GE Power
TIL 2086
11 JULY 2018
Compliance Category - **M**
Timing Code - **6**

# TECHNICAL INFORMATION LETTER

## CONTROL SYSTEM LIFETIME LIMITATION DUE TO CYBER RISK

### APPLICATION

All turbines and equipment with Mark* V or later GE control systems.

*Trademark of General Electric Company

### PURPOSE

To provide guidance that reduces system cyber attack exposure due to component end of life (EoL), obsolescence, and failure to apply firmware/software patches.

### COMPLIANCE CATEGORY

| | |
|---|---|
| **M - Maintenance** | Identifies maintenance guidelines or best practices for reliable equipment operation. |
| **C - Compliance Required** | Identifies the need for action to correct a condition that, if left uncorrected, may result in reduced equipment reliability or efficiency. Compliance may be required within a specific operating time. |
| **A - Alert** | Failure to comply with the TIL could result in equipment damage or facility damage. Compliance is mandated within a specific operating time. |
| **S - Safety** | Failure to comply with this TIL could result in personal injury. Compliance is mandated within a specific operating time. |

### TIMING CODE

| | |
|---|---|
| **1** | Prior to Unit Startup / Prior to Continued Operation (forced outage condition) |
| **2** | At First Opportunity (next shutdown) |
| **3** | Prior to Operation of Affected System |
| **4** | At First Exposure of Component |
| **5** | At Scheduled Component Part Repair or Replacement. |
| **6** | Next Scheduled Outage |

## BACKGROUND DISCUSSION

Modern GE turbine control systems employ Ethernet-based computer networks to provide paths for data flow between controllers, human machine interfaces (HMIs), input/output devices, time devices, historians, etc. The HMI and historians have user interfaces between the human operator and control system. HMIs are used to monitor and provide operator commands to the control system. Historians are used as data archival systems for storage and display of power plant data. Many plants also have additional network devices like an on site monitor (OSM), remote service gateway (RSG), time device, and/or third party devices. There are generally three separate Ethernet-based networks found in modern GE turbine control systems. Figure 1 shows a basic plant network configuration.

IONet - transports data between the controller and input/output circuit boards.

UDH (unit data highway) - transports data and commands between the controller panels and the HMIs, OSM, etc.

PDH (plant data highway) - transports data between the HMIs and the distributed control system (DCS), etc.

