GridLink Utilities

Operational Technology Gap Assessment

January 5th 2024

Frederic Gariepy
Montreal, QC, Canada

Table of contents

Executive Summary

This report represents findings from an Operational Technology Gap Assessment of GridLink Utilities OT environment. The goals of this assessment include:

- Performing a current state assessment of GridLink Utilities' OT environment and existing security measures.
- Mapping GridLink Utilities' OT network to the Purdue Model.
- Identification of security gaps in GridLink Utilities' Environment
- Providing recommendations to address identified gaps and to improve GridLink GridLink Utilities' 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 a number of key stakeholders from the OT department and 7 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	3	0

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

- A **critical risk** gap related to not having multi-factor authentication or remote access to the OT environment.

- A **high risk** gap related to end of life Windows servers with unpatched vulnerabilities.
- A **high risk** gap related to insufficient network segmentation of DMS and OMS.
- A **high risk** gap related to a lack of firewall between Public and Enterprise zones.

- A **medium risk** gap related to unprotected Windows systems in transformer & distribution stations.
- A **medium risk** gap related to limited security monitoring coverage over OT equipment.
- A **medium risk** gap related to unclear remote OT environment access policy.

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

Current State Analysis

System Overview

GridLink Utilities is a medium-sized company responsible for the transmission and distribution of electricity to service its customers in two relatively large cities and the surrounding area. It provides this utility service with its 10 transformer stations and 50 distribution stations.

The company operates a primary control centre and a backup control centre for their OT network which is approximately 30 minutes apart, and is used to manage the physical processes of the utility. The control center, transformers and distribution stations are connected via a wide-area network.

OT Operations team manages approximately 250 Windows servers and 75 Linux servers at their primary and backup control centres. Each station has 1 or 2 workstations that are used to manage the OT devices located at each of the stations.

Key applications of the OT environment includes:

- Distribution management system (DMS) that delivers power to their customers,
- Energy management system (EMS) which helps to monitor, control and optimize the performance of the transmission system, and
- Outage management system (OMS) which provides outage notifications to their customers through automated phone calls, SMS messages and a mobile application.

GridLink Utilities also operates a corporate IT network that is separated from the OT network by firewalls and an industrial DMZ which is used to securely move data between the corporate and OT networks.

Existing Security Measures

GridLink's corporate and OT networks are separated by an industrial demilitarized zone (iDMS), with next-generation firewalls (NGFW) controlling traffic between them. IDS sensors monitor OT network traffic in key areas, while legacy firewalls at stations are being replaced with NGFWs that have built-in IDS. OT network internet access is restricted to specific systems for vendor updates, and external-facing proxy servers control communications with websites. Internet access is prohibited for transformer and distribution stations, and ACLs on station routers manage network traffic in and out.

Internet-facing VPN appliances allow remote employee or vendor access to the OT network, while jump box/server infrastructure enables corporate network users to manage OT systems.

Security patches are applied monthly to servers and workstations in the control center and stations via an automated platform, with quarterly application patches for DMS and EMS. An agent-based vulnerability scanner scans end-user workstations and servers weekly, while network-based scanners scan OT network devices, routers, and switches monthly. Anti-virus software is deployed on Windows and Linux OT workstations and servers in control centers and stations.

Mapping of GridLink's Network to the Purdue Model

	Security Level	Devices	Function
Public Zone	Level 5 Internet Level	Email Server	External Communication
Enterprise Zone	Level 4 Enterprise Level	Corporate Web Server, Enterprise Domain Controllers	Internal Communication
		Industrial Demilitarized Zone (iDMZ)	
Operations Zone	Level 3 Control Level	Historian Servers, Engineering Workstations, Operator Workstation SCADA / Application Servers, OT Domain Controllers	Internal Operations / Communications
		Legacy and Next Gen Firewalls	
Physical Assets Zone	Level 2 Facility Level	Remote Terminal Units (RTUs) Gateways	Local control, Asset Monitoring, Process Data
	Level 1 Subsystem Level	Intelligent Electronics Devices (IEDs)	Process Control, Local control, Telemetry, Data Acquisition
	Level 0 Process Level	Breakers, Line Sensors	Physical Process Interface

