WorkstationST*
Device Manager Gateway
Instruction Guide

June 2020
These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and GE makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that GE may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the GE products referenced herein.

GE may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Public Information – This document contains non-sensitive information approved for public disclosure.

GE provides the following document and the information included therein as is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

For further assistance or technical information, contact the nearest GE Sales or Service Office, or an authorized GE Sales Representative.

Revised: June 2020
Issued: May 2011


* Indicates a trademark of General Electric Company and/or its subsidiaries.
All other trademarks are the property of their respective owners.

We would appreciate your feedback about our documentation.
Please send comments or suggestions to controls.doc@ge.com

Public Information
### Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td><strong>Overview</strong></td>
<td>Added Honeywell FDM to Third-party Asset Management Support table</td>
</tr>
<tr>
<td></td>
<td><strong>Third-party Asset Management Software</strong></td>
<td>Added Honeywell FDM</td>
</tr>
<tr>
<td></td>
<td><strong>Configure HART Communications in Honeywell Field Device Manager (FDM)</strong></td>
<td>Added new section</td>
</tr>
<tr>
<td></td>
<td><strong>Appendix J Add HART Multiplexers to Honeywell Field Device Manager (FDM)</strong></td>
<td>Added new appendix</td>
</tr>
<tr>
<td></td>
<td><strong>Appendix K Honeywell Field Device Manager (FDM) Configuration</strong></td>
<td>Added new appendix</td>
</tr>
<tr>
<td>H</td>
<td><strong>Secure System Operation</strong></td>
<td>Added reference to Control Server — Domain Services Maintenance Guide (GEH-6845), the section Create and Deploy SDI Certificates for WorkstationST Features</td>
</tr>
<tr>
<td>G</td>
<td><strong>HART Messages</strong></td>
<td>Added three additional I/O packs that support HART devices: YSIL, PUAA, and YHRA, and updated the figures to reflect all I/O packs that support HART devices</td>
</tr>
<tr>
<td></td>
<td><strong>FDT Frame Applications</strong></td>
<td>Changed references to PHRA I/O pack to generic term I/O packs to include all I/O packs that support HART devices</td>
</tr>
</tbody>
</table>

### Acronyms and Abbreviations

- **DM**: Device Manager
- **DME**: Device Manager Essentials
- **DMG**: Device Manager Gateway
- **FDM**: Field Device Manager
- **FDT**: Field Device Tool
- **HMI**: Human-Machine Interface
- **MUX**: Multiplexer
- **OS**: Operating System
- **PDH**: Plant Data Highway
- **UDH**: Unit Data Highway
**Safety Symbol Legend**

---

**Warning**

Indicates a procedure or condition that, if not strictly observed, could result in personal injury or death.

---

**Caution**

Indicates a procedure or condition that, if not strictly observed, could result in damage to or destruction of equipment.

---

**Attention**

Indicates a procedure or condition that should be strictly followed to improve these applications.
**Control System Warnings**

- **Warning**
  To prevent personal injury or damage to equipment, follow all equipment safety procedures, Lockout Tagout (LOTO), and site safety procedures as indicated by Employee Health and Safety (EHS) guidelines.

- **Warning**
  This equipment contains a potential hazard of electric shock, burn, or death. Only personnel who are adequately trained and thoroughly familiar with the equipment and the instructions should install, operate, or maintain this equipment.

- **Warning**
  Isolation of test equipment from the equipment under test presents potential electrical hazards. If the test equipment cannot be grounded to the equipment under test, the test equipment’s case must be shielded to prevent contact by personnel.
  
  To minimize hazard of electrical shock or burn, approved grounding practices and procedures must be strictly followed.

- **Warning**
  To prevent personal injury or equipment damage caused by equipment malfunction, only adequately trained personnel should modify any programmable machine.

- **Warning**
  Always ensure that applicable standards and regulations are followed and only properly certified equipment is used as a critical component of a safety system. Never assume that the Human-machine Interface (HMI) or the operator will close a safety critical control loop.
Contents

1 Overview......................................................................................................................................................... 9

2 Third-party Asset Management Software .................................................................................................. 11
   2.1 FOUNDATION Fieldbus Messages ........................................................................................................... 11
   2.2 HART Messages ....................................................................................................................................... 14
   2.3 Configuration (Quick Start) ................................................................................................................... 15
      2.3.1 Enable the Device Manager Gateway ............................................................................................... 16
      2.3.2 Enable the Foundation Fieldbus Message Server ........................................................................... 17
      2.3.3 Enable the HART Message Server ................................................................................................. 20
      2.3.4 Configure HART Communications in Emerson™ AMS ............................................................... 22
      2.3.5 Configure HART Communications in Yokogawa Plant Resource Management (PRM) ........... 23
      2.3.6 Configure HART Communications in Honeywell Field Device Manager (FDM) ...................... 24
      2.3.7 Configuration Changes and Management ...................................................................................... 26
      2.3.8 FOUNDATION Fieldbus Configuration Changes ......................................................................... 28
      2.3.9 HART Configuration Changes ....................................................................................................... 30
   2.4 Monitor Status ......................................................................................................................................... 31
      2.4.1 WorkstationST Status of Features .................................................................................................. 31
      2.4.2 Windows Event Viewer ............................................................................................................... 32
      2.4.3 Device Manager Gateway Status Viewer ........................................................................................ 32
   2.5 Systems with Multiple UDH Networks .................................................................................................. 39
      2.5.1 Common Asset Management System ............................................................................................ 41
   2.6 Performance and Limitations ................................................................................................................ 45
      2.6.1 Device Manager Gateway .............................................................................................................. 45
      2.6.2 Asset Management System ....................................................................................................... 45
   2.7 Systems with a Remote Asset Management System ............................................................................ 46
      2.7.1 FOUNDATION Fieldbus Device Support .................................................................................... 46
      2.7.2 HART Device Support ................................................................................................................ 46

3 FDT Frame Applications .............................................................................................................................. 49

4 Device Manager Gateway Security .............................................................................................................. 59
   4.1 System Security ....................................................................................................................................... 61
   4.2 Open System Operation ....................................................................................................................... 62
   4.3 Secure System Operation ................................................................................................................... 64
   4.4 SDI Connection Issues ....................................................................................................................... 67
      4.4.1 Controller Offline ............................................................................................................................ 67
      4.4.2 SDI Connection Failure ............................................................................................................... 67
   4.5 Security Failures During Initialization ................................................................................................ 68
      4.5.1 Missing Device Manager Gateway Feature Certificate ............................................................... 68
      4.5.2 Insufficient Device Manager Gateway Feature Certificate Privileges ..................................... 70

Appendix A Add a HSE Network to an Emerson AMS ...................................................................................... 73
Appendix B Add HART Multiplexers to an Emerson AMS .................................................................................. 77
Appendix C Loopback Adapter Configuration .............................................................................................. 83
Appendix D Startup Errors ............................................................................................................................ 85
   Unable to Locate FOUNDATION Fieldbus Virtual HSE Adapter .............................................................. 85
   FOUNDATION Fieldbus Virtual Linking Device Limit .............................................................................. 86
1 Overview

The Device Manager Gateway is a WorkstationST* feature that enables communication between the asset management system and fieldbus devices. The gateway handles FOUNDATION fieldbus™, HART®, and PROFIBUS® devices.

**Warning**

The Device Manager Gateway allows communication with third-party device management software that can modify the I/O device configurations at any time.

