**GridLink Utilities**

# **Operational Technology Gap Assessment**

**February 2,2025**

Seran Sathya

Toronto, ON

## Executive Summary

GridLink Utilities, a key energy provider, underwent a Security Gap Assessment to identify vulnerabilities within its Operational Technology (OT) environment. The assessment revealed several high-risk security gaps that could expose critical infrastructure to cyber threats.

Key findings include:

* Lack of Multi-Factor Authentication (MFA) for VPN access, increasing the risk of credential-based attacks.
* Insufficient segmentation of OMS and DMS, allowing potential lateral movement in case of a breach.
* Unpatched legacy Windows Server 2012 systems, making them vulnerable to known exploits.
* Weak security hardening on Windows 10 OT workstations, increasing risks from insider threats and unauthorized access.
* Inadequate logging for OT equipment at remote stations, leaving critical assets unmonitored.

The recommended mitigations, aligned with NIST 800-82r3, focus on deploying MFA, segmenting critical OT applications, replacing outdated systems, enforcing system hardening policies, and integrating OT logs into SIEM. By implementing these measures, GridLink can reduce cyber risk, strengthen resilience, and protect its critical energy infrastructure from evolving threats.

## Current State Analysis

### **System Overview**

GridLink Utilities is a medium-sized utility company responsible for the transmission and distribution of electricity for two relatively large cities. They operate using a primary control center and a backup control center for OT network that are 30mins apart. GridLink Utilities

operates using 10 transformers and 50 distribution stations that cover two medium sized cities and the surrounding area.

The company operates using about 250 Windows servers and 75 Linux servers at their primary and backup control centers. Each station has 1 or 2 workstations that are used to manage the OT devices located at each of the stations. They also operate a distribution management system (DMS), energy management system (EMS) and an outage management system (OMS).

### **Existing Security Measures**

GridLink Utilities also operates a corporate IT network that is separated from the OT network by firewalls and an iDMZ. Next generation firewalls are also deployed at all their stations that also have built in intrusion detection capabilities. IDS are also placed in key areas of their OT network to monitor traffic. Internet access in these OT networks is limited to systems or services that need to pull updated files from specific vendors. Externally facing Proxy servers are used to control which systems can communicate to specific websites along with control lists on routers at their stations to control network traffic. Internet access is not permitted from the GridLink transformer and distribution stations.

GridLink uses pairs of internets facing VPNs that allow vendors and or employees to connect remotely to the OT network. A jump server is also used to allow users from their corporate network to manage systems that reside in the OT network. Patches are applied to servers and workstations automatically monthly with application patches to systems like DMS and EMS on a quarterly basis. An agent based automated vulnerability scanning platform has been deployed to scan the end user workstations, the Linux and Windows servers in the control center on a weekly basis. GridLink has deployed anti-virus software on their OT workstations in the control centers and the stations as well as the Windows and Linux servers located in the control centers.

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

A diagram of a computer security system

AI-generated content may be incorrect.

## Gap Analysis

### **H-01: Lack of MFA in VPN**

|  |  |
| --- | --- |
| **High** | **Lack of MFA in VPN** |
| **Description** | Remote access VPN are used to provide access for operators to access control center workstations from home. The authentication involves integration with OT active directory but no hardware token or OTP code. |
| I**mpact** | High - Without MFA, attackers who obtain or guess an operator's username and password can log in without further verification. VPNs expose a login portal on the internet, making them a prime target for brute-force attacks or exploitation of VPN vulnerabilities. |
| **Probability** | High- Attackers actively exploit VPN vulnerabilities and the energy sector is the prime target for cyber threats. Past attacks such as the Colonial Pipeline ransomware attack (2021) and Oldsmar water treatment hack (2021) are examples of remote access or VPN being compromised due to compromised logins that lacked MFA. |
| **Recommendations** | Recommendation will include implementing MFA for all remote user access using VPN. This can include a hardware token such as RSA token with OTP and password. This would ensure if logins credentials were compromised that access to remote users accounts would still remain safe. |
| **NIST 800-82r3 Recommendations** | 6.2.1.4.4 multi – factor authentication |

### **H-02: Insufficient segmentation of OMS and DMS**

|  |  |
| --- | --- |
| **High** | **Insufficient segmentation of OMS and DMS** |
| **Description** | GridLink has segmented their OT network but have not segmented DMS and OMS from the production zone and other OT applications. This means if the OMS or DMS gets compromised a threat actor could move laterally and potentially disrupts physical processes. Such disruptions can cause financial and reputable damage to the company. |
| I**mpact** | High – A successful attack on DMS or OMS could lead to unauthorized control of power distribution systems, resulting in service disruptions, cascading failures, or potential blackouts. Attackers could also modify system settings to cause operational inefficiencies or physical damage. |
| **Probability** | Medium – While direct exploitation of OMS/DMS is challenging due to existing firewalls, the lack of full segmentation allows for lateral movement in case of a breach. If attackers compromise an adjacent system, they can pivot into OMS or DMS. |
| **Recommendations** | To mitigate the risk of insufficient segmentation between OMS and DMS, GridLink should implement VLAN segmentation and firewalls to fully separate these systems from the production OT networks. This can be achieved through firewalls, VLANs, and access control lists (ACLs) to enforce strict network isolation. Additionally, adopting a Zero Trust Architecture (ZTA) will further enhance security by implementing role-based access controls (RBAC) and least privilege access, ensuring that only authorized users can interact with these critical systems. |
| **NIST 800-82r3 Recommendations** | 6.2.1.3. Network Segmentation and Isolation |