Gap Analysis

C-01: Absence of MFA for VPN remote access to OT environment

Critical	**Absence of MFA for VPN remote access to OT environment.**
Description	Internet facing VPN appliances giving operators remote access to OT control centers relies solely on OT Active Directory authentication. This creates a single point of failure.If credentials are compromised, network based attackers could gain access to the OT environment and ultimately compromise it altogether.
Impact	**Very High**: The impact of unauthorized access to the OT environment and further downstream critical OT systems could 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. Attacks may use tactics such as brute forcing, phishing or other network vector attack tactics to compromise credentials. There is a high chance that if an attacker gained access to the IT network, they'd try to access the OT network using found credentials.
Recommendations	Multi-factor authentication (MFA) should be enabled for VPN remote access to the OT environment. MFA can be safely applied to most OT/ICS environments. As pointed out in the SANS 5 Critical Controls article, MFA has been shown to significantly reduce the number of adversary attack paths. MFA is a control measure proven to restrict access and protect from unauthorized remote access.
NIST 800-82r3 Recommendations	Section 6.2.1.4.4 Multi-Factor Authentication

H-01: End of Life (EOL) Windows 2012 Servers with Unpatched Vulnerabilities

High	**EOL Windows 2012 Servers with Unpatched Vulnerabilities**
Description	Multiple EOL Windows 2012 servers running the Distribution Management System (DMS) have known vulnerabilities and cannot be patched due to lack of vendor support, creating significant security exposure until next year's planned upgrade.
I**mpact**	**High**: EOL servers in DMS infrastructure could be exploited and compromised. Attackers with DMS control could severely impact operations in electric distribution.
Probability	**High**: End-of-life systems with known vulnerabilities are prime targets for attackers. Without security patches, exploitation risk increases over time.
Recommendations	Accelerate DMS upgrade timeline. Along regular vulnerability scanning, implement additional compensating control of network segmentation or isolation of the vulnerable components.
NIST 800-82r3 Recommendations	6.2.11. Flaw Remediation and Patch Management 6.2.1.3. Network Segmentation and Isolation

H-02: Insufficient Network Segmentation of DMS and OMS

High	**Insufficient Network Segmentation of distribution management system (DMS) and the Outage Management System (OMS)**.
Description	Existing DMS and OMS both reside in the production zone without proper segmentation from other OT applications. This weakness is known and meant to be addressed in the current year. The lack of segmentation weakens the organization's defence-in-depth, and increases the overall likelihood of successful attacks.
I**mpact**	**High**: Without network segmentation, compromise of one system can lead to lateral movement in the network and result in the compromise of both systems. Impact to these systems being compromised may lead to service disruption and impact customer communications during outages.
Probability	**Medium**: Although existing network security controls may dampen intrusion attempts, the lack of segmentation increases the overall likelihood of an attacker with production access to move laterally within the network and compromise both systems.
Recommendations	Accelerate planned network segmentation. Deploy internal firewalls and monitor traffic logs between segments.
NIST 800-82r3 Recommendations	E.1. Network Segmentation and Isolation

H-03: Lack of firewall between Public and Enterprise zones

High	**Lack of firewall between Public and Enterprise zones**
Description	Review of the existing security measures reveals a lack of a firewall between public facing Layer 5 (Internet Level) and IT enterprise Layer 4 (Enterprise Level).
I**mpact**	**High**: Without firewall between the public facing layer and internal IT layer, the organization's IT systems face an increased exposure to direct attacks from the internet. Attacks may lead to unauthorized access, malware propagation, data breaches or IT system compromises.
Probability	**Medium**: Although the organization uses external facing proxies, public facing systems are attack surfaces which receive constant probing from attacks. Without a firewall attackers have a direct path to the Enterprise Level and can exploit its systems if there is a vulnerability exposed.
Recommendations	Deploy a dedicated firewall to segment the public facing (Level 5) and enterprise network (Layer 4). Enforce access controls, monitor traffic and deploy intrusion prevention or intrusion detection systems.
NIST 800-82r3 Recommendations	E.1.1. Firewalls E.2.1. Centralized Logging