Follow all safety procedures provided by the third-party device manager and device manufacturers when modifying any I/O device configuration. Failure to follow safety precautions when modifying device configurations could potentially cause equipment mis-operation, which could lead to injury or death.

**Note**

Only Mark* Vle controllers support the FOUNDATION fieldbus, HART, and PROFIBUS device pass-through capabilities required by the Device Manager Gateway.
The Device Manager Gateway enables communication with FOUNDATION fieldbus and HART devices using native communication interfaces supported by third-party asset management software. The Device Manager Gateway also enables communication with HART and PROFIBUS DPV1 capable devices in Field Device Tool (FDT™) frame applications using GE supplied communication device type managers (DTMs) hosted by the frame applications. Metso™ Fieldcare, PACTware™, and Yokogawa® DTM Works are examples of FDT frame applications. The following table lists the device types and software supported.

### Third-party Asset Management Support

<table>
<thead>
<tr>
<th>Device</th>
<th>Emerson AMS</th>
<th>Yokogawa PRM</th>
<th>Yokogawa DTM Works</th>
<th>Honeywell FDM</th>
<th>FDT Frame Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>HART</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FOUNDATION Fieldbus</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PROFIBUS DPV1</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2 Third-party Asset Management Software

The Device Manager Gateway uses virtual hardware interfaces to communicate with third-party asset management software by emulating physical devices connected to the virtual interfaces. It enables Emerson AMS communication with FOUNDATION Fieldbus devices. The gateway also enables communication with HART devices for Emerson AMS, Yokogawa PRM, and Honeywell FDM.

2.1 FOUNDATION Fieldbus Messages

The asset management system is physically separated from the FOUNDATION fieldbus linking devices. The Device Manager Gateway uses the Virtual High-speed Ethernet (HSE) network and virtual linking device communication objects to make the system act as a set of physical linking devices on a local HSE network.
WorkstationST Computer with Device Manager Gateway, Asset Management System, and FOUNDATION Fieldbus

UDH Network

FOUNDATION Fieldbus HSE Messages

SDI Wrapped HSE Messages

FOUNDATION Fieldbus H1 Messages

UDH Network

WORKSTATION

Asset management system

Virtual Linking Devices

Device Manager Gateway

FOUNDATION Fieldbus HSE

Mark Vle controller

IONet Network

FOUNDATION Fieldbus Linking Device

FOUNDATION Fieldbus H1 Network

FOUNDATION Fieldbus Device

WorkstationST Computer with Device Manager Gateway, Asset Management System, and FOUNDATION Fieldbus
The following diagram illustrates the system from the asset management system perspective. The asset management system is not aware of the Device Manager Gateway and thinks that it is talking directly to the linking devices.
2.2 HART Messages

The Device Manager Gateway has the ability to enable communication between the asset management system and HART devices. The Device Manager Gateway creates a set of virtual COM ports to communicate with the asset management system. It emulates physical multiplexer (MUX) networks on the asset management system side and has the controller exchange messages with the actual HART devices using messages to and from the PHRA, YHRA, YSIL, and PUAA I/O packs.

Note YHRA will be identified as a PHRA.
2.3 Configuration (Quick Start)

A common system consists of the asset management system and Device Manager Gateway running on a single WorkstationST computer on a single UDH Network. Refer to the figure WorkstationST Computer with Device Manager Gateway and Asset Management System.

Configure the Device Manager Gateway as follows:

- Install the asset management system on a WorkstationST computer with a connection to the UDH network.
- Enable the gateway on the WorkstationST computer with the asset management system installed.
- Enable the FOUNDATION Fieldbus Message Server property and configure the Loopback Adapter if the system has FOUNDATION fieldbus devices. Configure an HSE network in the asset management system using the loopback adapter.
- Enable the HART Message Server property if the system has HART devices. Configure the asset management system as specified by the Device Manager Gateway Status Viewer.
2.3.1 **Enable the Device Manager Gateway**

*Note* There are no dependencies between the Device Manager Gateway and the other WorkstationST Features.

➢ To enable the Device Manager Gateway

1. From the *Start* menu, select *Programs, GE ControlST*, *ToolboxST*, and *ToolboxST* to display the *ToolboxST System Editor*.

2. From the *Tree View*, double-click the WorkstationST component (such as *EWS1*) to display the *Component Editor*.

![Diagram of a computer interface showing how to enable the Device Manager Gateway](image)

**Warning**

The Device Manager Gateway allows communication with third-party device management software that can modify the I/O device configurations at any time. Enable the Device Manager Gateway Feature only when there is a specific need to interface to third-party device management software.

When the Device Manager Gateway feature is enabled, follow all safety procedures provided by third-party device manager and device manufacturers when modifying any I/O device configuration. Failure to follow safety precautions when modifying device configurations could potentially cause equipment mis-operation, which could lead to injury or death.
2.3.2 Enable the FOUNDA TION Fieldbus Message Server

**Note** For help with common FOUNDA TION fieldbus questions, refer to *Appendix D Startup Errors*.

➢ To enable the FOUNDA TION Fieldbus Message Server

1. Enable the FOUNDA TION fieldbus DTM Message Server property.

   From the **Device Manager Gateway** tab, select **Device Manager Gateway Configuration**.

   From the **Property Editor**, set **Enable FOUNDA TION Fieldbus DTM Message Server** to **True**.
The default settings are optimal and do not need to be changed.

2. Configure the loopback adapter to enable the communication between the asset management system and Device Manager Gateway. Refer to Appendix C Loopback Adapter Configuration for the procedure.

   **Note** For Emerson AMS, to allow write access to FOUNDATION fieldbus device parameters, refer to Appendix G Enable Write Access to FOUNDATION fieldbus parameters.

3. Perform a Build and Download the WorkstationST computer to make the configuration active.

4. Configure the asset management system. Refer to Appendix A Add an HSE Network to an Emerson AMS for the procedure.
Configure the asset management system to use the Virtual HSE Adapter IP Address as the HSE address.
2.3.3 **Enable the HART Message Server**

**Note** Refer to *Appendix H HART Message Server Upgrade Issues.*

➢ To enable the HART Message Server

![Image of Device Manager Gateway configuration]

- From the **Device Manager Gateway** tab, select **Device Manager Gateway Configuration**.
- From the **Property Editor**, set **Enable HART Message Server** to **True**.

---

*When true, enables the HART Message Server functionality in the Gateway. Set this to false to use the standalone HART server on the AMS computer (a separate install selection from the ControlS.*
Referenced device list; all devices are selected by default

Device Manager Software Type: select the type of Device Manager being used

DTM Communication Timeout Period (Minutes): sets the length of time the Device Manager Gateway will wait before closing the connection to a client that is inactive (not sending messages). The Device Manager Gateway will close the connection when there is no client activity and wait for the client to reconnect when further communications are desired.

Enable FOUNDATION Fieldbus Message Server when True, enables communication with FOUNDATION Fieldbus devices.

AMS computer Host or IP Address of remote AMS computer, or localhost if the AMS is on the same workstation.

Enable HART Message Server when True, enables communication with HART devices.

Enable HART Module Type Translation when True, enables the translation of the HART Module Device Type to a type supported by Emerson AMS. (This parameter only applies when Emerson AMS is selected as the Device Manager Software Type, and it is hidden when any other type is selected.)

Maximum Virtual Port Value is the maximum COM Port number the gateway is allowed to use.

