**GridLink Utilities**

# **Operational Technology Gap Assessment**

**May 4th, 2024.**

Leonard Offor

Edmonton. AB.

## 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.

A workshop was held with several key stakeholders from the OT department and 4 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** |
| 1 | 3 | 1 |  |

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

* A **critical risk** gap related to having components of the Distribution Management System (DMS) application running on legacy Operating system which is not patch supported by the vendor.
* A **high risk** gap related to not having a monitoring, detection and Incident response capability on equipment in the OT network.
* A **high risk** gap related to insufficient network segmentation within the OT environment for the DMS and OMS application.
* A **high risk** gap related to not having multi-factor authentication enabled for the remote connection to the OT network via VPN devices.
* A **medium risk** gap related to not hardening 10 Windows computers in the stations.

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

## Current State Analysis

### **System Overview**

Gridlink Utilities is a medium sized power utility that operates transmission and distribution systems. The company has been in business for 75 years and services 2 customers in 2 relatively large cities and their surrounding areas. Gridlink operates 10 transformer stations and 50 distribution stations that adjust voltages for long-distance transmission and for local distribution. They also operate a primary and a back-up control center that are located 30-mins apart. The control centers control and monitor the flow of electricity through the power grid and manage load balancing.

Gridlink operates an Operation Technology (OT) network which consist of 250 windows servers and 75 Linux servers at primary and back-up control centers, to manage the physical processes of the utility. The corporate (IT) network is separated from the OT network by firewalls (50% of which are still legacy Firewalls) and by an industrial DMZ.

A WAN connecting the control centers to their transformer and distribution station is in place. Each station has 1 or 2 workstations that is used to manage the OT devices located at each of the stations. IDS sensors are deployed in key areas of the OT network to monitor traffic. There is limited internet access to OT using external facing proxy servers while there is no internet access from transformer or distribution stations.

The three main applications that reside in Gridlink’s control centers are the Distribution Management System (DMS), Energy Management System (EMS) and the Outage Management System (OMS). The DMS is a software platform designed to improve the efficiency, reliability and safety of the electrical distribution grid, which is part of the electrical power system that distributes power from transmission systems to individual customers. EMS is a software platform that monitors, controls and optimizes the performance of the power transmission system. OMS provides outage notifications to their customers through automated phone calls, SMS messages and a mobile application.

### **Existing Security Measures**

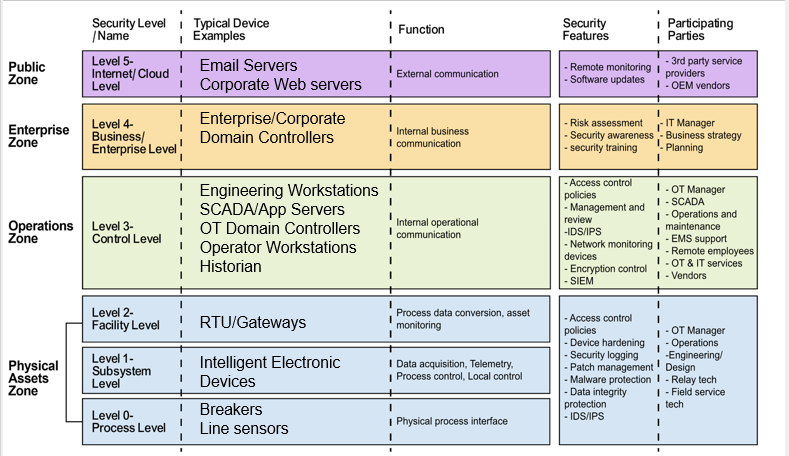
Gridlink has taken some steps to separate their corporate/IT network from their Operational Technology (IT) environment by deploying a DMZ. IDS sensors are deployed in key areas of the OT network to monitor traffic. Additionally, firewalls have been deployed at all stations with 50% of them still to be changed to Next-generation Firewall with inbuilt intrusion detection capabilities. Antivirus software has been deployed on all Windows and Linux systems as well as all workstations in Gridlink’s OT environment.

Gridlink has limited Internet access from the OT network. Proxy servers have been implemented to limit the devices that can connect to the Internet. GridLink has pairs of Internet facing virtual private network (VPN) appliances that allow employees or vendor partners to connect remotely to the OT network. Jump box deployed which allows users from the corporate network to manage systems that reside in the OT network. There is no Internet access permitted from the transformer and distribution stations. Access Control list (ACL) is implemented on routers at the stations to control network traffic in and out of station network.

Gridlink performs security patches on a monthly basis using an automated patch deployment platform. App patches applied are applied quarterly. Gridlink deployed an agent-based vulnerability scanning platform on end-user workstations, the Linux and Windows servers in the control center and this scans all endpoints on a weekly basis Network based scanners have been deployed on the OT network that scan on a monthly basis.

