Cyber Security Related Supplemental Information for Monitoring & Diagnostics (M&D) Products

Date: May 11, 2021

TILs- 1777, 1881 are archived/obsoleted and users are recommended to refer TIL-2086 and GEH-6839 for GE recommendations related to Cyber Security guidelines, Secure Deployment of GE products and offerings. These does not specifically cover Monitoring & Diagnostics (M&D) OSM or RSG, so this document is intended to provide some guidelines on UDH Firewall to be used with OSM and the status of Lockbox.

Recommendations

1. **Install UDH network traffic filtering equipment capable of checking and removing all non-control related traffic**

For sites with OSM, GE recommends the application of a network traffic filter between the UDH network and OSM. This device will block all non-control related traffic from entering the UDH from an OSM. This can provide an additional layer of security within the plant perimeter.

S3C (Support Segment Security Connector)

The M&D platform is configured to provide customers with a secured data connection helping them to achieve their cyber security compliance requirements. The basis for network security comes down to permitting only what is necessary to maintain the performance and operation of required services. GE offers the S3C with an auditable, defensive position to facilitate this. However, you are recommended to provide your own UDH Firewall consistent with the rest of your security perimeter implementation. If this is being done and the additional functionality of Deep Packet Inspection is required, GE can provide SNORT (or similar) ruleset to perform this functionality.

Perimeter Protection: Like an Internet Firewall, the S3C is inserted at the edge of your electronic security perimeter on your Unit Data Highway (UDH). It serves as the gateway for ALL traffic between your M&D on-site monitoring equipment and devices within your control system network. The S3C inspects and filters all incoming or outgoing communications required for monitoring or remote tuning of your assets.

Controlled Communication: Only the network communications that explicitly match those permitted by our custom policies will traverse through the S3C, all other communications should be denied and then captured for your review.

