**GridLink Utilities**

# *Operational Technology Gap Assessment*

28 July 2024


Angel Mary George
Edmonton, Alberta

# *Executive Summary*

This report represents findings from an Operational Technology Gap Assessment of GridLink's OT environment. This assessment took place over the last 3 months. The goals of this assessment include:

- Performing a current state assessment of GridLink's OT environment and existing security measures.
- Identification of security gaps in GridLink's environment
- Mapping GridLink's OT network to the Purdue Model.
- Providing recommendations to address identified gaps and to improve GridLink's OT security posture
- Prioritizing gaps discovered
- Recommending an implementation roadmap that includes estimated duration and resources required to address the gaps identified Current State Analysis.

A workshop was held with a number of key stakeholders from the OT department and 5 different gaps were identified. Identified gaps have been risk rated based on the likelihood and impact of the gaps being exploited.

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

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

- A high risk gap related not having multi-factor authentication for the virtual private network (VPN) appliances used to access the control centre.
- A high risk gap related to insufficient network segmentation within the OT environment.
- A medium risk gap related to use of unsupported Legacy operating systems in the Operational Technology environment.
- A medium risk gap related to not hardening Windows 10 Systems in the OT environment.

## ***System Overview***

GridLink Utilities, a venerable entity with 75 years in the industry, operates within the critical infrastructure sector, servicing two medium-sized cities and their surrounding areas. The company manages a primary control centre and a backup control centre, situated approximately 30 minutes apart, to ensure robust operational reliability. GridLink's extensive network includes 10 transformer stations and 50 distribution stations, forming a wide-area network that links these

control centres to various stations, thereby maintaining seamless operational control over their service regions.

At the heart of GridLink's operations is their Operational Technology (OT) network, which oversees and manages the physical processes essential to the utility's function. This network is securely segregated from the corporate IT network by firewalls and an industrial DMZ, facilitating secure data transfers between the two environments. The OT Operations team is responsible for approximately 250 Windows servers and 75 Linux servers housed within the primary and backup control centres. Each station under GridLink's management is equipped with one or two workstations dedicated to managing OT devices on-site, ensuring localized control and monitoring.

GridLink's OT environment is powered by several critical applications. The Distribution Management System (DMS) is pivotal for delivering power to customers, ensuring efficient distribution across the network. The Energy Management System (EMS) plays a crucial role in monitoring, controlling, and optimizing the transmission system's performance, enhancing the reliability and efficiency of power supply. Additionally, the Outage Management System (OMS) provides timely outage notifications to customers via automated phone calls, SMS messages, and a mobile application, ensuring that customers are well-informed and can manage disruptions effectively.

## ***Existing Security Measures***

GridLink Utilities's corporate network and the OT network is separated by an industrial demilitarized zone (DMZ).Next-generation firewalls are placed to restrict and monitor traffic between the two networks. Intrusion detection sensors (IDS) are deployed in critical areas of the OT network to continuously monitor and detect any anomalous activities.Additionally, firewalls are installed at all stations, with an ongoing upgrade process to replace legacy firewalls with next-generation ones that offer built-in intrusion detection capabilities.Internet access within GridLink's OT network is tightly controlled and limited to essential systems or services that need to pull update files from specific vendors. External-facing proxy servers are utilized to manage and control which systems can access specific websites, while internet access is strictly prohibited from transformer and distribution stations. Access control lists (ACLs) on routers at each station further regulate network traffic, ensuring only authorized communications occur within and outside the station networks.

