**GridLink Utilities**

# **Operational Technology Gap Assessment**

**[2024-06-07]**

[Rishabh Gautam]

[Whitby, ON]

## Executive Summary

This report presents findings from an Operational Technology (OT) Gap Assessment of GridLink Utilities' OT environment, conducted over the past 12 months. The objectives of this assessment were to:

* Perform a current state evaluation of GridLink Utilities' OT environment and existing security measures.
* Identify security gaps within GridLink Utilities' OT environment.
* Map GridLink Utilities' OT network to the Purdue Model.
* Provide recommendations to address identified gaps and improve GridLink Utilities' OT security posture.
* Prioritize the discovered gaps.
* Recommend an implementation roadmap, including estimated duration and resources required to address the identified gaps.

A workshop was conducted with key stakeholders from the OT department, during which four distinct gaps were identified. These gaps have been risk-rated based on their likelihood and potential impact if exploited

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

The Following level of gaps were identified in the report: -

* A high-risk gap for not having multi-factor authentication in user connecting over VPN in OT domain.
* A high-risk related to end of life of software such as Window 2012 servers for which vendor specific patches were not fixed
* A high-risk gap related to insufficient network segmentation within the OT environment.
* A medium risk gap related to lack of system hardening of devices/ end-points in transformers and distribution centre.
* A risk-gap where due to improper security monitoring OT equipment’s within the stations are not send to the grid link SIEM systems for log monitoring and incidence response

## Current State Analysis

### **System Overview**

GridLink Utilities, a stalwart in the utility sector with a 75-year legacy, provides essential services to two medium-sized cities and their environs. The company operates 10 transformer stations and 50 distribution stations strategically located to ensure reliable power distribution across its service area.  
  
Company maintains a robust infrastructure that includes a primary and a backup control centre for their Operational Technology (OT) network. These centre’s are strategically positioned approximately 30 minutes apart, ensuring redundancy and continuous monitoring of critical operations.  
  
Gridlinks ‘s operational framework includes OT network which is dedicated to managing the physical process of the utility ensuring seamless operation of transformer and distribution stations.IT network in the framework separated for OT network using firewall and an Industrial DMZ , the IT network handles corporate function such as customer services , billing and regulatory compliance. Whereas the Wide area network connects the company’s control centre with transformer and distribution station, facilitating real- time monitoring and control.

The operation team also oversees the substantial infrastructure which includes 250 windows serves and 75 Linux servers distributed across the primary and backup centres. Moreover each station operated by GridLink is equipped with 1 or 2 workstation dedicated to managing OT devices and ensuring operational continuity.

GridLink Utilities relies on several key application essentials to it operations such as :-

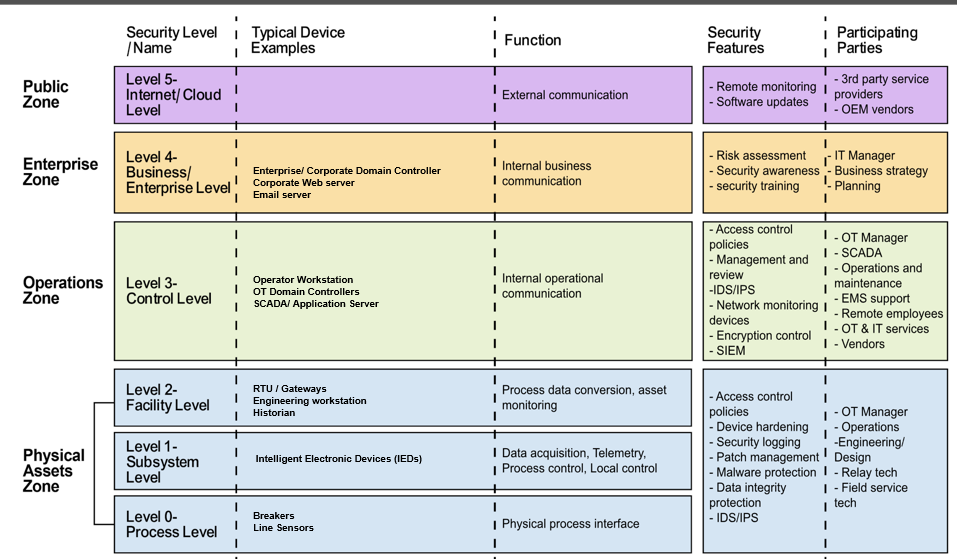
1. **Distribution Management System (DMS)**: Optimizes the efficiency, reliability and safety of the electrical distribution grid , ensuring consistent power delivery to customers.
2. **Energy Management System (EMS):** Monitors, controls, and optimizes the performance of the transmission system, enhancing grid stability and efficiency.
3. **Outage Management System (OMS):** Provides timely outage notifications to customers via automated phone calls, SMS messages, and a mobile application, enabling swift response and issue resolution.