Minimum Virtual Port Value is the minimum COM Port number the gateway is allowed to use (Used to establish communications to the AMS.)

**Note** When the Yokogawa PRM® is selected as the Device Manager Application, the Maximum Virtual Port Value must be set to 99, and the Minimum Virtual Port Value should be set to 5.

The default settings are optimal and should not be changed. The asset management system software must be configured to match the gateway configuration and the HART device configuration in the controllers.
2.3.4 Configure HART Communications in Emerson™ AMS

➢➢➢ To configure HART communications in the Emerson AMS

1. From the Start menu, select Programs, GE ControlST, WorkstationST, and Device Manager Gateway Status to start the Device Manager Gateway Status Viewer.

2. Add a HART Multiplexer for each MUX Network entry. Refer to Appendix B Add HART Multiplexers to Emerson AMS.

Note The asset management system configuration for HART devices is uploaded from the controllers when the Device Manager Gateway starts up. The controllers must be online for the Upload command. The controllers can be added to the system incrementally, however, the final asset management system configuration cannot be determined until all controllers have been uploaded. The configuration must be updated each time a new controller is added, or a controller's HART configuration changes.
2.3.5 Configure HART Communications in Yokogawa Plant Resource Management (PRM)

➢➢➢ To configure HART communications in the Yokogawa PRM

1. From the Start menu, select Programs, GE ControlST, WorkstationST, and Device Manager Gateway Status to start the Device Manager Gateway Status Viewer.

2. Add a HART Multiplexer to the asset management system for each MUX Network entry. Refer to Appendix I Add HART Multiplexers to Yokogawa PRM.

Note The asset management system configuration for HART devices is uploaded from the controllers when the Device Manager Gateway starts up. The controllers must be online for the Upload command. The controllers can be added to the system incrementally, however, the final asset management system configuration cannot be determined until all controllers have been uploaded. The configuration must be updated each time a new controller is added, or a controller's HART configuration changes.
2.3.6 Configure HART Communications in Honeywell Field Device Manager (FDM)

➢ To configure HART communications in the Honeywell FDM

1. From the Start menu, select Programs, GE ControlST, WorkstationST, and Device Manager Gateway Status to start the Device Manager Gateway Status Viewer.

2. Add a HART Multiplexer to the asset management system for each MUX Network entry. Refer to Appendix J Add HART Multiplexers to Honeywell FDM.
**Note** The asset management system configuration for HART devices is uploaded from the controllers when the Device Manager Gateway starts up. The controllers must be online for the Upload command. The controllers can be added to the system incrementally, however, the final asset management system configuration cannot be determined until all controllers have been uploaded. The configuration must be updated each time a new controller is added, or a controller's HART configuration changes.
2.3.7 Configuration Changes and Management

The Device Manager Gateway is self-configuring. However, differences in the way FOUNDATION fieldbus and HART devices are managed in the asset management system affect configuration changes in the controllers.

Changes to the gateway configuration are detected as soon as the WorkstationST computer is downloaded. These changes cause the gateway to restart as soon as the download occurs. Modifications to the asset management system configuration may be necessary for it to accurately represent the state of the system. Using the AMS software, perform a Rebuild Hierarchy operation against the HSE network in the asset management system so it will detect the changes and re-configure itself.

**Note** When AMS software is discussed, it is referring to the Emerson AMS Suite, which was used when testing the asset management system.
To communicate with the HART devices, the Device Manager Gateway HART Multiplexer configuration must be updated to match the Status Viewer Configuration tab. Refer to the section *Configure HART Communications in Emerson AMS* or *Configure HART Communications in Yokogawa Plant Resource Management (PRM).*

![Device Manager Gateway Configuration Tab](image)

*Device Manager Gateway Configuration Tab*
2.3.8 FOUNDATION Fieldbus Configuration Changes

**Note** This section only applies to the Emerson AMS. Yokogawa PRM support for FOUNDATION Fieldbus is not supported by the Device Manager Gateway.

FOUNDATION fieldbus technology uses an Ethernet network with an automatic discovery type of architecture. The linking devices broadcast their presence on the HSE network and the asset management system uses these messages to discover the linking devices and query each linking device to determine the field devices connected to it. Any changes to the gateway configuration or the linking devices are automatically detected by the gateway and reflected to the HSE network through HSE annunciation messages. Using the AMS software, perform a Rebuild Hierarchy operation against the HSE network in the asset management system so it will detect the changes and configure itself.

![AMS Suite: Intelligent Device Manager](image)

![Device Explorer](image)

**Rebuild Hierarchy Operation**
If a Mark V1e controller is downloaded with a new configuration that changes the FOUNDATION fieldbus topology under it, the Device Manager Gateway detects the change and reinitializes the virtual linking devices accordingly. The gateway logs an event in the Windows® Event Log whenever this type of change occurs.

This change is automatically reflected in the HSE annunciation messages sent to the asset management system. Perform a Rebuild Hierarchy operation in the AMS software against the HSE network so it will detect the changes and configure itself.
2.3.9 **HART Configuration Changes**

*Note* Refer to the sections [Configure HART Communications in Emerson AMS](#) and [Configure HART Communications in Yokogawa Plant Resource Management (PRM)](#) for additional information.

HART devices communicate with the asset management system through physical multiplexer devices connected to COM ports on the WorkstationST computer. All COM port connections must be configured by the user. This makes automatic configuration of the HART devices impossible at the asset management system level. Whenever a change is downloaded to a Mark VIe controller that affects associated HART devices, the WorkstationST Service shuts down and restarts the gateway. This updates all the controller’s HART devices. The gateway logs an event to the Windows Event Log.

![Windows Event Log](image-url)
2.4 Monitor Status

2.4.1 WorkstationST Status of Features

The Device Manager Gateway status displays in the WorkstationST Status Monitor: Features Status dialog box. The running status and any high-level error conditions are displayed.

The gateway communicates with third-party device management software that can modify the I/O device configurations at any time. The WorkstationST Status Monitor displays the following warning if the gateway is already running when it is started (typically during user logon to the computer) and also whenever the gateway is started while the WorkstationST Status Monitor is already running (typically as a result of a WorkstationST configuration change).
2.4.2 **Windows Event Viewer**

Device Manager Gateway startup and shutdown messages, as well as error conditions display in the Windows Event Viewer.

![Windows Event Viewer and Log](image)

**2.4.3 Device Manager Gateway Status Viewer**

The Device Manager Gateway Status Viewer determines the configuration and status of the gateway and associated devices. It can be used to quickly diagnose configuration or device communication issues. The status viewer connects to the gateway running at the specified hostname or IP Address and displays live information.
2.4.3.1 Configuration Tab

The Configuration tab displays the running gateway configuration. If the HART Message Server is enabled, it also displays the required Emerson AMS or Yokogawa PRM configuration.

![Configuration Tab for Emerson AMS HART Configuration](image-url)
The Yokogawa PRM Mode displays.

The PRM Configuration displays.

Device Manager Gateway Status Viewer Configuration Tab for Yokogawa PRM HART Configuration
2.4.3.2 **Fieldbus Tab**

The Fieldbus tab displays both the physical topology from the controller point of view and the virtual HSE network topology as seen by the asset management system.

