**GridLink Utilities**

# **Operational Technology Gap Assessment**

**[05|06|24]**

[Indo Bishmang]

[Mississauga, ON]

## Executive Summary

This report presents findings from an Operational Technology (OT) Gap Assessment of GridLink Utilities' OT environment, conducted over the past three months. The goals of this assessment were to:

* Assess the current state of GridLink’s OT environment and existing security measures.
* Identify security gaps in GridLink’s environment.
* Map GridLink’s OT network to the Purdue Model.
* Provide recommendations to address identified gaps and improve GridLink’s OT security posture.
* Prioritize the discovered gaps.
* Recommend an implementation roadmap with estimated duration and resources needed to address the identified gaps.

A workshop with key stakeholders from the OT department revealed four different gaps, which were risk-rated based on the likelihood and impact of exploitation.

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

The following high-level summary outlines the identified gaps:

* A **high-risk** gap due to the absence of a dedicated incident response plan for the OT environment.
* A **high-risk** gap stemming from insufficient network segmentation within the OT environment.
* A **high-risk** gap from the lack of multi-factor authentication for the virtual private network used to access OT assets.
* A **medium-risk** gap due to the lack of hardening of workstations and servers in the OT environment.

Top of Form

Bottom of Form

## Current State Analysis

### **System Overview**

GridLink Utilities, a company with 75 years of experience, operates a primary and a backup control center for their Operational Technology (OT) network, which are about 30 minutes apart. They manage 10 transformer stations and 50 distribution stations across two medium-sized cities and their surrounding areas, servicing customers in these regions.

The company uses an OT network to manage physical processes and a separate IT network, connected via firewalls and an industrial DMZ to securely transfer data between the networks. A wide-area network links the control centers to the transformer and distribution stations. The OT Operations team oversees approximately 250 Windows servers and 75 Linux servers across the primary and backup control centers. Each station has 1 or 2 workstations for managing OT devices.

GridLink's key OT applications include a distribution management system (DMS) for delivering power, an energy management system (EMS) for monitoring, controlling, and optimizing transmission performance, and an outage management system (OMS) for providing outage notifications to customers through automated calls, SMS, and a mobile app.

### **Existing Security Measures**

GridLink's Utilities corporate network is separated from their OT network by an industrial demilitarized zone (DMZ) and next-generation firewalls to restrict traffic between the two networks. They have deployed intrusion detection sensors (IDS) in key areas of their OT network and are halfway through replacing legacy firewalls at their stations with next-generation firewalls featuring built-in intrusion detection capabilities.

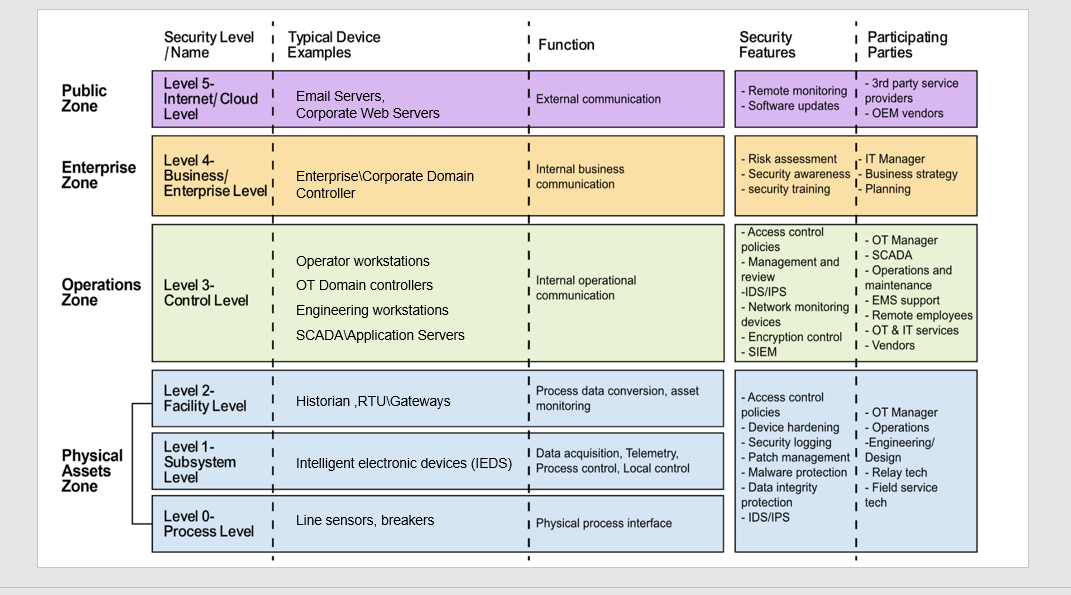
Internet access within the OT network is limited to necessary systems and services, with external-facing proxy servers controlling access to specific websites. Internet access is not allowed from GridLink's transformer and distribution stations. Access control lists (ACLs) on routers at their stations manage network traffic.