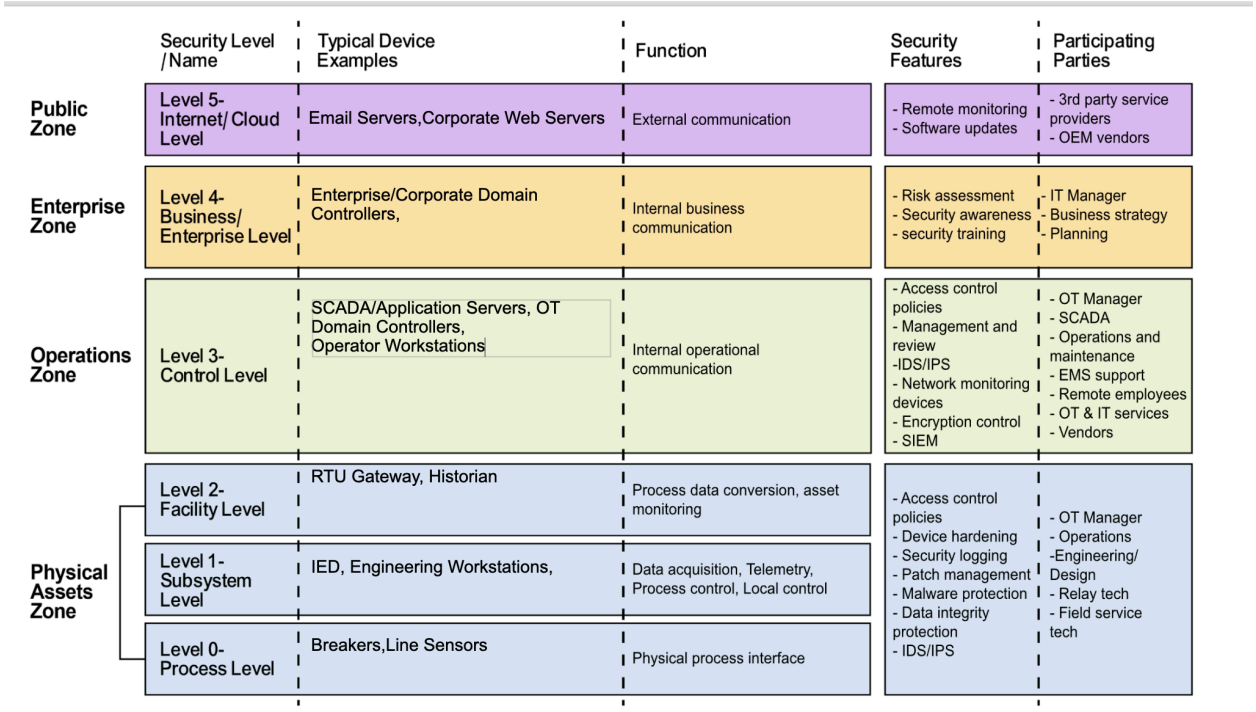
To facilitate secure remote access, GridLink has deployed pairs of Internet-facing virtual private network (VPN) appliances, allowing employees and vendor partners to connect to the OT network securely. Additionally, a jump box/server infrastructure enables users from the corporate network to manage systems residing within the OT network.

GridLink is using an automated patch deployment platform to apply security patches for servers and workstations located at the control center and the stations on a monthly basis .Application-

related patches for critical systems such as the distribution management system (DMS) and the energy management system (EMS) are applied quarterly. GridLink employs an agent-based automated vulnerability scanning platform to conduct weekly scans of end-user workstations and servers in the control center. Network-based scanners are deployed at strategic points within the OT network to perform monthly scans of the routers and switches and other network based devices that support the OT network.

Anti-virus software is installed on OT workstations and both Windows and Linux servers in the control centers, providing an additional layer of defense against malware and other cyber threats.

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



# *Gap Analysis*

## ***H-01: Single Factor Authentication for Remote Access***

| **High** | Single Factor Authentication for Remote Access |
|---|---|
| **Description** | GridLink has implemented robust multi-factor authentication (MFA) for their terminal services farm but lacks MFA for their virtual private network (VPN) appliances, which were installed to provide remote access for operators to access their control centre workstations from home. |
| **Impact** | **High:** Due to the the lack of multi-factor authentication (MFA) for VPN appliances ,the attackers could exploit weaker single-factor authentication mechanisms and potentially gain unauthorized access to critical control centre workstations within the OT environment. |
| **Probability** | **High:** When attackers target an organization, an internet-facing VPN is a frequent point of attack because it provides a direct entryway into the network. Without multi-factor authentication (MFA), attackers can more easily exploit weak or stolen credentials, making unauthorized access highly probable. |
| **Recommendations** | GridLink should implement multi-factor authentication (MFA) on their virtual private network (VPN) appliances to better secure remote access to their control center workstations. Even though robust MFA is in place for the terminal services farm, the lack of MFA on the VPN creates a high probability of unauthorized access, as internet-facing VPNs are frequent attack targets. As pointed out in the SANS 5 Critical Controls article, MFA has been shown to significantly reduce the number of adversary attack paths. |
| **NIST 800-82r3 Recommendations** | Section 6.2.1.4.4 Multi-Factor Authentication |