The physical linking devices and their IONet addresses display. The virtual PFFA connections also display. The Fieldbus tab displays the redundant linking device status and the status of the devices below them. For example, if a device in the asset management system is unresponsive, the Fieldbus tab information determines if the device and/or its hosting linking device is online and communicating with the gateway.
A Detail View (selected from the View menu) displays low-level information for debugging purposes. The following figure displays the detail view of controller AnalogM6e, a single redundant linking device pair, and two FOUNDATION fieldbus devices.

**Fieldbus Tab Detail View**

The asset management system sees a virtual linking device at address 10.1.58.22, and the gateway is currently routing HSE messages to the linking device at the primary IONet address of 192.168.1.22. Each linking device displays its IONet address and its redundancy role (primary or backup). Each device entry displays its online status and basic information about the device. In this example, the backup linking device is offline, and the link and device entries below it are grayed out to indicate that the information is not current.

*Note* The same field devices display under each linking device in a redundant pair.
### 2.4.3.3 HART Tab

The HART tab displays the controllers and their configured I/O packs. The I/O pack communication and channel status is also provided. If a device is present on a channel, its ID displays. The virtual COM port connection for each set of I/O packs in a particular I/O cabinet (MUX network from the asset management system perspective) also displays. Communication issues between the asset management system and gateway devices are identified. For example, if a device is unresponsive in the asset management system, the HART tab information determines if the corresponding I/O pack is online and communicating with the Device Manager Gateway.
2.4.3.4 HART AMS Connection Tab

The HART AMS Connection tab displays the status of the virtual COM ports created by the Device Manager Gateway. The ports pass HART messages between the gateway and the asset management system.
2.5 Systems with Multiple UDH Networks

Systems with multiple UDH networks require multiple Device Manager Gateways and potentially more than one asset management systems.

Note Refer to Appendix E UDH Partitioning.

The default Device Manager Gateway configuration supports systems with one asset management system/gateway pair per UDH network. With this configuration, each pair can see only the devices on its associated UDH network.

Note The gateway configuration is limited to the UDH network connections of the host WorkstationST computer.

One Asset Management System/Device Manager Gateway Pair per UDH Network
The gateway configuration allows the selection of the UDH Network. All devices on that network are visible to the asset management system by default.

Note Refer to the section Configuration (Quick Start) for message server configuration options.
2.5.1 Common Asset Management System

The Device Manager Gateway configuration supports multiple gateways sending information to a single asset management system. However, the asset management system must be installed on a separate computer. A physical HSE network supporting all computers is necessary if FOUNDATION fieldbus message support is required. The WorkstationST computer with the asset management system installed must also run the Remote HART Message Server Connection Server.

Common Asset Management System for Multiple UDH Networks and its ToolboxST Configuration
2.5.1.1 FOUNDATION Fieldbus Message Server Configuration

➢ To configure the FOUNDATION fieldbus message server: from the ToolboxST System Editor, double-click the WorkstationST component (such as EWS1_FF) to display the Component Editor.

From the **Device Manager Gateway** tab **Tree View**, select **Device Manager Gateway**.

From the **Property Editor**, in the **UDH Network** text box, select the appropriate **UDH network** from the drop-down list.

In the **Virtual HSE Adapter IP Address** text box, enter the address of the WorkstationST computer hosting a gateway.
2.5.1.2 HART Message Server Configuration

➢ To configure the HART Message Server: from the ToolboxST System Editor, double-click the WorkstationST component (such as EWS1_FF) to display the Component Editor.

From the **Device Manager Gateway** tab **Tree View**, select **Device Manager Gateway**.

From the **Property Editor**, in the **AMS computer Host or IP Address** text box, enter the **PDH address** of the asset management system computer for all gateways.

Select **Maximum Virtual Port Value** and **Minimum Virtual Port Value**, and select a virtual COM Port range in each Device Manager Gateway. Ensure the ranges do not overlap (for example one can use 10 – 99 and another can use 100 – 254).

**Note** Refer to the section *Systems with a Remote Asset Management System* for further details about configuration options.

Optionally, the Device Manager Gateways can be configured to send HART messages over the virtual HSE network by using the virtual HSE network address of the asset management system computer instead of its PDH address. Supporting both **FOUNDATION** fieldbus and HART message traffic on the virtual HSE network can degrade Device Manager Gateway performance.
2.5.1.3 HART Message Server Client Configuration

Perform this procedure on the WorkstationST computer running the asset management system.

➢ To configure the HART Message Server Client: from the ToolboxST System Editor, double-click the WorkstationST component (such as EWS2) to display the Component Editor.

From the Device Manager Gateway tab Tree View, select Device Manager Gateway.

From the Property Editor, select Enable Remote HART Message Server Client and in the text box, select True from the drop-down menu.

No further configuration is needed as the Remote HART Message Server Client waits for the gateways to connect and provide configuration information.
2.6 Performance and Limitations

The Device Manager Gateway and the controller pass-through mechanism can delay overall asset management system performance. However, the effects should be negligible when compared to asset management system performance with connections to a true HSE network with physical linking devices. Combined performance depends primarily on the size of the system (number of linking devices and fieldbus devices) and the capability of the computer running them.

2.6.1 Device Manager Gateway

Improve performance by:

• **Dedicated WorkstationST computer** – Run the Device Manager Gateway on a WorkstationST computer with no other WorkstationST Features enabled and no other resource intensive software installed. All computer resources are then available to the gateway.

• **Server class computer** – Run the Device Manager Gateway on a server class computer to maximize gateway performance with WorkstationST Features and multiple devices.

*Note* Refer to Appendix E UDH Partitioning.

• **Partition multiple gateways** – Partition the system into multiple gateways per UDH to reduce the number of field devices supported by each gateway.

The Device Manager Gateway enforces a hard limit of 500 virtual linking devices per gateway. Systems with more than 500 virtual linking devices (stand-alone and redundant linking device pairs) must partition the system between multiple gateways.

2.6.2 Asset Management System

Asset management system speed for performing high-traffic tasks such as rebuild hierarchy drops as the number of devices increases. Partition the system into multiple asset management system/gateway pairs per UDH to reduce the number of field devices supported by each asset management system.
2.7 Systems with a Remote Asset Management System

The Device Manager Gateway supports FOUNDATION Fieldbus and/or HART communications between the ToolboxST application and a remote asset management system.

2.7.1 FOUNDATION Fieldbus Device Support

Note Refer to Appendix F Create a Virtual HSE Network for additional information.

A virtual HSE network connection between the asset management system computer and the WorkstationST computer running the Device Manager Gateway is necessary for communication. The gateway broadcasts the system topology on the virtual HSE network and the asset management system uses these messages to configure itself whenever a Rebuild Hierarchy command is issued.

Remote Computer with Third-party Asset Management System and its ToolboxST Configuration

2.7.2 HART Device Support

Communications between a third-party asset management system computer and the Device Manager Gateway for HART devices requires the installation of the WorkstationST application on the remote computer, and an Ethernet connection between the asset management system computer and the gateway. Any Ethernet network can be used, including the virtual HSE network connection if FOUNDATION fieldbus support is also required.
2.7.2.1 Remote Computer Configuration
Install the ToolboxST and WorkstationST applications on the asset management system computer and create a system with one WorkstationST component. Enable the Device Manager Gateway and the Remote HART Message Server Client properties.

