise/Corporate Domain Controllers | External communication | - Remote monitoring<br>- Software updates | - 3rd party service providers<br>- OEM vendors |
| Enterprise Zone | Level 4- Business/ Enterprise Level | • Historian | Internal business communication | - Risk assessment<br>- Security awareness<br>- security training | - IT Manager<br>- Business strategy<br>- Planning |
| Operations Zone | Level 3- Control Level | • SCADA/Application servers<br>• OT Domain Controllers | Internal operational communication | - Access control policies<br>- Management and review<br>-IDS/IPS<br>- Network monitoring devices<br>- Encryption control<br>- SIEM | - OT Manager<br>- SCADA<br>- Operations and maintenance<br>- EMS support<br>- Remote employees<br>- OT & IT services<br>- Vendors |
| Physical Assets Zone | Level 2- Facility Level | • Engineering Workstations<br>• Operation Workstations | Process data conversion, asset monitoring | - Access control policies<br>- Device hardening<br>- Security logging<br>- Patch management<br>- Malware protection<br>- Data integrity protection<br>- IDS/IPS | - OT Manager<br>- Operations<br>-Engineering/ Design<br>- Relay tech<br>- Field service tech |
| | Level 1- Subsystem Level | • RTU/Gateways<br>• Intelligent Electronic Devices (IEDs) | Data acquisition, Telemetry, Process control, Local control | | |
| | Level 0- Process Level | • Line Sensors<br>• Breakers | Physical process interface | | |

# Gap Analysis

## C-01: Unpatched Legacy Systems (Windows 2012)

| **Critical** | **Unpatched Legacy Systems (Windows 2012)** |
|---|---|
| **Description** | GridLink is using unsupported Windows 2012 servers in the Distribution Management System (DMS), which cannot be patched due to the lack of vendor support. |
| **Impact** | **Critical**: these unpatched systems are highly vulnerable to exploitation, as attackers could leverage known vulnerabilities in outdated software to compromise critical OT systems. |
| **Probability** | **High**: with known vulnerabilities in Windows 2012, the likelihood of an exploit is high, especially as these servers continue to handle essential operational processes. |
| **Recommendations** | Expedite the upgrade of these legacy systems and, in the meantime, apply compensating controls such as network segmentation, isolation, and virtual patching. |
| **NIST 800-82r3 Recommendations** | Section 5.2.5 Layer 5 – Software Security, Section 5.2.5.2 Patching |

## H-01: Insufficient VPN Authentication for Remote Access

| **High** | **Insufficient VPN authentication for remote access** |
|---|---|
| **Description** | GridLink's VPN appliances allow remote access for operators but do not require multi-factor authentication (MFA). While OT Active Directory is integrated, the lack the hardware tokens or one-time passcode (OTP) exposes the network to credential theft risks. |
| **Impact** | **High**: the absence of MFA creates a significant risk, as compromised credentials could allow unauthorized access to OT systems. This could lead to potential sabotage or disruption of critical operations in the power utility. |
| **Probability** | **High**: given the increasing frequency of phishing and credential theft attacks, the risk of compromised accounts is considerable without MFA. |
| **Recommendations** | Implement MFA for all remote access systems, especially for VPNs. This can be achieved using hardware tokens or software-based OTPs. |

| | |
|---|---|
| **NIST 800-82r3 Recommendations** | Section 6.2.1.4.4 Multi-Factor Authentication, Section 6.2.10 Remote Access |

## H-02: Insufficient Segmentation for Critical OT Applications

| High | **Insufficient Segmentation for Critical OT Applications** |
|---|---|
| **Description** | The Distribution Management System (DMS) and Outage Management System (OMS) are not properly segmented from other OT applications. Both reside in the same production network zone without proper isolation. |
| **Impact** | **High**: inadequate segmentation could allow an attacker or malware to move laterally across systems, compromising multiple critical OT applications. |
| **Probability** | **Medium**: while firewalls exist between OT and IT, the lack of internal segmentation within the OT environment increases the risk of exposure. |
| **Recommendations** | Accelerate the segmentation of critical OT applications to minimize lateral movement and reduce the risk of widespread compromise. |
| **NIST 800-82r3 Recommendations** | Section 5.2.3.1 Network Architecture, Section 6.2.1.3 Network Segmentation and Isolation |