### **Existing Security Measures**

GridLink Utilities has implemented robust security measures to protect their Operational Technology (OT) network and ensure the reliability of their utility services.

1. **Network Segmentation:** GridLink maintains a clear separation between their corporate and OT networks using an industrial Demilitarized Zone (DMZ) and next-generation firewalls. These firewalls include intrusion prevention/detection capabilities to monitor and control traffic between the OT and corporate networks.
2. **Intrusion Detection and Prevention**: Intrusion detection sensors (IDS) are deployed strategically across GridLink’s OT network to monitor traffic and detect potential security incidents promptly.
3. **Firewall Deployment**: Firewalls are deployed at all stations, with plans to upgrade to next-generation models that offer enhanced capabilities, including built-in intrusion detection. This upgrade strengthens the network's ability to defend against advanced threats.
4. **Internet Access Control**: Internet access within the OT network is strictly controlled. External-facing proxy servers manage access to specific websites, allowing only systems requiring vendor-provided updates to connect. No internet access is permitted from transformer and distribution stations, reducing exposure to external threats.
5. **Access Control Lists (ACLs) and VPN Access**: Access control lists (ACLs) on routers at stations control network traffic, ensuring only authorized communication. GridLink employs pairs of Internet-facing VPN appliances to securely facilitate remote access for employees and vendor partners into the OT network.
6. **Jump Box/Server Infrastructure**: GridLink utilizes a jump box/server infrastructure for secure management of OT systems from the corporate network, maintaining operational integrity and security.
7. **Patch Management:** Security patches are deployed monthly to servers and workstations across control centres and stations using an automated platform. Application-related patches for critical systems like the Distribution Management System (DMS) and Energy Management System (EMS) are applied quarterly.
8. **Vulnerability Management:** An agent-based automated vulnerability scanning platform conducts weekly scans on end-user workstations and servers in control centres. Network-based scanners are deployed monthly across strategic points on the OT network, ensuring comprehensive vulnerability assessment and management.
9. **Antivirus Protection:** GridLink has deployed antivirus software on all OT workstations in control centres, as well as on Windows and Linux servers, providing real-time protection against malware and other security threats.

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



## 

## Gap Analysis

### **[MFA not used]**

|  |  |
| --- | --- |
| **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **MFA not used** |
| **Description** | Single factor authentication was used by user connecting over VPN on OT domain |
| I**mpact** | **High**: the use of a terminal services farm in GridLink’s OT environment, where remote access authentication relies solely on a combination of Active Directory credentials and a one-time password (OTP) generated from a hardware token. This single-factor authentication approach presents a significant risk, as compromise of either the AD credentials or the OTP could grant unauthorized access to critical systems in control centres and downstream transformer stations. Such unauthorized access could lead to severe consequences, including operational disruptions, potential data breaches compromising sensitive customer information, and even sabotage affecting utility service reliability. The high impact stems from the potential for widespread operational downtime, regulatory compliance issues, and reputational damage, underscoring the critical need for implementing multi-factor authentication (MFA) to mitigate these risks effectively |
| **Probability** | **Medium**: VPN appliances used by operators to access control centre workstations remotely in GridLink’s OT environment. Authentication for these VPN appliances rely solely on Active Directory credentials without an additional requirement for a hardware token or OTP. While this approach provides basic security through encrypted connections and AD integration, it has medium probability. Compromise of AD credentials could grant unauthorized access to internal systems, potentially disrupting operational efficiency and exposing sensitive data. Implementing multi-factor authentication (MFA) for VPN access would enhance security by adding an additional layer of protection against unauthorized access attempts and credential theft |
| **Recommendations** | Implementing multi-factor authentication (MFA) across all remote access methods is crucial. This includes both the terminal services farm and VPN appliances used for remote operations. MFA adds an extra layer of security beyond username and password credentials, typically requiring a second form of authentication such as a hardware token OTP or biometric verification. This approach significantly reduces the likelihood of unauthorized access due to compromised credentials. Additionally, conducting regular security awareness training for employees to recognize and respond to phishing attacks and other social engineering tactics can further bolster defenses against potential threats. Regular monitoring of access logs and prompt response to any suspicious activities are also essential practices to maintain the security and integrity of GridLink's operational technology infrastructure |
| **NIST 800-82r3 Recommendations** | 6.2.1.4.4. Multi-Factor Authentication (page 123) [Guide to Operational Technology (OT) Security (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### 