2.7.2.2 Local Computer Configuration
Enable the HART Message Server on the local WorkstationST computer. Configure as normal and enter the IP Address of the remote asset management system computer in the HART Message Server configuration.
2.7.2.3 Remote HART Message Server Client Status

The HART AMS Connection tab of the Device Manager Gateway Status Viewer displays connection and virtual COM port status.
3  FDT Frame Applications

FDT technology is an interoperability standard that standardizes the communication and configuration interface between all field devices and host systems. FDT provides a common environment for accessing the devices’ most sophisticated features. Any device can be configured, operated, and maintained through the standardized user interface, regardless of supplier, type, or communication protocol. For a complete description of FDT technology, refer to the FDT Group™ web site at www.fdtgroup.org.

To support a broader set of field devices and device management/asset management applications, GE has leveraged the benefits of FDT technology by developing a set of FDT Group certified DTMs to provide HART over Ethernet and PROFIBUS DP-V1 over Ethernet Device Manager capability in coordination with the Device Manager Gateway. The DTMs allow management of HART and PROFIBUS DP-V1 devices from any FDT frame application from virtually any computer. For further details, refer to the Device Manager User Guide (GEH-6821).

GE has also developed the Device Manager Essentials FDT frame application that provides basic device management capabilities. More advanced device management and asset management capabilities can be realized by using more fully featured third-party software such as Metso Fieldcare or PACTware™.

The Device Manager Gateway WorkstationST feature runs on a WorkstationST computer with UDH network connectivity to the Mark VIe controllers. The FDT frame application can run on this computer, any other WorkstationST computer, or even a customer computer, that does not have the WorkstationST application installed, provided that it has network connectivity (typically over the PDH network) to the WorkstationST computer running the Device Manager Gateway feature. The DTMs are installed on the computer hosting the FDT frame application, as illustrated in the following figure. An instance of the communication DTM is added to the FDT frame application, and the communication DTM requests the ToolboxST system topology from the Device Manager Gateway to automatically create instances of the corresponding I/O module DTMs. The I/O module DTMs are then used to scan for devices connected to them, and instances of the corresponding device DTMs are automatically created.
WorkstationST Computer with Device Manager Gateway and FDT Frame Application
The GE DTMs are software components running in a FDT frame application that provide a consistent interface between the frame application and the Device Manager Gateway. The same communication code runs in every Frame Application regardless of the vendor, eliminating vendor specific issues associated with native interfaces.

Providing DTMs and a TCP/IP interface between the communication DTM and the Device Manager Gateway provides compatibility with the wide array of FDT frame applications available on the market and provides the freedom to run that software from virtually anywhere on any computer.

To configure the Device Manager Gateway for FDT/DTM support, the Device Manager Gateway feature must be enabled in a WorkstationST computer that has UDH network connectivity.

**Note** Large systems or systems with multiple UDH networks may require multiple Device Manager Gateways running on different workstation computers. Refer to *Appendix E UDH Partitioning* for more information.

➢➢➢ To configure the Device Manager Gateway for FDT/DTM support

1. From the Start menu, select Programs, GE ControlST, ToolboxST, and ToolboxST to display the ToolboxST System Editor.

2. From the Tree View, double-click the WorkstationST component (such as Wkstn) to display the Component Editor.

From the General tab, select Features.

From the Summary View, select Device Manager Gateway and set to True.
From the **Device Manager Gateway** tab **Tree View**, select the **Device Manager Gateway** item.

From the **Property Editor**, select **Device Manager Software Type** and from the drop-down list select the type to use.

FDT/DTM support will be enabled if the type selected represents an DFT frame application.

---

**Note**  The list includes all of the tested Device Manager application types. The Emerson_AMS and Yokogawa_PRM_Native types use virtual COM ports to provide the communication interface. All other types are FDT frame applications and selecting them enables the DTM communication interface. If the software type being used is an FDT frame application not in the Device Manager Software Type drop-down list, select **Other_FDT Frame Application**.
From the **Property Editor**, select **DTM Communication Timeout Period (Minutes)** and enter the time (refer to the definition).

From the **Property Editor**, enable the **Foundation Fieldbus**, **HART**, and/or **Profibus Message Server** as needed.
After enabling a server, you are offered the option of selecting *Referenced* devices.

3. Build and download the workstation.

   From the **WorkstationST Status Monitor**, verify that the download is successful and the **Device Manager Gateway Feature** starts up and runs without errors.
Optional Steps

a. From the WorkstationST Status Monitor, right-click the Device Manager Gateway Feature and select View Device Manager Gateway Status from the shortcut menu to display the Device Manager Gateway Status Viewer.

b. The Configuration tab displays the running configuration of the Device Manager Gateway.

From the Configuration tab, the downloaded configuration displays.

Verify that the HART Message Server and HART Communication DTM Interface are enabled.

Verify the state of the PROFIBUS Message Server and FOUNDATION Fieldbus Interfaces match the configured state.
c. The **HART** tab displays the physical topology of the system from the HART perspective by listing all of the controllers referenced by the Device Manager Gateway, and the status of the I/O modules and connected devices beneath them.

![Example HART PHRA I/O Pack Topology](image)

**Example HART PHRA I/O Pack Topology**

d. The **PROFIBUS** tab displays the physical topology of the system from the PROFIBUS perspective by listing all of the controllers referenced by the Device Manager Gateway, and the status of the PPRF modules and devices on their respective PROFIBUS networks.

![Example PROFIBUS Topology](image)

e. The **Foundation Fieldbus DTM** tab displays the physical topology of the system from the FOUNDATION fieldbus perspective by listing all of the controllers referenced by the Device Manager Gateway, and the status of the PFFA modules and devices.
f. The **CommDTM Connections** tab displays all of the active Device Manager Gateway connections to PROFIBUS, HART, and FOUNDATION Fieldbus communication DTMs running in FDT Frame Applications.
4 Device Manager Gateway Security

Beginning with in ControlST V06.00.00 and later, the Device Manager Gateway feature communicates over secure SDI connections with the Mark VIe controllers in secure systems. The following diagram illustrates how the Device Manager Gateway feature uses the certificate found in the certificate store of the computer on which it is running, and uses that certificate to authenticate with the controller to establish a secure SDI connection.

The controllers use the secure SDI connections to prevent unauthorized software from connecting to and exchanging data with the controllers. Refer to the ToolboxST User Guide for Mark Controls Platform (GEH-6700), the section Security for additional information on secure system configuration and certificate management.
Device Manager Application

Certificate Store

Device Manager Gateway

Secure SDI Connection

CA Server

Mark Vie Controller

IO Modules

Field Devices

Device Manager Gateway SDI Certificate Authentication
4.1 System Security

The Device Manager Gateway uses the CA Server Full Name and CA Server IP Address system level properties to determine whether it is running in a secure system.

If CA Server Full Name and CA Server IP Address are specified (not empty) then DMG will operate in secure mode, otherwise DMG will operate in Open mode.
4.2 Open System Operation

Device Manager Gateway reads the CA Server Full Name and CA Server IP Address values during its initialization. If the Security Server properties are empty, DMG will start up and operate in Open mode. The Configuration tab of the Device Manager Gateway Status Viewer displays the configured System Security mode detected by the DMG at startup. The following figure shows an example where System Security has not been configured and DMG will operate in Open mode.
DMG and the controllers will operate in Open mode in a system without a configured Security Server. There is no change in operation from previous versions of Device Manager Gateway in Open mode. Certificates are not used and are not needed in an Open system. DMG will use Open SDI connections to exchange data with the controllers. The fieldbus tabs of the Device Manager Gateway Status Viewer show the state of the SDI connections to the controllers. The following figure shows the SDI connections to three controllers under the HART tab.