### 

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



## 

## Gap Analysis

### **C-01: Unpatched Legacy Operating system in the OT Application**

|  |  |
| --- | --- |
| **Critical** | **Unpatched Legacy Operating system in the OT Application** |
| **Description** | Components of the Distribution Management System (DMS) still running legacy Operating system (windows 2012) which Microsoft no longer supports patching for. |
| **Impact** | **Very high**: Inability to patch legacy systems leaves them vulnerable to a wide range of cyber attacks that can have far reaching effects to Gridlink’s information security and operational safety. |
| **Probability** | **High**: Many threat actors in the energy industries are known to target windows vulnerabilities as a means of gaining access to the network. Successful attacks have been recorded that exploited one or more windows vulnerabilities e.g the NotPetya ransomware attack in Ukraine (2017). |
| **Recommendations** | DMS operating systems components running legacy operating systems need to be upgraded to modern operating systems that are supported with patch management from vendor. In the case when not possible, additional controls need to be put in place to secure the environment from attempts to exploit known vulnerabilities. Some tools such as web application firewalls (WAF) and IPS, could be configured to provide additional protection to detect or prevent attacks against unpatched vulnerabilities while the organization waits for an opportunity to apply the OS updates. Other tools such as bump-in-the-wire security devices, can be installed in line with devices that cannot be updated or are using obsolete operating systems |
| **NIST 800-82r3 Reference** | [Section 5.2.5.2 Patching](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### **H-01: No monitoring & detection capacity on OT equipment in the stations**

|  |  |
| --- | --- |
| **High** | **No monitoring & detection capacity on OT equipment in the stations** |
| **Description** | Although Gridlink does have separate incident response program for both IT and OT networks, there are several OT equipment logs that are not being forwarded to the SIEM for monitoring and threat detection. |
| **Impact** | **High**: Prescence of blind spots in the network greatly undermines incidence response capability and this can be impactful to the organization’s security. An attacker can gain local entry to the OT network and traverse laterally through systems causing significant damage and this would not be detected. |
| **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 occured 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** | All OT network devices and endpoints logs should be aggregated and forwarded to the SIEM. Use cases for threat detection should be established and incidence response plans updated for each of them. A log forwarder should be deployed that will collect logs from all assets within the stations and forward them securely to the SIEM. |
| **NIST 800-82r3 Reference** | [Section 3.3.8 Develop an Incident Response Capability](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

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

|  |  |
| --- | --- |
| **High** | **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. However, Gridlink should further segment their OT network to separate systems based on function. For example, Gridlink should segment their Distribution Management System and Outage Management System from other production apps as they serve different purposes. |
| **Impact** | **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 Reference** | [Section 6.2.1.3 Network Segmentation and Isolation](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### **H-03: Single Factor Authentication**

|  |  |
| --- | --- |
| **High** | **Single Factor Authentication** |
| **Description** | Gridlink has implemented multi-factor authentication (MFA) for access to their OT networks through the jump servers but there is no multifactor authentication when operators remotely access the OT network from over the internet using the pair of VPN appliances |
| **Impact** | **High**: The impact of a disgruntled employee or an attacker gaining access to the OT environment through the abuse of VPN connection with compromised credentials could be high. An attacker could potentially gain unauthorized access to critical OT systems and cause outages or put human lives at risk. |
| **Probability** | **Medium**: When attackers try to gain access to an OT environment, they frequently target an organization’s IT environment first as user’s typically have access to email and to the Internet. Attackers frequently use 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 VPN device authentication that is used to access the OT environment from the IT environment. 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. Even though MFA has been applied to the external facing VPN appliances, it should also be applied to the internal VDI infrastructure as a measure to better restrict access to and to protect OT environment. |
| **NIST 800-82r3 Reference** | [Section 6.2.1.4.4 Multi-Factor Authentication](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### **M-01: Lack of Security Hardening of Windows Computers in the stations**

|  |  |
| --- | --- |
| **Medium** | **Lack of Security Hardening of Windows Computers in the stations** |
| **Description** | During the workshop, it was revealed that Gridlink’s 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 that there are 10 windows computers used in the transformer and distribution stations that have not yet been hardened due to limited connection from these stations to the internet. |
| **Impact** | **High**: The impact from not hardening endpoints in the OT environment could be high. Due to the ubiquity of windows computers several exploits exist for them in the wild and there is strong need to reduce the attack surface of these devices to strengthen their security. 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 data breaches, network disruptions or compliance violations. |
| **Probability** | **Low**: As the devices 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 designate a competent security employee to adopt CIS benchmark on the identified windows computers in the local stations. A plan should be put in place to regularly review the security compliance for local systems and ensure they are up to date. |
| **NIST 800-82r3 Reference** | [Section 5.2.4 - Hardware Security](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

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** | | |
| **P**  **Probability** | | |

## Prioritization of Findings

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding (in priority order)** | **Risk Rating** | **Duration** | **Resources** |
| **H-03: Single Factor Authentication** | **High** | **Low** (less than 3 months) | **Low** (1 resource) |
| **C-01: Unpatched Legacy Operating System in the OT Application** | **Critical** | **Low** (less than 3 months) | **Medium** ( 2 resources) |
| **H-01: No monitoring & detection capacity on OT equipment in the stations** | **High** | **Medium** (3-6 months) | **Medium** (2 resources) |
| **H-02: Insufficient network segmentation** | **High** | **High** (6+ months) | **High** (3+ resources) |
| **M-01: Lack of Security Hardening of Windows Computers in the stations** | **Medium** | **Medium** (3-6 months) | **Medium** (2 resources) |

## Implementation Roadmap

A screenshot of a computer

Description automatically generated

## 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 was 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 Utilities has made strides in securing its Operational Technology environment, the gaps contained in this report highlight areas for improvement to mitigate cybersecurity risks effectively. Addressing these gaps will not only comply with industry best practices and regulatory requirements but also enhance the resilience of GridLink Utilities against emerging cybersecurity threats.