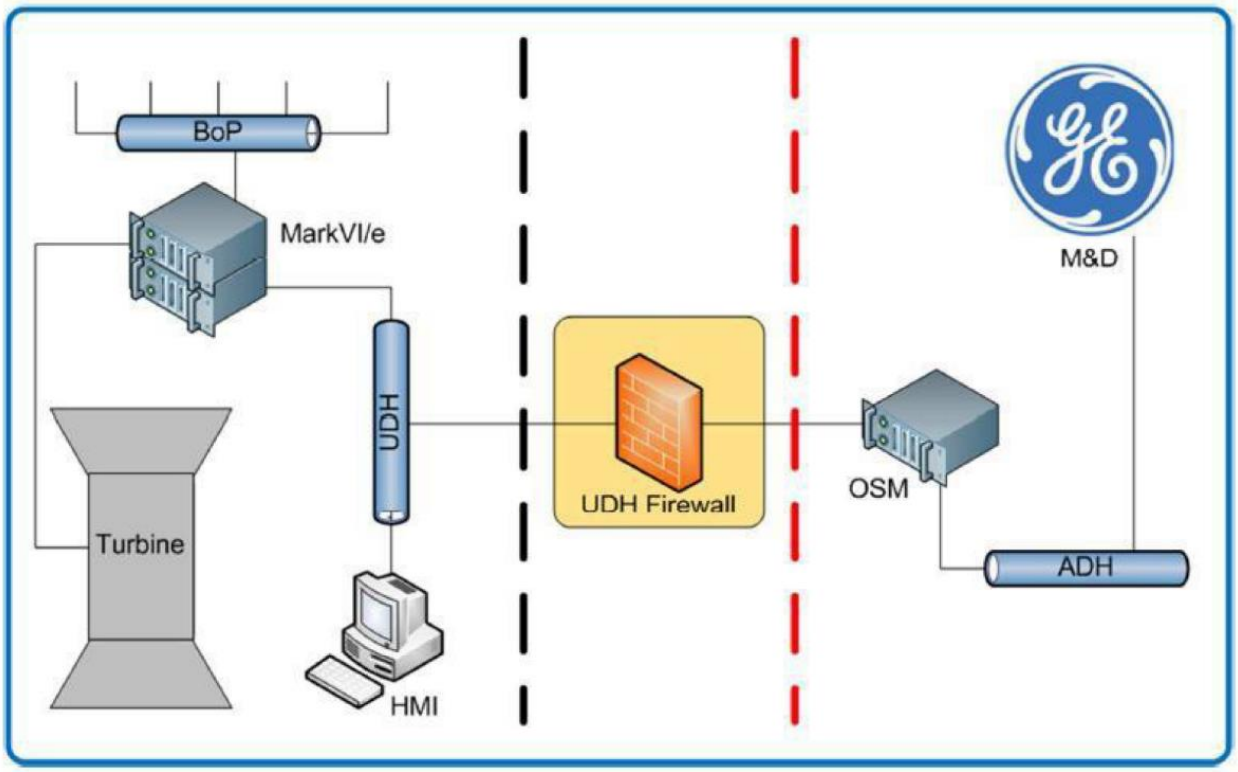

Figure 1: S3C (UDH Firewall) shown inserted between OSM and the UDH

Tiered Inspection: The S3C inspects communications passing between interfaces and evaluates it against multiple criteria established in custom policies specifically tailored for M&D services. Any traffic that does not conform to ALL the criteria defined within a policy is denied access to its network target.

Permitted Services: Only communications necessary for legitimate functionality and operation of approved resources should be permitted. The S3C provides exactly this level of control. GE security engineers have systematically identified all required communication ports and protocols for M&D services for required functions with their associated resources. These have been documented and authored into the S3C policies to permit these communications.

Security Management: M&D is committed to providing a solution that fits into your enterprise security management. Embedding industry best practices for security management into the S3C allows for a seamless integration into your existing infrastructure and technology administration. We provide security that allows vendor transparency and maintains your independence from external security policies.

Configuration: Some site-specific configuration will be required.

Ordering: Because some site-specific setup and configuration is required GE's S3C devices should be ordered via the upgrade process so that the correct site-specific parts and configuration can be installed.

Management Features: Independent Management Interface, event Logging, traffic Logging, SNMP Alerts.

2. **Maintain any remote service lock boxes in the OFF position when not in use**

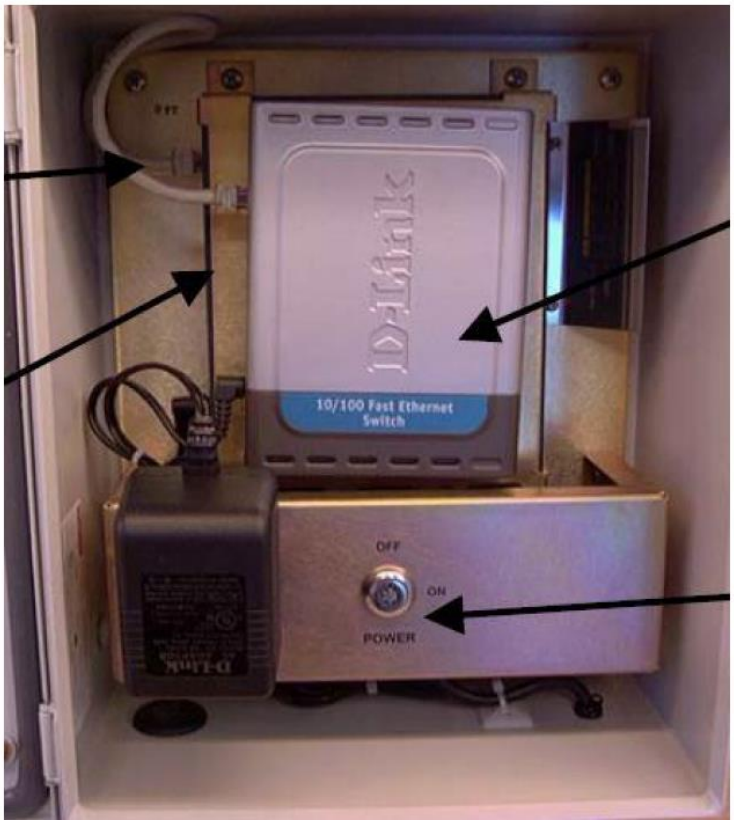

Figure 2: Example Remote Connection Lockbox

The lockbox is a device that can power up/ down the router which enables access to the HMI via the OSM or in some cases the RSG. The lockbox physically isolates the power to the router that enables this communication pathway and access to both the box and the key should be controlled. To reduce disruption to maintenance activity, there should be a secure, well defined process to get this turned on or off as required. When no pre-arranged tuning or diagnostic activity is in progress, it should be in the locked off position.

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.