### **M-01: Lack of hardening on Windows 10 computers**

|  |  |
| --- | --- |
| **Medium** | **Lack of hardening on Windows 10 computers** |
| **Description** | Windows 10 computers used in GridLink transformers and distribution stations are used for local controls. These systems are not hardened due to limited access to the stations by firewall and the absence of internet access. |
| I**mpact** | High – If compromised, attackers could manipulate local controls, disrupt energy distribution, or modify critical settings, leading to power instability, operational downtime, or even physical damage to infrastructure. Insider threats or rogue employees could also abuse system weaknesses to cause disruptions. |
| **Probability** | Low – While firewalls and air-gapping reduce external attack vectors, these systems are still vulnerable to physical access attacks, malware introduced via USB drives, unpatched vulnerabilities, and unauthorized insider activity. Since these machines lack proper hardening, any unauthorized access could result in significant system compromise. |
| **Recommendations** | Implement robust hardening protocols in alignment with NIST hardening guidelines to enhance security for Windows 10 computers in transformers and distribution stations. This should include disabling unnecessary services, enforcing strong authentication mechanisms, and restricting administrative privileges to limit unauthorized access. Additional measures such as application whitelisting and USB restrictions should be implemented to prevent unauthorized software execution and mitigate the risk of malware introduction via removable media.  Since these computers are air-gapped and protected by firewalls, the primary threats are insider threats and physical tampering. Therefore, a stronger focus should be placed on physical security controls, including securing access to devices and stations, restricting unauthorized entry, and implementing tamper detection mechanisms to prevent unauthorized modifications or malicious activity. |
| **NIST 800-82r3 Recommendations** | 5.2.5.4 Configuration Management |

### **H-03: Legacy Windows 2012 servers unpatched**

|  |  |
| --- | --- |
| **High** | **Legacy Windows 2012 servers unpatched** |
| **Description** | Several Windows 12 servers are still in use with the DMS being due for an update next year. These systems have number of vulnerabilities but cannot be patched as they no longer supported by Microsoft. |
| I**mpact** | High - If exploited, attackers could gain control of the DMS, potentially disrupting power distribution, altering grid operations, or shutting down critical energy infrastructure. Unpatched vulnerabilities could also be used for ransomware attacks or data exfiltration. |
| **Probability** | High - Legacy systems are among the most common attack vectors for cybercriminals, and known vulnerabilities in Windows 2012 servers are widely available. Since these servers cannot be patched, they remain continuously vulnerable to exploitation. |
| **Recommendations** | Accelerate Decommissioning of Windows 2012 Servers – Instead of waiting for the planned DMS upgrade next year, prioritize replacing or migrating critical systems to a supported OS (e.g., Windows Server 2019 or 2022). Implement Compensating Controls – Since these systems cannot be patched, apply network segmentation, application whitelisting, and strict access controls to limit exposure. Use host-based intrusion detection systems (HIDS), endpoint security tools, and continuous monitoring to detect potential threats targeting these systems. |
| **NIST 800-82r3 Recommendations** | 5.2.5.2 Patch management |

### **M-02: Lack of Logs for OT equipment in the station**

|  |  |
| --- | --- |
| **Medium** | **Lack of Logs for OT equipment in the station** |
| **Description** | GridLink’s security team receives logs from network devices, servers, and workstations in the control center, which are sent to the SIEM for threat detection. However, OT equipment in remote stations does not generate logs for centralized monitoring, creating a visibility gap in detecting and responding to security threats in critical infrastructure systems. |
| I**mpact** | Medium – Without OT log collection, threats targeting field equipment (e.g., RTUs, PLCs, IEDs) could go undetected until they cause operational disruptions. A cyberattack on unmonitored OT assets could lead to grid instability, unauthorized system manipulations, or downtime. However, GridLink does have strong firewalls, segmentation, and planned security improvements to prevent this impact therefore making this a impact of medium. |
| **Probability** | Medium – While IT systems have stronger monitoring, OT environments often lack security logging due to legacy infrastructure and operational constraints. Threat actors actively target industrial control systems (ICS), increasing the risk of undetected compromises. If malware or insider threats target OT devices, GridLink’s security team would have no immediate visibility, delaying response efforts. |
| **Recommendations** | Start ingesting logs from RTUs, PLCs, IEDs, and other field devices into the existing SIEM for centralized monitoring. – Define behavioral analytics and anomaly detection rules for OT environments to identify unauthorized commands, network anomalies, or abnormal control actions. |
| **NIST 800-82r3 Recommendations** | 5.2.3.2 Centralized Logging |

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-01: Lack of MFA in VPN | High | Short- less than 3 months | Low -1 resource |
| H-03: Legacy Windows 2012 servers unpatched | High | Short - Less than 3 months | Medium - 2 resources |
| H-02: Insufficient segmentation of OMS and DMS | High | High - 6+ months | High - 3+ resources |
| M-01: Lack of hardening on Windows 10 computers | Medium | Medium 3 - 6 months | Medium - 2 resources |
| M-02: Lack of Logs for OT equipment in the station | Medium | Medium 3 - 6 months | Medium - 2 resources |

## A screenshot of a computer AI-generated content may be incorrect.Implementation Roadmap

## Conclusion

This Security Gap Assessment highlights critical vulnerabilities in GridLink’s OT environment, including weak remote access security, insufficient segmentation, unpatched legacy systems, lack of endpoint hardening, and inadequate security monitoring. By implementing MFA, network segmentation, system upgrades, endpoint security measures, and SIEM log integration, GridLink can reduce cyber risks, enhance resilience, and align with NIST 800-82r3 best practices.

Addressing these gaps will strengthen GridLink’s ability to prevent, detect, and respond to cyber threats, ensuring secure and reliable energy operations while meeting regulatory and industry security standards.