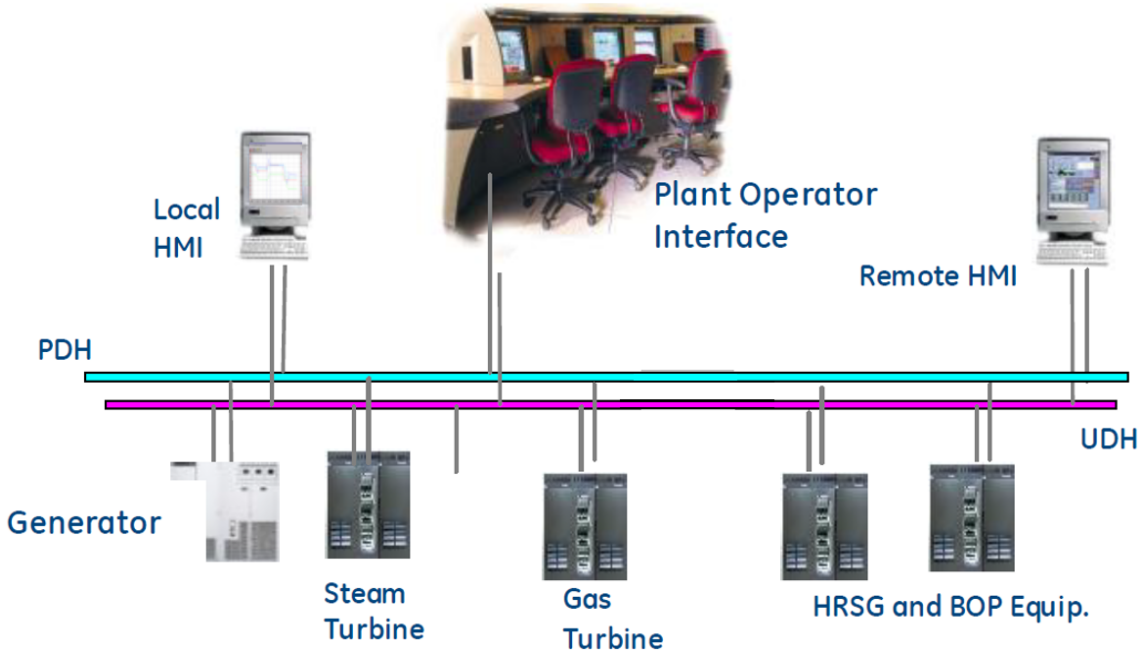


**Figure 1: Typical, basic plant network configuration**

A power plant's vulnerability to cyber attacks increases as a result of unknown (zero-day) and known vulnerabilities. GE control system networks are an integration of other original equipment manufacturer (OEM) components such as network switches, Microsoft* Windows-based HMIs or On Site Monitoring (OSM) computers, time devices, etc. Each component typically has a finite life or recommended upgrade cycle from the OEM. The component OEMs often mitigate vulnerabilities through product updates in the form of patches and signatures.

*Trademark of Microsoft Corporation

Any of these component manufacturers may also publish an end of life (EoL) communication or update their recommended obsolescence interval due to technology maturity. Therefore, routine control system network cyber security assessments are important to reduce cyber attack exposure.

An effective cyber security plan uses a combination of robust maintenance procedures, employee training/awareness, and up to date technology.

## RECOMMENDATIONS

GE recommends adopting a cyber security risk management program which includes proactive assessment based on the plant's inventory of control system network components. This includes monitoring and planning for near and long-term actions to protect your system from component EoL and cyber risks.

Suggested actions include basic inspection of control component version for both hardware and software, including patching status and OEM EoL plans for component lifecycle. This status needs to be evaluated against the user's corporate governance and risk tolerance. At times, an individual EoL component may be an acceptable risk based on the total system configuration, but acknowledging that component and making longer term plans to upgrade should be planned. GE can support your specific operational technology cyber needs through a variety of products and services. Please contact your GE representative for details.

In addition, GE also monitors supplier EoL notifications and vulnerabilities and periodically documents known cyber communications in the My Dashboard internet portal. As OEM communications typically roll out continuously over the component life, not all cyber vulnerabilities are documented in this portal. This portal also oftentimes provides early background and preliminary recommendations for exploited cyber threats (i.e. WannaCry ransomware). Contact your local GE representative for assistance in obtaining a GE single sign on (SSO) number and obtaining access to the My Dashboard internet portal.

Due to the variation in customer networks and frequency of OEM patch releases, GE cannot validate all firmware or software patch updates. As a result, the following general guidelines should be considered.

- Take an image backup of the device to be updated (HMI, historian, etc.)
- Test the applicable OEM's software/firmware update. In rare instances, updates may impact the device's function. As such, new updates should be tested within a testbed platform before installing into a production environment. If a testbed is not feasible, apply update to only one or two devices before being propagated to the entire plant.
- Install the applicable OEM's software/firmware update
- Update the antivirus definitions/software

This TIL is considered complete when proactive, periodic control system component assessments have been added to periodic maintenance plans and when necessary, updates to the components are planned/executed.

## PLANNING INFORMATION

### Compliance

• Compliance Category: **M**
• Timing Code: **6**

### Manpower Skills

Varies based on component assessment needs, but routine assessments are recommended.

### Reference Documents

GEH-6839

TIL 1777

TIL 1789

TIL 1881-R2

TIL 1951

## TIL DISPOSITION

Disposition of TILs should be entered in local records and also in GE Power ServiceNow. Follow the below instructions for entering the disposition record;

- Log into the Power ServiceNow at https://gepowerpac.service-now.com/til_new/ using your GE SSO number and password.
- Select "TIL Disposition".
- Click on the TIL for the serial number you want to update.
- Choose the most appropriate "Disposition Status" and enter "Disposition Notes".
- Click "Save".

**Contact your local GE Services representative for assistance or for additional information**