### **[Insufficient Network Segmentation within OT environment]**

|  |  |
| --- | --- |
| **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Lack of network segmentation within OT environment** |
| **Description** | DMS and OMS are not segmented from other OT application |
| I**mpact** | High: GridLink’s Operational Technology (OT) network architecture includes the use of firewalls to separate OT and IT networks, which is critical for preventing cyber threats from traversing between these environments. The industrial demilitarized zone (iDMZ) is also of high importance, as it securely allows access to OT data from the corporate network, ensuring data integrity and security. Additionally, the need for further segmentation of the existing Distribution Management System (DMS) and Outage Management System (OMS) is high-impact due to their current vulnerability to lateral movement within the network, which could be exploited in a breach. Addressing these high-impact areas is crucial for maintaining the security and reliability of GridLink’s OT network |
| **Probability** | Medium: Company’s Operational Technology (OT) network architecture involves the ongoing segmentation of the OT network, such as the creation of a secure, firewalled zone for the recently upgraded Energy Management System (EMS). This segmentation enhances security by isolating critical systems, thereby helping to contain breaches and limit their impact. Additionally, the implementation of next-generation firewalls to separate the development environment from the production network is significant for preventing accidental or malicious changes from affecting live systems. However, until the Distribution Management System (DMS) and Outage Management System (OMS) are fully segmented, they remain at medium probability due to potential security gaps. |
| **Recommendations** | Strengthening firewall policies and regular audits between OT and IT networks should be prioritized to prevent cyber threats. Additionally, continuously monitor and update the industrial demilitarized zone (iDMZ) to ensure secure access to OT data from the corporate network. Implementing robust intrusion detection and prevention systems, along with regular security training for staff, will further fortify the network against potential threats and breaches. |
| **NIST 800-82r3 Recommendations** | 6.2.1.3. Network Segmentation and Isolation (PR.AC-5) page 102  [Guide to Operational Technology (OT) Security (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### 

### **[Lack of Security Hardening of devices /endpoints]**

|  |  |
| --- | --- |
| **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Lack of Security Hardening of devices /endpoints** |
| **Description** | Windows10 computer used within transformer and distribution centre are not securely hardened |
| I**mpact** | High: GridLink’s OT network architecture includes the implementation of firewalls between OT and IT networks, which is essential for preventing cyber threats from moving between these environments. The industrial demilitarized zone (iDMZ) also has a high impact, as it ensures secure access to OT data from the corporate network and maintains data integrity and security. Additionally, the lack of segmentation for the Distribution Management System (DMS) and Outage Management System (OMS) is a high-impact concern, as it poses significant security risks until the planned upgrade is completed. Addressing these areas is crucial for maintaining the overall security and reliability of GridLink's OT network. |
| **Probability** | Low: the redundant 10 Gbps dark fibre links connecting the primary and backup control centers, which enhance reliability and availability but have a relatively low impact on security. The creation of a secure firewalled zone for the recently upgraded Energy Management System (EMS) is important but has a lower impact compared to more critical security measures. Similarly, the separation of the development environment from the production network using next-generation firewalls is a good security practice but is considered low probabilityin comparison to the higher-priority areas that directly affect critical systems and data access |
| **Recommendations** | Enhance the segmentation of the Distribution Management System (DMS) and Outage Management System (OMS) to mitigate vulnerabilities. Strengthen and regularly audit firewall policies between OT and IT networks to ensure robust protection against cyber threats. Continuously monitor and update the industrial demilitarized zone (iDMZ) to maintain secure access to OT data from the corporate network. Additionally, ensure the redundant 10 Gbps dark fibre links are regularly tested for reliability. Implement comprehensive intrusion detection and prevention systems, coupled with regular security training for staff, to further safeguard the network against potential breaches and enhance overall security posture. |
| **NIST 800-82r3 Recommendations** | 5.2.4. Layer 4 – Hardware Security (page93) [Guide to Operational Technology (OT) Security (riseusercontent.com)](https://riseusercontent.com/rise/versions/1aaa8d5b-8e98-4c8d-9710-f65833791e02/o7HPBo8wxVKajAAR-NIST.SP.800-82r3.pdf) |