## ***H-02 Insufficient Segmentation***

| **High** | Insufficient Segmentation |
|---|---|

| | |
|---|---|
| **Description** | The IT and OT networks of GridLink are segmented, and the EMS is separated into a secure, firewalled zone. However, GridLink's Distribution Management System (DMS) and Outage Management System (OMS) currently reside in the production zone without being segmented from other OT applications. |
| **Impact** | **High:** Insufficient network segmentation in GridLink's OT environment presents significant risks. The current lack of segmentation for the Distribution Management System (DMS) and Outage Management System (OMS) from other applications in OT exposes these systems to potential threats, allowing malware or ransomware to spread or enabling attackers to move laterally across the network. |
| **Probability** | **Medium**: While there are controls in place to separate IT and OT networks, as well as development and production sites, additional segmentation is needed to isolate the DMS (Distribution Management System) and the Outage Management System (OMS) from other applications within the production environment. |
| **Recommendations** | A dedicated Incident response plan should prioritize actions based on the potential for operational impact and how to position the system to operate through an attack so that it reduces the effect of the attack and the impact on the process under control. |
| **NIST 800-82r3 Recommendations** | Section 6.2.1.3 Network Segmentation and Isolation |

## ***H-03: Lack of Monitoring for OT Equipment***

| | |
|---|---|
| **High** | Lack of Monitoring for OT Equipment |
| **Description** | Although GridLink's monitoring team receives logs from network equipment, servers, and workstations in the control centre, they do not receive logs from OT equipment located in their stations |
| **Impact** | **High:** The absence of log monitoring for OT equipment in GridLink's stations significantly affects the ability to detect and respond to potential threats promptly. This gap increases the risk of undetected incidents, potentially leading to severe operational disruptions or breaches in critical infrastructure. |

| | |
|---|---|
| **Probability** | **Medium**: Although GridLink's stations lack log monitoring for OT equipment, other security measures such as firewalls, access controls, and intrusion detection systems are in place to mitigate some threats.Additionally,the monitoring is planned but not yet implemented. |
| **Recommendations** | GridLink should implement log monitoring for all OT equipment in their stations to enhance threat detection and response capabilities. Additionally, they should conduct regular reviews and updates of their security measures to ensure they remain effective against evolving threats. |
| **NIST 800-82r3 Recommendations** | Section: 6.2.6.1 - Logging |

## ***M-01: Unhardened Windows 10 Systems:***

| | |
|---|---|
| **Medium** | Unhardened Windows 10 Systems |
| **Description** | The OT team follows the CIS Benchmarks for all Windows and Linux server builds. However, the Windows 10 computers used for local control in GridLink's transformer and distribution stations are not hardened, relying instead on firewalls and restricted Internet access for security. |
| I**mpact** | **High** : Insider threats have the potential to cause significant harm due to the insider's access and knowledge of the system. They can exploit vulnerabilities to cause disruptions, steal sensitive data, or compromise critical infrastructure. |
| **Probability** | **Low**: As the workstations are scanned for vulnerabilities regularly and the network team applies patches to address vulnerabilities on a regular basis the probability of this finding being compromised is relatively low. |
| **Recommendations** | GridLink's network team should adopt the Center for Internet Security's Benchmarks or other hardening guidelines from reputable organizations such as NIST to enhance the security of their network devices. In the absence of specific benchmarks, the team should consult with manufacturers for their security recommendations and best practices. |

| | |
|---|---|
| **NIST 800-82r3 Recommendations** | Section 5.2.4 - Hardware Security |