All of the SDI connections are established and actively exchanging data (indicated by the <CONNECTED> status). The SecurityState value indicates the Security State of the controller, and in this example system security is not enabled, so all of the controllers are in Open mode. The Directive value indicates the security level that DMG is using to establish the connection. DMG will use an Open SDI connection type whenever the controller Security State is Open, which is the only possible security state for the controller in an Open system.
4.3 Secure System Operation

The Security Servers properties are filled out as part of the configuration of a secure system. A certificate named GeCssDeviceManagerGateway must also be created and assigned to the My substore under the LocalMachine location in the Certificate Store of the PC running the DMG. For the procedure to create the Device Manager Gateway SDI certificate and deploy it to the computer hosting the Device Manager Gateway feature, refer to the Control Server — Domain Services Maintenance Guide (GEH-6845), the section Create and Deploy SDI Certificates for WorkstationST Features.

The Feature Certificates tab of the WorkstationST Certificate Manager (which is launched from the Tools item of the main menu in WorkstationST Status Monitor) can be used to view the feature certificates and their properties in the local PC Certificate Store.

When DMG starts up, it examines the Security Servers properties to determine if it is running in a secure system. If it determines that it is running in a secure system it will search the Certificate Store on the local PC to locate the required Device Manager Gateway feature certificate. If the GeCssDeviceManagerGateway certificate is found, DMG displays the Security Servers values and the Device Manager Gateway feature certificate information on the Configuration tab of the Device Manager Gateway Status Viewer.
**Note** If the feature certificate cannot be found in the store, DMG will report the missing certificate error and suspend its operation until a valid certificate is imported into the Certificate Store and the feature is restarted. DMG will also report an error and suspend operation if the feature certificate that it finds does not provide at least the minimum capability level required to perform all secure Read and Write operations over a Secure SDI connection. Refer to the [Security Failures During Initialization](#) section for more information.

Once Device Manager Gateway initialization is complete, the fieldbus tabs of the Device Manager Gateway Status Viewer show the state of the SDI connections to the controllers. The screen shot below shows the SDI connections to three controllers under the HART tab.
All of the SDI connections are established and actively exchanging data (indicated by the <CONNECTED> status). The SecurityState value indicates the security state of the controller and in this example system security is enabled and all of the controllers are in Secure mode. The Directive value indicates the security level that DMG is using to establish the connection. DMG uses the AuthenticateAndEncrypt security directive to establish the SDI connection whenever the controller Security State is Secure.

**Note** A controller in a secure system can be taken out of Secure mode and put in Open mode. DMG determines which directive to connect with based on the controller’s security state. DMG will use the Open directive if the controller is in Open mode, and DMG will use the AuthenticateAndEncrypt directive if the controller is in Secure mode. Based on this criteria, DMG will connect using the Open directive when the controller is in Open mode in a secure system, which is a valid and supported mode of operation. In the invalid and essentially impossible case where the controller is in Secure mode in a system where the **Security Servers** properties are not filled out, DMG will attempt to connect with the AuthenticateAndEncrypt directive and will fail to connect because it will not have the necessary certificate information to establish a secure SDI connection with the controller.
4.4 SDI Connection Issues

4.4.1 Controller Offline

The controller connection status is shown as <OFFLINE> in the Device Manager Gateway Status Viewer if the controller is not responding on the network.

4.4.2 SDI Connection Failure

If there is a security failure when attempting to establish an SDI connection to the controller the connection status will be shown as <CONNECT ERROR> in the Device Manager Gateway Status Viewer. Hovering over the connection with the mouse will bring up a tooltip with additional information about the cause of the failure.

In the example above, the Security Servers properties were cleared and the controllers were left in secure mode. The tooltip text contains the following message, which clearly indicates that the certificate information is not available to establish the SDI connection:

Secure Connection failed: cannot create a secure connection. Missing system level data like CA Server name and domain, and/or user login name
4.5 Security Failures During Initialization

Device Manager Gateway relies on the GeCssDeviceManagerGateway certificate to be able to connect to the controllers in secure mode in a secure system. Device Manager Gateway detects issues with its feature certificate and suspends its operation during its initialization phase if a valid certificate cannot be found.

4.5.1 Missing Device Manager Gateway Feature Certificate

When Device Manager Gateway starts up, it examines the Security Servers properties to determine if it is running in a secure system. If it determines that it is running in a secure system it will search the Certificate Store on the local PC to locate the required Device Manager Gateway feature certificate. If the GeCssDeviceManagerGateway certificate is not found, Device Manager Gateway will suspend its operation and report the error in both the WorkstationST Status Monitor and the Windows Event Log.

*Note* The Device Manager Gateway Status Viewer will not be able to connect to the Device Manager Gateway Feature in the certificate not found state because the feature operation has been suspended.

The figure above shows the Error reported by the Device Manager Gateway feature when the certificate cannot be found. The full text of the error message is:

*A Certificate named GeCssDeviceManagerGateway could not be found in the Certificate Store- Device Manager Gateway feature operation will be suspended until a certificate is provided and the feature is restarted.*
The error is also reported to the Windows event log as follows:

![Event Viewer](image)

The Feature Certificates tab of the WorkstationST Certificate Manager can be used to view the contents of the LocalMachine \My certificate store. The WorkstationST Certificate Manager can be launched from the Tools Menu of the WorkstationST Status Monitor utility.

![WorkstationST Status Monitor](image)

To restore Device Manager Gateway operation, import the GeCssDeviceManagerGateway feature certificate into the LocalMachine location My substore and restart the Device Manager Gateway feature.

![WorkstationST Certificate Manager](image)
4.5.2 Insufficient Device Manager Gateway Feature Certificate Privileges

When Device Manager Gateway starts up, it examines the Security Servers properties to determine if it is running in a secure system. If it determines that it is running in a secure system it will search the Certificate Store on the local PC to locate the required Device Manager Gateway feature certificate. If the GeCssDeviceManagerGateway certificate is found, Device Manager Gateway will determine the certificate’s configured Capability level. Device Manager Gateway requires a Capability level of Set or higher to operate correctly. If the GeCssDeviceManagerGateway certificate has only Base level Capability, Device Manager Gateway will suspend its operation and report the error in both the WorkstationST Status Monitor and the Windows Event Log.

Note The Device Manager Gateway Status Viewer will not be able to connect to the Device Manager Gateway Feature in the certificate not found state because the feature operation has been suspended.

The figure above shows the Error reported by the Device Manager Gateway feature when the GeCssDeviceManagerGateway feature certificate has insufficient capability. The full text of the error message is:

The Device Manager Gateway feature certificate does not have sufficient Capability to support secure data exchanges with the controllers. The supplied certificate has Base Capability, while a certificate with a minimum of Set Capability is required. Feature operation will be suspended until a certificate with sufficient capability is provided and the feature is restarted.
The error is also reported to the Windows event log as follows:

The Feature Certificates tab of the WorkstationST Certificate Manager can be used to view the contents of the LocalMachine \My certificate store. The WorkstationST Certificate Manager can be launched from the Tools Menu of the WorkstationST Status Monitor utility.
Public Information
Appendix A Add a HSE Network to an Emerson AMS

Perform the following procedure to add the HSE network to a computer with the Emerson AMS software.