### **[ End of life system]**

|  |  |
| --- | --- |
| **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **End of life system** |
| **Description** | End of life system such as Window 2012 servers are still being used for which vendor “Microsoft” patch are not supported |
| I**mpact** | High: GridLink's OT network includes the use of unpatched Windows 2012 servers for the Distribution Management System (DMS), which have known vulnerabilities and are no longer supported by Microsoft, posing a significant security risk. Additionally, the non-hardened Windows 10 computers used in transformer and distribution stations, despite being protected by firewalls and lacking internet access, remain critically vulnerable if perimeter defenses are breached. These unaddressed vulnerabilities could lead to severe operational disruptions and data compromises, necessitating immediate attention and mitigation |
| **Probability** | Medium: the alignment of server builds with the Centre for Internet Security (CIS) Benchmarks, which enhances the security of Windows and Linux servers. The practice of conducting weekly vulnerability scans and applying monthly patches ensures that systems remain secure and up-to-date. Additionally, the use of firewalls at transformer and distribution stations provides a robust layer of protection, helping to mitigate risks associated with non-hardened systems at these critical locations |
| **Recommendations** | Transition from Windows 2012 servers to supported and secure systems. Immediate hardening of the Windows 10 computers at transformer and distribution stations is crucial, even with existing firewall protections. Strengthen the regular vulnerability scanning and patch management processes by considering more frequent scans and faster patch deployment cycles. Additionally, implement continuous monitoring and advanced threat detection systems to quickly identify and respond to potential security incidents |
| **NIST 800-82r3 Recommendations** | 5.2.5.2. Patching (page 94) [Guide to Operational Technology (OT) Security (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf) |

### **[Improper security monitoring]**

|  |  |
| --- | --- |
| **Note level of impact and change colour of this cell as appropriate (red or yellow)** | **Improper Security Monitoring** |
| **Description** | Logs from OT equipment’s within the stations are not send to the grid link SIEM systems for log monitoring and incidence response |
| I**mpact** | High: GridLink’s use of a Security Information and Event Management (SIEM) system to collect and analyze logs from network equipment, servers, and workstations in the control center is highly impactful for threat detection and response. The maintenance of distinct incident response plans for IT and OT environments, along with annual tabletop exercises and detailed playbooks, ensures robust preparedness and effective incident management. These practices collectively enhance GridLink’s security posture and ability to respond swiftly to potential threats. |
| **Probability** | High: The lack of current log monitoring from OT equipment in stations presents a high probability of undetected threats in these critical areas. This gap significantly increases the risk of successful attacks or unnoticed incidents within the OT environment. Although there are plans to implement OT log monitoring in the coming years, the existing vulnerability underscores the need for immediate action to mitigate potential risks and enhance comprehensive threat detection |
| **Recommendations** | The maintenance of distinct incident response plans for IT and OT environments, along with annual tabletop exercises and detailed playbooks, ensures robust preparedness and effective incident management. These practices collectively enhance GridLink’s security posture and ability to respond swiftly to potential threats. However, the lack of current log monitoring from OT equipment in stations presents a high probability of undetected threats in these critical areas, significantly increasing the risk of successful attacks or unnoticed incidents within the OT environment. To address this vulnerability, it is recommended that GridLink expedite the implementation of OT log monitoring and consider interim solutions to bridge the gap, such as more frequent manual log reviews and enhanced physical security measures at OT stations |
| **NIST 800-82r3 Recommendations** | 5.2.3.3. Network Monitoring (page 91) [Guide to Operational Technology (OT) Security (riseusercontent.com)](https://riseusercontent.com/rise/versions/1aaa8d5b-8e98-4c8d-9710-f65833791e02/o7HPBo8wxVKajAAR-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

<<Add your responses to the below template>>

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding (in priority order)** | **Risk Rating** | **Duration** | **Resources** |
| Implementing Multi- Factor Authentication | High | Short - Less than 3 months | Low - 1 resource |
| End of life | High | Short-Less than 3 months | Medium- 2 resources |
| Security monitoring | High | Medium3-6 months | Medium- 2 resources |
| Lack of System hardening | Medium | Medium3-6 months | Medium- 2 resources |
| Insufficient Network Segmentation | High | High - 6+ months | High - 3+ resources |

## Implementation Roadmap

A screenshot of a computer

Description automatically generated

## Conclusion

Over the past 12 months, the GridLink Utilities security team conducted an OT gap assessment encompassing the following areas:

* Evaluating the current state of GridLink Utilities' OT environment and existing security measures.
* Identifying security gaps within the OT environment.
* Mapping the OT network to Purdue model for better understanding and alignment
* Assessing and prioritizing the identified gaps from a risk perspective.
* Developing a recommended implementation roadmap, including estimated duration and required resources to address the gaps.

In conclusion, while GridLink Utilities has made significant progress in securing its Operational Technology environment, the identified gaps in this report underscore critical areas that require attention to effectively mitigate cybersecurity risks. By addressing these gaps, GridLink Utilities will not only adhere to industry best practices and regulatory standards but will also strengthen its resilience against evolving cybersecurity threats, ensuring a more secure and robust OT environment