M-01: Unprotected Windows 10 Systems in transformer & distribution stations

Medium	**Unprotected Windows 10 Systems in transformer & distribution stations**
Description	Windows 10 computers used for local control in transformer and distribution stations are not hardened, with security justified solely by firewall access controls and lack of Internet access. This defense-in-depth weakness could allow unauthorized access if network perimeter controls or physical access are compromised.
I**mpact**	**High**: Unhardened systems controlling critical infrastructure components could be compromised, potentially leading to loss of control over transformer and distribution stations, service disruptions, and safety risks.
Probability	**Low**: While station firewalls provide protection, and disconnection from the internet eliminates network attack vectors, the lack of system hardening creates a significant vulnerability if perimeter controls (network or physical) are bypassed. Attackers who gain initial access could more easily compromise these systems and move laterally.
Recommendations	Implement system hardening on all Windows 10 systems in stations.
NIST 800-82r3 Recommendations	5.2.5. Layer 5 – Software Security

M-02: Limited Security Monitoring Coverage over OT equipment

Medium	**Limited Security Monitoring Coverage over OT equipment**
Description	Security Operations Center does not receive or monitor logs from *some* OT equipment in stations, creating visibility gaps that could allow threats to go undetected.
I**mpact**	**Medium:** Lack of monitoring coverage for station equipment limits threat detection capabilities and incident response effectiveness for the portion of the OT environment which does not transmit logs.
Probability	**Medium**: While there is existing monitoring for network equipment, servers and workstations in the control centre, the gap in station coverage creates opportunities for attackers to operate undetected in un-monitored segments of the network.
Recommendations	Accelerate planned implementation of station equipment logging timeline. Define and implement logging requirements for all OT assets.
NIST 800-82r3 Recommendations	E.2.1. Centralized Logging

M-03: Unclear BYOD policy for remote OT environment access

Medium	**Unclear personal device (Bring your own device, BYOD) policy for remote OT environment access**.
Description	There is no clear policy on the use of personal devices used in the remote VPN access to the OT environment. The system implemented during the pandemic does not indicate whether corporate devices are required or personal devices are allowed to access the OT environment remotely.
I**mpact**	**Medium**: Unmanaged use of personal devices to connect into the internal network brings with potential threats such as malware, compliance issues, and unauthorized access.
Probability	**Medium**: Without clear policies or controls on allowed devices used for remote access, it is likely that some personal devices are or were used for remote access into the OT environment, especially during the pandemic when transition to work-from-home developed rapidly.
Recommendations	Develop and implement clear policies for remote access. Require the use of managed devices for remote OT access or allow for personal devices with device management capabilities. Enforce compliance of remote access policies at VPN endpoint connections.
NIST 800-82r3 Recommendations	E.3.6. Remote Access 6.2.3. Data Security (PR.DS)

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:

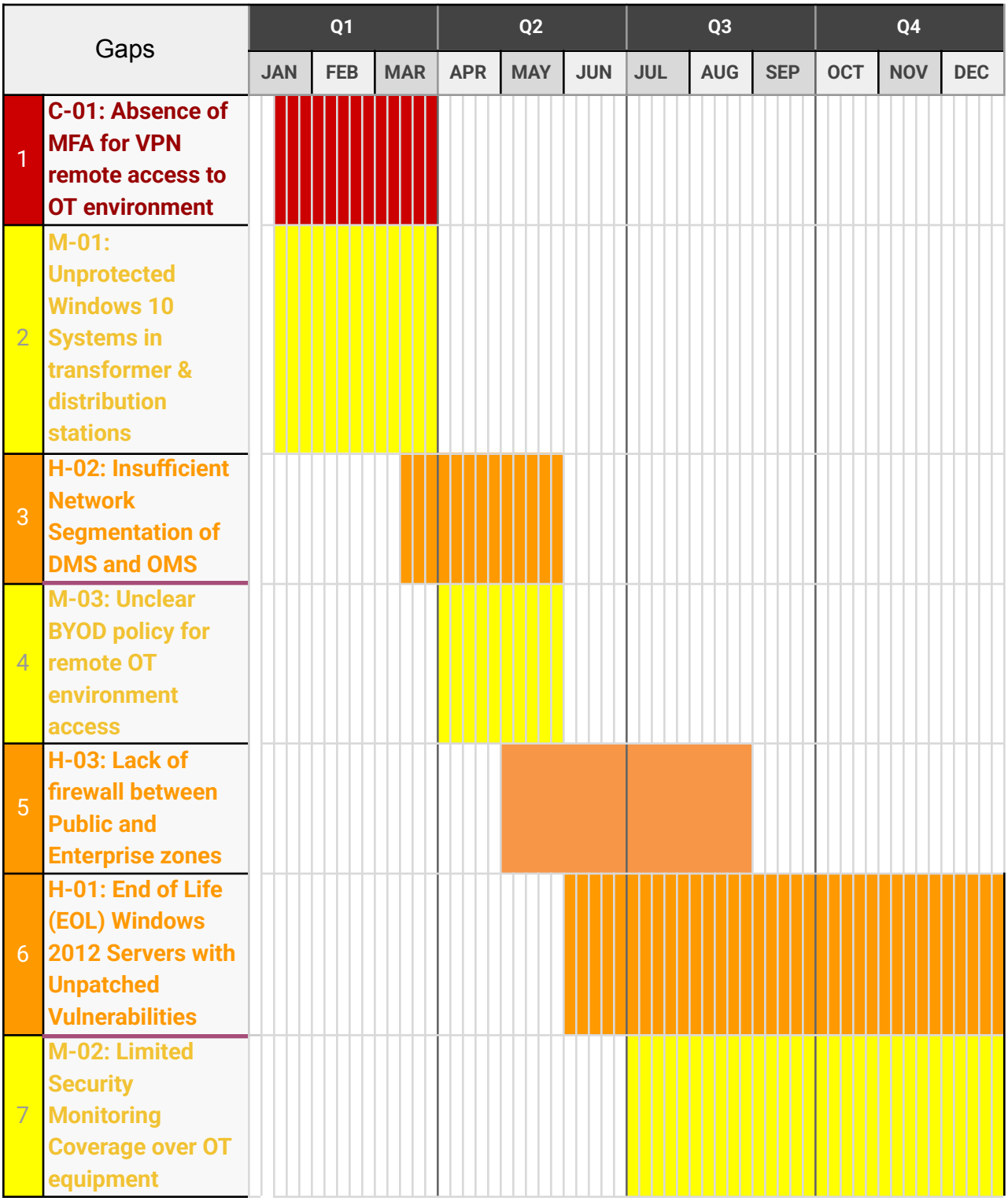
1. **Low**: Minimal impact, easily manageable.
2. **Medium**: Some impact, manageable with some effort.
3. **High**: Significant impact, requires substantial resources to manage.
4. **Critical**: Severe impact, challenging to manage and could cause significant disruption.

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

Prioritization of Findings

Finding (in priority order)	Risk Rating	Duration	Resources
C-01: Absence of MFA for VPN remote access to OT environment	**Critical**	**Low** (less than 3 months)	**Low** (1 resource, Multiple accounts)
H-01: End of Life (EOL) Windows 2012 Servers with Unpatched Vulnerabilities	**High**	**High** - 6+ months	**High** (multiple resources)
H-02: Insufficient Network Segmentation of DMS and OMS	**High**	**Low** (less than 3 months)	**Medium** (2 resources)
H-03: Lack of firewall between Public and Enterprise zones	**High**	**Medium** (3 - 6 months)	**High** (multiple resources)
M-01: Unprotected Windows 10 Systems in transformer & distribution stations	**Medium**	**Low** (less than 3 months)	**High** (multiple resources)
M-02: Limited Security Monitoring Coverage over OT equipment	**Medium**	**High** - 6+ months	**Medium** (some OT resources)
M-03: Unclear BYOD policy for remote OT environment access	**Medium**	**Low** (less than 3 months)	**Low** (1 resource)

Implementation Roadmap



Conclusion

The GridLink Utilities security team has performed an OT gap assessment.
The following areas were in scope for the assessment.

- A current state assessment of GridLink Utilities' OT environment and existing security measures.
- Mapping GridLink Utilities' OT network to the Purdue Model
- Identification of security gaps in GridLink Utilities' OT environment
- Gaps in GridLink Utilities' 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 Utilities is actively making 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 and strengthen its own goal commitments.