➢ To add a HSE network to an Emerson AMS computer

From the Start menu, expand AMS Device Manager and select Network Configuration.

From the Network Configuration dialog box, click Add.
Select the type of network to install (such as FF HSE Network). Click **Install** and **Next**.

In the **Network Name** text box, enter a name for the network (such as **FF HSE Net 1**). Click **Next**.
From the Connection tab, in the Primary HSE NIC Address text box, select the appropriate address from the drop-down menu.

Click to select Enable processing and acknowledgement of FF device alerts if required.

Click OK.
Appendix B Add HART Multiplexers to an Emerson AMS

The Device Manager Gateway creates several COM ports for Multiplex networks. The Device Manager Gateway Status Viewer Configuration tab displays the MUX networks at the bottom of the window.

Perform the following procedure to add the MUX Network specified in the Device Manager Gateway Status Viewer to an Emerson AMS. In the following figure, the networks GT1_WrkStn and SIL1_Cab1 have been created. For this example, use the AMS Network Configuration to add Multiplexer Networks named GT1_WrkStn at COM10 and SIL1_Cab1 at COM11.
The name of the Device Manager is based upon the individual computer or site naming conventions.

➢➢

To add a Multiplexer Network to an Emerson AMS: from the Start menu, expand AMS Device Manager and select Network Configuration.
From the AMS Network Configuration dialog box, click **Add** to select a network type.

Select the network type to install (Multiplexer Network is selected for this example), then click **Install**.
Click **Next** to begin installation.

Enter the network name (**GT1_WrkStn for this example**) and click **Next** to continue.
Continuing with our example, COM10 was listed as a MUX network and the Multi-drop Range was listed as 0 to 2. (Refer to the figure Device Manager Gateway Status Viewer Configuration Tab.)

Select COM10 for the COM Port and select 0 to 2 for the RS485 Address from / to range.

Click OK to complete the connection.
Appendix C Loopback Adapter Configuration

➢ To configure a Microsoft® Loopback Adapter
1. From the Control Panel, select Add Hardware.
2. From the Add Hardware Wizard, click Next and select Yes, I have already connected the hardware. Click Next.
3. Select Install the hardware that I manually select from a list (Advanced) and click Next.
4. From the Hardware type dialog box, select Network Adapters and click Next. The list of hardware manufacturers and drivers displays.

Select Microsoft Loopback Adapter and click Next twice.
Appendix D Startup Errors

Unable to Locate FOUNDATION Fieldbus Virtual HSE Adapter

The Device Manager Gateway uses the Virtual HSE Adapter IP Address property value to locate the physical or loopback adapter acting as the Virtual HSE Network Adapter for the WorkstationST computer. This address is sometimes referred to as the base address, and is used in calculating the Virtual Linking Device IP Addresses used by the gateway.

**Device Manager Gateway Tab**

- **Description**: An adapter with the Virtual HSE Adapter IP Address cannot be found and the Device Manager Gateway sends an error to the Windows Event Log and shuts down.
- **Possible Cause**: The base address was not entered, or was entered incorrectly
- **Solution**: Add the base address to the Virtual HSE Network Adapter in the WorkstationST computer, or enter the correct Virtual HSE Network Adapter base address in the Virtual HSE Adapter IP Address field.
**FOUNDATION Fieldbus Virtual Linking Device Limit**

**Description** The Device Manager Gateway has an internal limit of 500 virtual linking devices. The number of virtual linking devices created by the Device Manager Gateway *Consumed Devices* list exceeds the internal limit, an error is sent to the Windows Event Log and the gateway shuts down.

**Possible Cause** More than 500 virtual linking devices are required for the configuration

**Solution** Partition the linking devices between multiple Device Manager Gateways on the target UDH network. Refer to *Appendix E UDH Partitioning* for additional information.

---

**FOUNDATION Fieldbus Virtual HSE Address Collision**

**Description** The Device Manager Gateway detects that one or more of the virtual linking device addresses that it is attempting to use is already in use on the virtual HSE network. An error message is sent to the Windows Event Log and the gateway shuts down. The error message includes the address or addresses where the collision has occurred.

**Note** This should not occur when the gateway and asset management system communicate over a loopback adapter on the same computer.

**Possible Cause** When the gateway and asset management system are running on separate computers connected by a physical virtual HSE network, the cause is typically improper partitioning between multiple gateways. If multiple gateways reference the same device, the virtual linking device addresses for the devices under them will coincide, causing address collisions on the network.

**Solution**

- Verify by opening an instance of the Status Viewer for each gateway and compare the Consumed Devices list for devices consumed by multiple gateways. Fix the partitioning overlap and manually delete the virtual linking device addresses from the gateway virtual HSE adapters before restarting them.
- The collision could be the result of third-party devices on the virtual HSE network. The network is intended to be completely isolated between the asset management system and gateway computers, and should not have additional devices connected. If this cannot be avoided, use a different base address for the virtual HSE network adapter in the gateway. The gateway uses the first octet of the base address as the first octet in the virtual linking device addresses that it creates. For example, if there is a collision at address 10.1.38.21 with the default base address of 10.0.0.1, change the base address to 11.0.0.1 to move the virtual linking device address to 11.1.58.12.
Appendix E UDH Partitioning

The Device Manager Gateway consumes all controllers on the UDH by default. The configuration allows consumed device selection at the controller level to allow the controllers on the UDH network to be partitioned between multiple gateways running on multiple Workstation computers.

The partitioning is accomplished by selecting a mutually exclusive set of controllers in each configuration. An overlap between the consumed device lists is not allowed.
Appendix F Create a Virtual HSE Network

The Device Manager Gateway and the asset management system typically exist on the same computer configured with the Workstation ST application, and communicate using the loopback adapter. When they exist on different computers, a physical virtual HSE network is required. This network must be dedicated to the message traffic between the two, and be physically isolated from all other networks and devices. Virtual HSE network constraints include:

- A physical adapter in each gateway and asset management system computer connected only to the virtual HSE network
- Physically isolated network switches or hubs (or even a single crossover cable if computer proximity allows it) that is not part of or connected to the existing site switch
- No device or computer connections other than the WorkstationST computers hosting the gateway and asset management system software
Appendix G Enable Write Access to FOUNDATION Fieldbus Device Parameters

**Note** This option is only available when using the Emerson AMS gateway.

The Device Manager Gateway allows read-only access to FOUNDATION fieldbus device parameters by default.

Set **Enable Foundation Fieldbus Device Configuration Messages** to **True**. An error message is returned if a user attempts to modify a read-only value.

**Note** The **Enable FOUNDATION Fieldbus Device Configuration Messages** property allows or denies access to all FOUNDATION fieldbus device parameters. Access to the HART devices is configured at the I/O pack input/output level, and access to the HART device is unrestricted if HART is enabled on the input or output to which it is connected.
Example of PHRA Output with HART Enabled
Appendix H HART Message Server Upgrade Issues

Sites that upgrade to ControlST V04.03 and later, and use a stand-alone HART Message Server, can transition the HART Message Server functionality to the Device Manager Gateway or use an option where the stand-alone HART Message Server product continues to act as the gateway for HART messages while the Device Manager Gateway manages the FOUNDATION fieldbus devices. Upgrading to the Device Manager Gateway is recommended for long-term support reasons.