## H-03: Unhardened OT Workstations in Transformer and Distribution Stations

| High | **Unhardened OT Workstations in Transformer and Distribution Stations** |
|---|---|
| **Description** | Windows 10 computers used in the Transformer and Distribution stations are not hardened and rely solely on firewall protection and restricted Internet access for security. |
| **Impact** | **High**: unhardened workstations are vulnerable to internal attacks, especially if compromised through other means such as physical access or lateral movement from other parts of the OT network. |
| **Probability** | **Medium**: while physical access and Internet restrictions mitigate some risks, unhardened systems can still be compromised through lateral attacks or USB devices. |
| **Recommendations** | Apply security hardening to all OT workstations following CIS |

| | |
|---|---|
| | benchmarks ensuring that all devices idea to best practices for OS and application security. |
| **NIST 800-82r3 Recommendations** | Section 5.2.4 Layer 4 – Hardware Security |

## M-01: Lack of Log monitoring for OT Devices

| **Medium** | **Lack of Log monitoring for OT Devices** |
|---|---|
| **Description** | Logs from OT devices located in Transformer and Distribution stations are not collected or monitored by SIEM, leaving these critical devices without centralized business. |
| **Impact** | **Medium**: without logs, the ability to detect security incidents is significantly reduced, delaying potential incident response and increasing the attack surface. |
| **Probability** | **Medium**: the distributed nature of the OT devices located in Transformers and Distributions stations makes it less likely for centralized monitoring, but the potential impact of undetected breaches is still significant. |
| **Recommendations** | Implement logging and monitoring for all OT devices and integrate them with the centralized SIEM for improved visibility. |
| **NIST 800-82r3 Recommendations** | Section 5.2.3.3 Network Monitoring, Section 5.2.3.2 Centralized Logging |

## M-02: Incomplete Firewall Upgrades

| **Medium** | **Incomplete Firewall Upgrades** |
|---|---|
| **Description** | GridLink is only halfway through replacing its legacy firewalls at field stations with NGFWs (Next Generation Firewalls) that include built-in IDS capabilities. |
| **Impact** | **Medium**: legacy firewalls without IDS leave critical areas of the OT network vulnerable to undetected threats and intrusions, especially at the station levels. |
| **Probability** | **Medium**: the legacy firewalls remain in place at several stations, increasing the chance of exploitation before the upgrade process is complete. |
| **Recommendations** | Prioritize the completion of NGFW installations to ensure consistent monitoring and security across all station networks. |

| | |
|---|---|
| **NIST 800-82r3 Recommendations** | Section 5.2.3.1 Network Architecture, Section 6.2.1.3 Network Segmentation and Isolation |

The risks outlined in this report have been assessed using the GridLink Risk Rating Matrix.

**Probability Levels:**

1. **Low**: Unlikely to occur.
2. **Medium**: Could occur occasionally.
3. **High**: Very likely or frequently occurring.

