GEK121594
Aug. 2018

GE Power

Cyber Security Maintenance Requirements for Industrial Controls

These instructions do not purport to cover all details or variations in equipment nor to provide for every possible contingency to be met in connection with installation, operation or maintenance. Should further information be desired or should particular problems arise which are not covered sufficiently for the purchaser's purposes the matter should be referred to General Electric Company. These instructions contain proprietary information of General Electric Company, and are furnished to its customer solely to assist that customer in the installation, testing, operation, and/or maintenance of the equipment described. This document shall not be reproduced in whole or in part nor shall its contents be disclosed to any third party without the written approval of General Electric Company.

The following notices will be found throughout this publication. It is important that the significance of each is thoroughly understood by those using this document. The definitions are as follows:

NOTE

Highlights an essential element of a procedure to ensure correctness

CAUTION

Indicates a potentially hazardous situation, which, if not avoided, could result in minor or moderate injury or equipment damage

WARNING

INDICATES A POTENTIALLY HAZARDOUS SITUATION, WHICH, IF NOT AVOIDED, COULD RESULT IN DEATH OR SERIOUS INJURY

*****DANGER*****

INDICATES AN IMMINENTLY HAZARDOUS SITUATION, WHICH, IF NOT AVOIDED WILL RESULT IN DEATH OR SERIOUS INJURY

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

With the benefits of productivity, reliability and economics driving the inevitability of digital connectivity; critical infrastructure owner/operators are at exponentially increasing risk of cyber-attack. Protecting power generation assets from the threats of cyber-attack in a digitally connected world begins with secure design, secure products and on-going maintenance programs. In addition to cyber resiliency, a sustainable security program increases operational reliability of the assets under control and can increase equipment lifecycle.

This document provides background and requirements for maintaining cyber security equipment as part of the industrial control systems.

II. MAINTENANCE REQUIREMENTS

The following highlight areas of focus in understanding, maintaining and monitoring systems to defend against the regulatory and risk landscape;

A. Network Design

Segregation of networks increases cyber resiliency by creating layers of protection. Through monitoring and control of the digital information that passes between these network layers, the system is inherently more secure. Further, this creates defined segmentation lines allowing different privilege levels and the creation of an Electronic Security Perimeter (ESP) which is a regulatory requirement. Additionally, this design provides controlled access points beyond the individual controller to include the OSM, customer enterprise network, 3rd party and other customer configured equipment.

GE provides Network*ST 4.0™ as standard with all new Mark*VIe controls. This product is an integration of routers, firewalls and cabling that make up the network design both within and outside the ESP. Proper design and connection points increases cyber resiliency and positions for complaint application.