If the asset management system software is installed on a WorkstationST computer, enable the Device Manager Gateway, add a loopback adapter, and configure the FOUNDATION Fieldbus Message Server property as previously described. Leave the HART Message Server property of the Device Manager Gateway disabled to avoid conflicts with the stand-alone HART Message Server.

Modified Asset Management System and Device Manager Gateway System

If the asset management system software is installed on a computer not in the ToolboxST application, it must be added to the system configuration. Install the WorkstationST application on it, and enable and configure the Device Manager Gateway for FOUNDATION Fieldbus Message Server functionality only.

Add the computer to the ToolboxST application, and install the WorkstationST application on it. Uninstall the stand-alone HART Message Server product. On the Device Manager Gateway, enable the HART Message Server property (and FOUNDATION Fieldbus Message Server property if appropriate) and build and download the WorkstationST computer.
Appendix I Add HART Multiplexers to Yokogawa

The Device Manager Status Viewer Configuration Tab displays the configuration necessary for the Yokogawa PRM to communicate with HART devices through the Device Manager Gateway. The gateway creates virtual COM ports, which make the I/O packs appear to be HART multiplexers directly connected to the COM ports. The Device Manager Gateway recommends the multiplexers be grouped under projects with names based on the Mark VIe controller and I/O cabinet that they are physically located under. The PRM only supports COM port numbers 1 through 99, so the gateway configuration must limit the available COM ports to this range. Also, the PRM has an 8-character limit on the recommended names, so the project names may need to be shortened.

➢ To add a HART multiplexer to the PRM
1. Open the Device Manager Gateway Status Viewer and select the Configuration tab.
2. Open the **PRM Setup Tool**.

3. From the **Tree View**, expand **Field Communication** and **Device Path**, and select the **Local** communication path.

4. Right-click **LOCAL** network and select **New** to create a new project.

5. In the **Project Name** text box, enter the project name specified in the **Device Manager Gateway Status Viewer Configuration** tab (in this case **AnalogM6e_Cab1**, shortened to **AM6eCab1**). Click **OK**.

6. Right-click the new project and select **New**.
7. In the IOM Type text box, select MTL4840 from the drop-down list and click OK.

8. Add any additional multiplexers specified in the Device Manager Gateway PRM Configuration tab.

   In the COM Port No., Master No., Slave No., and Preamble text boxes, enter the information specified in the Device Manager Gateway Status Viewer Configuration tab. (The PRM limits the maximum COM port number to 99.)

   Click OK.
9. Click the **Restart Field Comm. Service** button to make the changes available to PRM.
10. Start the PRM if it is not already running.

Select **Network**.

From the **Tree View**, right-click **LOCAL** and select **Plug & Play** to initiate the scan of the physical multiplexers and devices.

The new project and the multiplexers display in the PRM Network view.
Appendix J Add HART Multiplexers to Honeywell Field Device Manager (FDM)

The procedure to configure HART Multiplexers in Honeywell FDM is provided in Appendix K Honeywell Field Device Manager (FDM) Configuration.
Honeywell Field Device Manager (FDM) provides HART device configuration and monitoring (asset management) for HART devices connected to HART Multiplexers connected to RS485 networks via local PC COM ports.

**FDM System Topology**

In the Mark V1e architecture, host applications like FDM do not have physical access to the HART enabled GE I/O modules, which emulate HART Multiplexers. GE developed the WorkstationST Device Manager Gateway (DMG) feature to create a virtual COM port interface that allows third-party device management applications like FDM to interact with the GE Multiplexer I/O Modules as if they were directly connected to a local RS485 network.
As shown in the system topology diagram above, Honeywell FDM typically runs on a PC that does not have access to the GE controller (UDH) network. DMG Server runs on an HMI with UDH access and connects to a DMG Client running on the FDM Server PC, which creates the virtual COM ports used by FDM.

➢➢ To Configure the Device Manager Gateway Server

1. Enable the Device Manager Gateway.

**Note** Enable the Device Manager Gateway on an HMI with UDH connectivity to the controller(s) with HART I/O Modules that will be monitored by FDM.
2. Configure the **Device Manager Gateway** tab.

   From the **Device Manager Gateway** tab, in the **Device Manager Software Type** field, select **Honeywell FDM**.

   In the **Enable HART Message Server field**, select **True**.

   In the **AMS computer Host or IP Address field**, enter the hostname or IP address of the FDM PC.

   In the **Maximum Virtual Port Value** and **Minimum Virtual Port Value fields**, enter values in a range that does not conflict with any physical COM ports in the FDM PC.

   Select **True** in the **Referenced** column for the controller(s) with HART devices to be monitored by DMG.

   **Note** The Virtual Port range must be between 1–255. FDM does not support COM port numbers above 255. Refer to the *FDM Installation and Configuration Guide*, section 4.5.

3. Build and Download the DMG Server Workstation configuration.
4. Open the **WorkstationST Status Monitor** and verify that the **Device Manager Gateway** feature is running.

Right-click on the **Device Manager Gateway** feature and select **View Device Manager Gateway Status**.
The Device Manager Gateway Status Viewer displays. The Configuration tab summarizes the CMG settings made in ToolboxST.

The Honeywell Field Device Manager (FDM) Configuration instructions display.

Run the FDM Server Management tool and create the following RS-485 HART Multiplexer Networks with the corresponding COM port assignments and polling address ranges.

See GEI-100757 WorkstationST Device Manager Gateway Instruction Guide for detailed information.

MUX Network = Dual_Cab1. COM10, Start Poll Address = 0, End Poll Address = 2
➢ To Configure the Device Manager Gateway Client on the FDM Server

1. Install and license **WorkstationST** on the FDM Server.
2. Create a **Workstation Device** in **ToolboxST** that corresponds to the FDM Server. In this example, it is named FDM_Server.
From the General tab, configure **Network Adapter 0** with the IP Address of the FDM Server.

This is the address that ToolboxST will use to download the Remote HART Message Server Client configuration that DMC will use to connect to the remote client.
3. Build and Download the FDM Server Workstation configuration.

4. Open the **Device Manager Gateway Status Viewer** and select the **HART Device Manager Connection** tab.
To Configure the Honeywell Field Device Manager (FDM)

Note: Make sure the **Start Poll Address** and **End Poll Address** corresponds to the values specified in the DMG Status Viewer.

---

**Honeywell Field Device Manager (FDM) Configuration**

Run the FDM Server Management tool and create the following RS-485 HART Multiplexer Networks with the corresponding COM port assignments and polling address ranges.

See GEI-100757 Workstation ST Device Manager Gateway Instruction Guide for detailed information.

**MUX Network = Dual_Cab1, COM10. Start Poll Address = 0, End Poll Address = 2**
Configure the network using the values specified in the DMG Status Viewer, then click OK.

The Network Interface Name field corresponds to the MUX Network in the DMG Status Viewer.

The Network Configuration window displays the configured network(s).

In this example, the Dual_Cab1 network is configured.
Open the FDM Client.

From the Network View tab, right-click on the COM network (in this example, Dual_Cab1) and select Build Network.

This starts the scan of the Multiplexers and connected devices.
The multipliers and connected devices are added under the COM network.

The Information tab shows the progress and when the process is complete.

In this example, the PHCA module was offline during the scan and not included in the network topology.

Double-click the device to view its status.

In this example, the PHCA TF status displays.

Network build operation for Dual_Cab1 is complete. No devices were discovered for this node.

Network build operation for Dual_Cab1 is in progress.

Network build operation for Dual_Cab1 is complete.