GridLink has pairs of Internet-facing virtual private network (VPN) appliances for remote connections to the OT network by employees or vendor partners. They also use a jump box/server infrastructure for corporate network users to manage OT network systems.

Security patches are applied monthly to servers and workstations at the control center and stations, while application-related patches for systems like the distribution management system (DMS) and the energy management system (EMS) are applied quarterly. An automated vulnerability scanning platform performs weekly scans of end-user workstations and servers in the control center. Network-based scanners perform monthly scans of routers, switches, and other network devices.

GridLink has deployed antivirus software on their OT workstations in the control centers and stations, as well as on the Windows and Linux servers in the control centers.

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



## Gap Analysis

### **H-01: Single Factor Authentication**

|  |  |
| --- | --- |
| **High**  **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Single Factor Authentication** |
| **Description** | Gridlink has implemented multi-factor authentication (MFA) for access to their OT environment for users located outside of GridLink’s control centers but has not implemented MFA for the Internet facing OT VPN appliances. |
| I**mpact** | **High**: The impact of a disgruntled employee or an attacker gaining access to the OT environment through the VPN could be high. An attacker could potentially gain unauthorized access to critical OT systems and cause outages or put human lives at risk. |
| **Probability** | **High**: When attackers try to gain access to an OT environment, they frequently target an organization’s IT environment first. Attackers having unauthorized remote access frequently via for example phishing emails to try to get end users to install software or provide their user credentials. There is a reasonable chance that if an attacker gained access to Gridlink’s IT network, they’d try to access the OT network. |
| **Recommendations** | Multi-factor authentication should be enabled on Gridlink’s Virtual private Network. MFA can be safely applied to most OT/ICS environments. As pointed out in the [SANS 5 Critical Controls](https://sansorg.egnyte.com/dl/R0r9qGEhEe) article, MFA has been shown to significantly reduce the number of adversary attack paths. This measure would restrict unauthorized access and protect OT environment. |
| **NIST 800-82r3 Recommendations** | [Section 6.2.1.4.4 Multi-Factor Authentication](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### 

### **[H-02: Insufficient Network Segmentation**

|  |  |
| --- | --- |
| **High**  **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Insufficient Network Segmentation** |
| **Description** | Gridlink has segmented their OT network from their IT network and they have also segmented their OT development environment from production. Additionally, with the IDMZ segmented access from the corportae network to OT data is also present. However, Gridlink should further segment their OT network to separate systems based on function. For example, Gridlink should segment their Distribution Management System(DMS) and Outage Management System (OMS) as they serve different purposes. |
| I**mpact** | **High**: Insufficient network segmentation presents risk in OT environments as it can expose vulnerable systems that were not designed with modern cybersecurity threats in mind. Inadequate segmentation could allow malware or ransomware to spread to other systems or could allow an attacker to move laterally across Gridlink’s OT network. |
| **Probability** | **Medium**: Although some controls are in place to segment OT from IT and the OT, development environment from production, and Gridlink stations from their control centres, they should also create additional segmentation zones to further segment systems. |
| **Recommendations** | A dedicated OT incident response program should be established. The 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](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### 

### **H-03: No Operational Technology Specific Incident Response Plan**

|  |  |
| --- | --- |
| **High**  **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **No Operational Technology/Industrial Control System Specific Incident Response Plan** |
| **Description** | Although Gridlink does have 2 seperate incident response programs, they do not have an Operational Technology (OT)/Industrial Control System (ICS) specific incident response plan. |
| I**mpact** | **High**: As OT environments are very different from IT environments, organizations should have OT specific incident response plans to account for the complexities and operational necessities of responding in operational environments. Without a dedicated and harmonized incident response plan for OT, Gridlink may not be prepared to handle security incidents in this environment. Additionally, technology decisions in OT may not align with the necessities of incident response if a dedicated plan does not exist. |
| **Probability** | **High**: Security incidents happen fairly regularly in both IT and OT incidents. Attacks against OT environments have become more common. In recent years high profile security incidents have occurred such as the ransomware attack against [Colonial Pipeline](https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack) and the [2015](https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack) and [2016](https://en.wikipedia.org/wiki/2016_Kyiv_cyberattack) attacks against Ukraine’s power grid. |
| **Recommendations** | A dedicated OT incident response program should be established. The 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 3.3.8 Develop an Incident Response Capability](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