## ***M-02: Legacy operating systems***

| | |
|---|---|
| **Medium** | Use of unsupported legacy operating systems |
| **Description** | GridLink is using several legacy operating systems, specifically Windows 2012 servers, which have numerous vulnerabilities that cannot be patched due to their lack of support from Microsoft. |
| **Impact** | **High**: The usage of legacy Windows 2012 servers is vulnerable due to outdated security patches, which could potentially lead to severe operational disruptions or breaches in the critical infrastructure. |
| **Probability** | **Low** : Although the legacy Windows 2012 Servers have unpatched vulnerabilities, GridLink has implemented several compensatory controls such as network segmentation, intrusion detection systems, and regular vulnerability scans. These measures help mitigate the risks but do not entirely eliminate the potential for exploitation. |
| **Recommendations** | GridLink should consider updating their operating systems or invest in compensatory controls, such as firewalls with deep packet inspection and intrusion prevention systems (IPS), to detect and prevent attacks targeting unpatched vulnerabilities. |
| **NIST 800-82r3 Recommendations** | Section 5.2.5.2. Patching |

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:

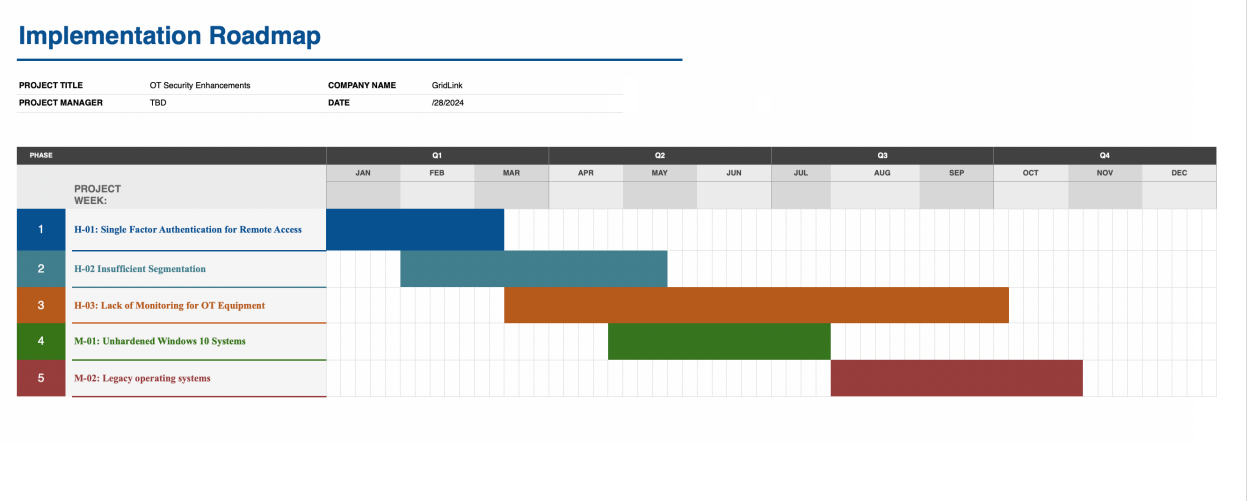
1. Low: Minimal impact, easily manageable.
2. Medium: Some impact, manageable with some effort.
3. High: Significant impact, requires substantial resources to manage.
4. Critical: Severe impact, challenging to manage and could cause significant disruption.

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

## *Prioritization of Finding*

| Finding (in priority order) | Risk Rating | Duration | Resources |
|---|---|---|---|
| H-01: Single Factor Authentication for Remote Access | High | **Low** (less than 3 months) | **Low** (1 resource) |
| H-02 Insufficient Segmentation | High | **Medium** (3-6 months) | **High** (3+ resources) |
| H-03: Lack of Monitoring for OT Equipment | High | **High**(6+ months) | **High**(3+resources) |
| M-01: Unhardened Windows 10 Systems: | Medium | **Medium** (3-6 months) | **Medium** (2 resources) |
| M-02: Legacy operating systems | Medium | **Medium** (3-6 months) | **Medium** (2+ resources) |

# *Implementation Roadmap*




# *Conclusion*

Over the past 3 months, the GridLink security team has performed an 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 GridLink's OT network to the Purdue Model.
- Gaps in GridLink's OT environment were assessed from a risk perspective and prioritized.
- A recommended implementation roadmap that includes estimated duration and resources required to address the gaps has been included.

In conclusion, while GridLink has made significant progress in securing its Operational Technology environment, the identified gaps in this report highlight areas needing improvement to mitigate cybersecurity risks effectively. Addressing these gaps will ensure compliance with industry best practices and regulatory requirements and enhance GridLink's resilience against emerging cybersecurity threats.