**Impact Levels:**

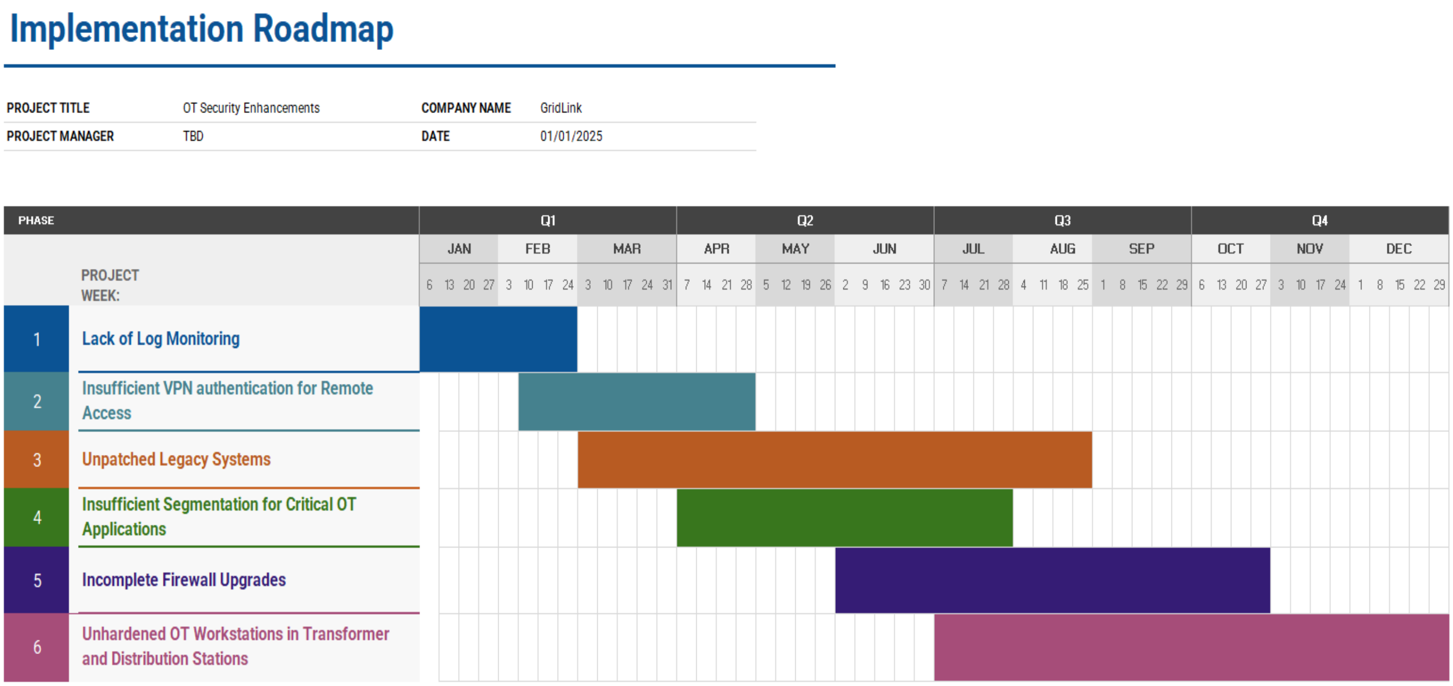
1. **Low**: Minimal impact, easily manageable.
2. **Medium**: Some impact, manageable with some effort.
3. **High**: Significant impact requires substantial resources to manage.
4. **Critical**: Severe impact, challenging to manage and could cause significant disruption.

| | | | | |
|---|---|---|---|---|
| **Impact** | **Critical** | High | Critical | Critical |
| | **High** | Medium | High | High |
| | **Medium** | Low | Medium | Medium |
| | **Low** | Low | Low | Low |
| | | **Low** | **Medium** | **High** |
| | | **Probability** | | |

## Prioritization of Findings

| Finding (in priority order) | Risk Rating | Duration | Resources |
|---|---|---|---|
| Lack of Log Monitoring for OT Devices | Medium | Low (less than 3 months) | Medium (2 resources) |
| Insufficient VPN authentication for Remote Access | High | Medium (3 months) | High (3+ resources) |
| Unpatched Legacy Systems | Critical | High (6 months) | High (3+ resources) |
| Insufficient Segmentation for Critical OT Applications | High | Medium (3+ months) | Medium (2 resources) |
| Incomplete Firewall Upgrades | Medium | Medium (3-6 Months) | Medium (2 resources) |
| Unhardened OT Workstations in Transformer and Distribution Stations | High | High (6+ months) | High (3+ resources) |

## Implementation Roadmap



### Implementation Roadmap

| | | | |
|---|---|---|---|
| PROJECT TITLE | OT Security Enhancements | COMPANY NAME | GridLink |
| PROJECT MANAGER | TBD | DATE | 01/01/2025 |

| PHASE | PROJECT WEEK: |
|---|---|
| 1 | Lack of Log Monitoring |
| 2 | Insufficient VPN authentication for Remote Access |
| 3 | Unpatched Legacy Systems |
| 4 | Insufficient Segmentation for Critical OT Applications |
| 5 | Incomplete Firewall Upgrades |
| 6 | Unhardened OT Workstations in Transformer and Distribution Stations |

# Conclusion

Over the past 3 months, the GridLink security team has conducted an Operational Technology (OT) gap assessment. The following areas were in scope for the assessment:

- A current state assessment of GridLink's OT environment and existing security measures.
- Identification of security gaps in the OT environment.
- Mapping of GridLink's OT network to the Purdue Model.
- Assessing identified gaps from a risk perspective and prioritizing them.
- Developing a recommended implementation roadmap with estimated duration and resources to address the identified gaps.

In conclusion, while GridLink has implemented strong security measures in their OT environment, the gaps identified in this report outline several areas where improvements can be made. By addressing these gaps, GridLink will enhance its overall cybersecurity posture, ensuring alignment with industry's best practices and regulatory standards, while also improving resilience to evolving threats.