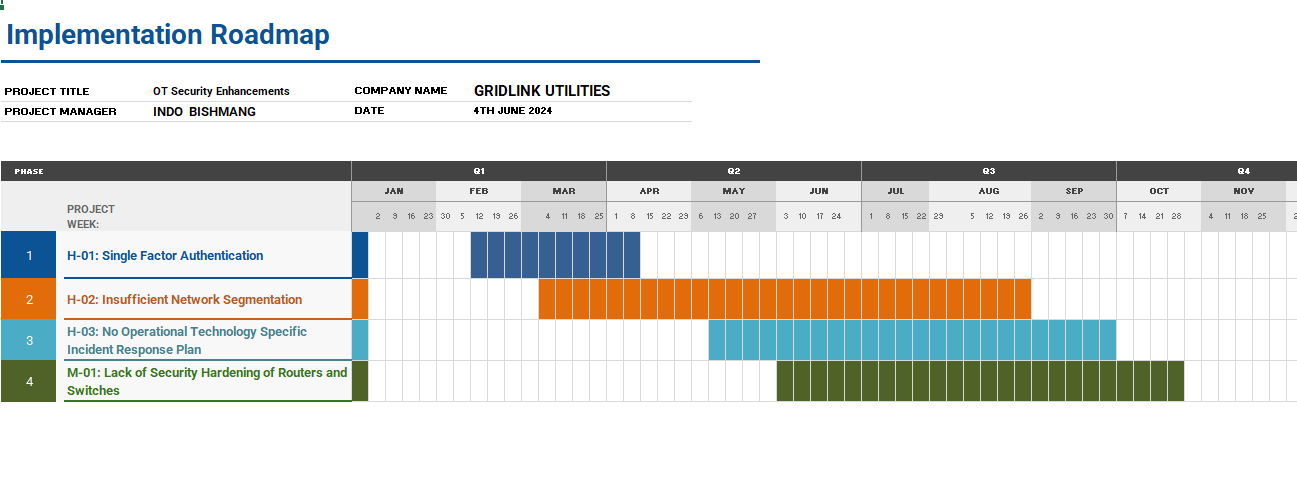
### **M-01: Lack of Security Hardening of Workstations and Servers**

|  |  |
| --- | --- |
| **MEDIUM**  **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Lack of Security Hardening of Workstations and Servers** |
| **Description** | During the workshop, it was revealed that Gridlink OT teams generally follow industry guidance such as the Center for Internet Security’s (CIS) Benchmarks to harden servers and other devices. One exception that was noted was the network team is not applying hardening processes workstations and servers in the OT environment. |
| I**mpact** | **High**: The impact from not hardening workstations and servers in the OT environment could be high. Gridlink’s communication infrastructure depends on the accurate server to workstation relationship. If these types of devices are not securely configured or are left in their default configuration, they can become prime targets for attackers. This could result in increased vulnerability, data breaches, system downtime or compliance violations. |
| **Probability** | **Low**: As the workstations and servers 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 look to adopt the Center for Internet Security’s Benchmarks or other hardening guidelines from organizations such as NIST to assist with hardening workstations and servers. If there are no benchmarks available, the network team should ask the manufacturers of the devices they are using for hardening recommendations. |
| **NIST 800-82r3 Recommendations** | [Section 5.2.4 - Hardware Security](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

## Prioritization of Findings

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding (in priority order)** | **Risk Rating** | **Duration** | **Resources** |
| **H-01: Single Factor Authentication** | **High** | **Low** (less than 3 months) | **Low** (1 resource) |
| **H-02: Insufficient network segmentation** | **High** | **High** (6+ months) | **High** (3+ resources) |
| **H-03: No Operational Technology Specific Incident Response Plan** | **High** | **Medium** (3-6 months) | **Medium** (2 resources) |
| **M-01: Lack of Security Hardening of Workstations and Servers** | **Medium** | **Medium** (3-6 months) | **Medium** (2 resources) |

## Implementation Roadmap



## Conclusion

GridLink Utilities security team has conducted an OT gap assessment, covering the following areas:

* 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.
* Assessment of gaps in GridLink’s OT environment from a risk perspective and prioritization of these gaps.
* A recommended implementation roadmap, including estimated duration and resources required to address the gaps.

In conclusion, while GridLink Utilities has made progress in securing its Operational Technology environment, the gaps identified in this report highlight areas needing improvement to mitigate cybersecurity risks effectively. Addressing these gaps will not only ensure compliance with industry best practices and regulatory requirements but also enhance GridLink's utility’s resilience against emerging cybersecurity threats.

Top of Form

Bottom of Form