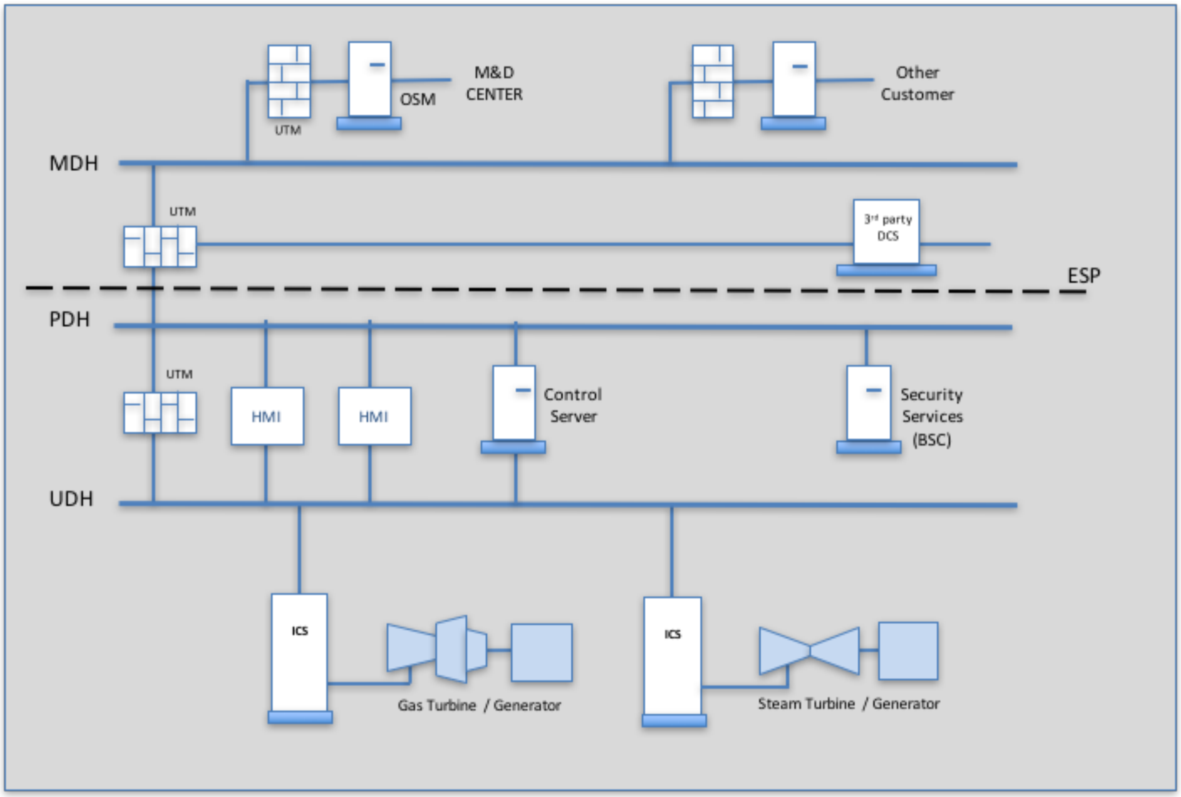

Figure 1. GT/ST Mark*VIe Reference Network Architecture

B. Patching & Anti-Virus Management

Scheduled patch updates are required to keep the OEM equipment protected from cyber threats and performing to its design intent. This is the owner/operator responsibility to remain current on patch versions, evaluating and testing OEM releases and maintain current product versions. Regularly updating logging and event management and backup keep systems are part of a cyber defense and recovery strategy. Patching usually refers to the end-point solution (HMI's) that run Microsoft operating systems and are vulnerable to similar malware as IT applications.

GE end-points and supporting equipment are shipped from our suppliers at current patch levels. With the long cycle nature of our business and the rapid intelligence on cyber risk, it is likely end-points will need to be updated again during the field commissioning before COD. From COD onward it is customer responsibility to manage and track updates status. GE provides services through 3rd party providers to aid customer in a patch management strategy.

C. Network Monitoring

Network traffic types and patterns in the network can be an early indicator of unauthorized activity in a digital control system. Early detection of anomalous network traffic can indicate cyber intrusion and initiate proactive measures by the owner/operator in preserving or recovering asset operation. This owner/operator process must complement device technology, system architecture and maintenance programs within the installed system, with a compressive plan at the asset, plant and enterprise level.

GE provides Baseline Security (BSC) with new Mark*VIe control systems as an option. Features included but not limited to; Log Aggregation, System Backup & Recovery, Configuration Management / Configuration Persistence & User Policy Enforcement and Network Device Management. These features aid the owner/operator in compliance and reporting functions often required for corporate policies or regional compliance. Also available with BSC is subscription services providing regular intelligence reporting including patch availability reporting and vulnerability management reporting. When selected as an option, BSC is packaged with the OEM control equipment.

D. Regulatory Compliance

Compliance is an owner/operator responsibility with the OEM providing equipment and system architecture capability for complaint program and operations. GE designs and builds its electronic control systems to facilitate the owner/operators strategy for compliance to regulatory standards. Failure to install and maintain these systems will increase cyber risk exposure and can lead to non-conformance with fines and penalties. GE provides controllers, network gear, reference architecture and services designed to integrate systems into a comprehensive owner/operator strategy for risk reduction and compliance.

GE provides a reference architecture design with customer review during the customer kick off, release and engineering meetings as part of a requisition release. Also available are GE Cyber Health Check Services for post COD commissioned sites. Contact your local account executive for options.

E. Lifecycle Management

Hardware and software devices have a finite lifecycle with recommended upgrade path often associated with cyber resiliency and discovered vulnerabilities. GE control systems are an integration of original and OEM products. As part of an owner/operator program, asset inventory and lifecycle tracking need to part of a regular maintenance program. As devices or software reach end of life, a risk assessment must be performed to evaluate system risk and balance with long term planning cycles on upgrades, patching or other mitigating controls.

III. APPLICABLE REFERENCE DOCUMENTATION

• Baseline Security Standard	MLI-A408
• Network Topology Drawing	MLI-4108
• Secure Deployment Guide	GEH-6839
• Product Security in Digital Age	GEA-32738

IV. TERMINOLOGY

BOP – Balance of Plant

BSC – Baseline security center

COD – commercial operation date

DiD – Defense in depth – multiple layers of security controls implemented through network segregation

End-Point Solution – at “the end” of the network, typically an operator interface or workstation

ESP – Electronic security perimeter

HMI – human machine interface

ICS – Industrial control system

Mark VIe - GE Automation & Control Product

M&D – Monitoring and diagnostics

Network*ST 4.0 – GE Automation & Control Product

OEM – original equipment manufacturer

OSM – On Site Monitoring

GE Power
General Electric Company
www.gepower.com